

Huansheng Ning (Ed.)

Communications in Computer and Information Science

1137

Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health

International 2019 Cyberspace Congress, CyberDI and CyberLife
Beijing, China, December 16–18, 2019
Proceedings, Part I



Part 1

 Springer

Communications in Computer and Information Science


1137

Commenced Publication in 2007

Founding and Former Series Editors:

Phoebe Chen, Alfredo Cuzzocrea, Xiaoyong Du, Orhun Kara, Ting Liu,
Krishna M. Sivalingam, Dominik Ślęzak, Takashi Washio, Xiaokang Yang,
and Junsong Yuan

Editorial Board Members

Simone Diniz Junqueira Barbosa 

*Pontifical Catholic University of Rio de Janeiro (PUC-Rio),
Rio de Janeiro, Brazil*

Joaquim Filipe 

Polytechnic Institute of Setúbal, Setúbal, Portugal

Ashish Ghosh

Indian Statistical Institute, Kolkata, India

Igor Kotenko 

*St. Petersburg Institute for Informatics and Automation of the Russian
Academy of Sciences, St. Petersburg, Russia*

Lizhu Zhou


Tsinghua University, Beijing, China

More information about this series at <http://www.springer.com/series/7899>

Huansheng Ning (Ed.)

Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health

International 2019 Cyberspace Congress, CyberDI and CyberLife
Beijing, China, December 16–18, 2019
Proceedings, Part I

Editor
Huansheng Ning 
University of Science and Technology
Beijing, China

ISSN 1865-0929 ISSN 1865-0937 (electronic)
Communications in Computer and Information Science
ISBN 978-981-15-1921-5 ISBN 978-981-15-1922-2 (eBook)
<https://doi.org/10.1007/978-981-15-1922-2>

© Springer Nature Singapore Pte Ltd. 2019, corrected publication 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd. The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

This volume contains the papers from the 2019 Cyberspace Congress which includes the International Conference on Cyberspace Data and Intelligence (CyberDI 2019) and the International Conference on Cyber-Living, Cyber-Syndrome, and Cyber-Health (CyberLife 2019) held in Beijing, China, during December 16–18, 2019.

The explosion of smart IoT and artificial intelligence has driven cyberspace entering into a new prosperous stage, and cyberspace in turn cultivates novel and interesting domains such as cyberspace data and intelligence, cyber-living, and cyber-life. Therefore, CyberDI 2019 and CyberLife 2019 were organized to explore cutting-edge advances and technologies pertaining to the key issues of data and intelligence, cyber syndrome, and health in cyberspace. The aim of the conference was to bring together researchers, scientists, as well as scholars and engineers from all over the world to exchange brilliant ideas, and the invited keynote talks and oral paper presentations contributed greatly to broadening horizons and igniting young minds.

Generally speaking, cyberspace attracts more and more attention serving as an emerging and significantly profound research area. However, some challenges still exist in the comprehensive understanding of basic theories, philosophy, and science. In CyberDI 2019 and CyberLife 2019, there were four main topics which the papers addressed, and the authors focused on the advanced theories, concepts, and technologies relating to data and intelligence, cyber-syndrome, and cyber-living in order to fully mine and dig out the hidden values in cyberspace.

CyberDI 2019 discussed intelligent ways of making full use of data and information, which are regarded as the foundation and core of cyberspace. It focused on data communication and computing, as well as knowledge management with different intelligent algorithms such as deep learning, neural networks, knowledge graphs, etc.

CyberLife 2019 focused on health challenges faced in existing cyberspace, and provided an interactive platform for exploring cyber-syndrome, cyber-diagnosis, as well as the way to healthy living in cyberspace.

In order to ensure the high quality of both conferences, we followed a rigorous review process in CyberDI 2019 and CyberLife 2019. CyberDI 2019 and CyberLife 2019 received 160 qualified submissions, and nearly 64 regular papers and 18 posters were accepted. All manuscripts were reviewed by peer-reviewers in a single-blind review process, and each paper had three reviewers on average chosen by the Program Committee members considering their qualifications and experience.

The proceeding editors wish to thank the dedicated Conference Committee members and all the other reviewers for their contributions. Sincerely, we hope that these proceedings will help a lot for interested readers, and we also thank Springer for their trust and support in publishing the proceeding of CyberDI 2019 and CyberLife 2019.

Organization

CyberDI 2019

Scientific Committee

Rongxing Lu	University of New Brunswick, Canada
J. Christopher Westland	University of Illinois – Chicago, USA
Cuneyt Gurcan Akcora	University of Texas at Dallas, USA
Fu Chen	Central University of Finance and Economics, China
Giancarlo Fortino	University of Calabria, Italy
Guangjie Han	Hohai University, China
Richard Hill	University of Huddersfield, UK
Farhan Ahmad	University of Derby, UK
Jin Guo	University of Science and Technology Beijing, China
Octavio Loyola-González	Tecnologico de Monterrey, Mexico
Constantinos Patsakis	University of Piraeus, Greece
Lianyong Qi	Qufu Normal University, China
Tie Qiu	Tianjin University, China
Xiang Wang	Beihang University, China
Qi Zhang	IBM T J Watson, USA
Chunsheng Zhu	Southern University of Science and Technology, China
Asma Adnane	Loughborough University, UK
Humaira Ashraf	International Islamic University Islamabad, Pakistan
James Bailey	The University of Melbourne, Australia
Ari Barrera-Animas	Tecnologico de Monterrey, Mexico
Winnie Bello	University of Huddersfield, UK
Milton Garcia Borroto	Instituto Superior Politécnico José Antonio Echeverría, Cuba
Fatih Kurugollu	University of Derby, UK
Manuel Lazo	Tecnologico de Atizapan, Mexico
Satya Shah	University of Bolton, UK
Yong Xue	University of Derby, UK
Danilo Valdes Ramirez	Tecnologico de Monterrey, Mexico
Ahmad Waqas	Beijing Normal University, China
Reza Montasari	University of Huddersfield, UK
Majdi Mafarja	Birzeit University, Palestine
Abdelkarim Ben Sada	University of Science and Technology Beijing, China
Mohammed Amine Bouras	University of Science and Technology Beijing, China
Lázaro Bustio-Martínez	National Institute of Astrophysics, Optics and Electronics, Mexico
Yaile Caballero	Universidad de Camaguey, Cuba

Barbara Cervantes	Tecnologico de Monterrey, Mexico
Leonardo Chang	Tecnologico de Monterrey, Mexico
Rania El-Gazzar	University South-Eastern, Norway
Hugo Escalante	National Institute of Astrophysics, Optics and Electronics, Mexico
Fadi Farha	University of Science and Technology Beijing, China
Virginia Franqueira	University of Kent, UK
Luciano García	Tecnologico de Monterrey, Mexico
Mario Graff	CONACYT Researcher – INFOTEC, Mexico
Andres Gutierrez	Tecnologico de Monterrey, Mexico
Raudel Hernández-León	Advanced Technologies Application Center, Cuba
Amin Hosseinian-Far	University of Northampton, UK
Rasheed Hussain	Innopolis University, Russia
Chaker Abdelaziz Kerrache	University of Ghardaia, Algeria
Mehmet Kiraz	De Montfort University, UK
Fatih Kurugollu	University of Derby, UK
Noureddine Lakouari	Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE), Mexico
Ismael Lin	Tecnologico de Monterrey, Mexico
Adrian Lopez	CIMAT, Mexico
Arun Malik	Lovely Professional University, UK
Diana Martín	CUJAE, Cuba
Safdar Nawaz Khan Marwat	University of Engineering & Technology, Peshawar, Pakistan
Arquimides Mendez Molina	Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE), Mexico
Senthilkumar Mohan	VIT University, India
Raúl Monroy	Tecnologico de Monterrey, Mexico
Abdenacer Naouri	University of Science Technology Beijing, China
Alberto Oliart	Tecnologico de Monterrey, Mexico
Felipe Orihuela-Espina	INAOE, Mexico
Nisha Panwar	University of California, Irvine, USA
Simon Parkinson	University of Huddersfield, UK
Luis Pellegrin	Universidad Autónoma de Baja California (UABC), Mexico
Airel Perez	CENATAV, Cuba
Claudia Pérez	Tecnologico de Monterrey, Mexico
Julio César Pérez Sansalvador	INAOE - Cátedra CONACyT, Mexico
Laura Pinilla-Buitrago	Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE), Mexico
Muthu Ramachandran	Leeds Beckett University, UK
Kelsey Ramírez Gutiérrez	Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE), Mexico
Praveen Kumar Reddy Maddikunta	Vellore, Tamil Nadu, Mexico

Jorge Rodriguez	Tecnologico de Monterrey, Mexico
Cosme Santiesteban-Toca	Centro de Bioplantitas, Cuba
Dharmendra Shadija	Sheffield Hallam University, UK
Nasir Shahzad	University of Leicester, UK

Organizing Committee

Kim-Kwang Raymond Choo	The University of Texas at San Antonio, USA
Ravi Sandhu	University of Texas at San Antonio, USA
Weishan Zhang	China University of Petroleum, China
ZhangBing Zhou	China University of Geosciences (Beijing), China
Huansheng Ning	University of Science and Technology Beijing, China
Qinghua Lu	CSIRO, Australia
Shaohua Wan	Zhongnan University of Economics and Law, China
Bradley Glisson	Sam Houston State University, USA
Haijing Hao	Bentley University, USA
Pengfei Hu	China Mobile Research Institute, China
Miguel Angel Medina Perez	Tecnologico de Monterrey, Mexico
Ata Ullah	National University of Modern Languages, Pakistan
Liming Chen	De Montfort University, UK
Mahmoud Daneshmand	Stevens Institute of Technology, USA
Keping Long	University of Science and Technology Beijing, China
Chunming Rong	University of Stavanger, Norway
Chonggang Wang	InterDigital, USA

CyberLife 2019

Scientific Committee

Mariwan Ahmad	IBM, UK
Karim Mualla	University of Leicester, UK
Yudong Zhang	University of Leicester, UK
Muhammad Ajmal Azad	University of Derby, UK
Hussain Al-Aqrabi	University of Huddersfield, UK
Junaid Arshad	University of West London, UK
Liangxiu Han	Manchester Metropolitan University, UK
Yong Hu	The University of Hong Kong, China
Chenxi Huang	Nanyang Technological University, Singapore
Jianxin Li	Beihang University, China
Liyang Wang	Nanjing Normal University, China
Kaijian Xia	China University of Mining and Technology; Changshu No. 1 People' Hospital, China
Likun Xia	Capital Normal University, China
Xiaojun Zhai	University of Essex, UK
Meifang Zhang	University of Science and Technology Beijing, China

Rongbo Zhu	South Central University for Nationalities, China
Nasser Alaraje	Michigan Technological University, USA
Abbes Amira	De Montfort University, UK
Kofi Appiah	Nottingham Trent University, UK
Hamza Djelouat	University of Oulu, Finland
Klaus D. McDonald-Maier	University of Essex, UK
Yanghong Tan	Hunan University, China
Bin Ye	Queens University of Belfast, UK
Wangyang Yu	Shaanxi Normal University, P.R. China
Bo Yuan	University of Derby & Data Science Research Center of University of Derby, UK
Yongjun Zheng	University of West London, UK
Zhifeng Zhong	Hubei University, China
Xingzhen Bai	Tongji University, P.R. China
Kieren Egan	Department of Computer and Information Sciences, University of Strathclyde Glasgow, UK
Preetha Phillips	West Virginia School of Osteopathic Medicine, USA
Pengjiang Qian	Jiangnan University, China
Junding Sun	Henan Polytechnic University, China
Xiaosong Yang	National Center for Computer Animation, Bournemouth University, UK
Maher Assaad	College of Engineering, Ajman University, United Arab Emirates
Yuan Yuan Chen	Beijing Fistar Technology Co., Ltd., China
Ming Ma	School of Medicine, University of Stanford, USA
Wajid Mumtaz	Department of Computer Science, Faculty of Applied Sciences, University of West Bohemia, Czech Republic
Li Tan	School of Computer and Information Engineering, Beijing Technology and Business University, China
Kedi Xu	Qiushi Academy for Advanced Studies, Zhejiang University, China
Susu Yao	Institute for Infocomm Research, A*STAR, Singapore
Da Zhang	College of Information Engineering, Capital Normal University, China
Shaomin Zhang	Qiushi Academy for Advanced Studies, Zhejiang University, China
Yizhang Jiang	Jiangnan University, China
Jin Yong	Changshu Institute of Technology, China
Vishnu Varthanan Govindaraj	Kalasalingam Academy of Research and Education, India
Li Yuexin	Hubei University, China
Shan Zhong	Changshu Institute of Technology, China
Haider Ali	University of Derby, UK
Nyothiri Aung	University of Science and Technology Beijing, China
Ra'ed Bani Abdelrahman	Loughborough University, UK

Luis Castro	Instituto Tecnológico de Sonora, Mexico
Yuanyuan Chen	Beijing Fistar Technology Co., Ltd., China
Federico Cruciani	Ulster University, UK
Shoaib Ehsan	University of Essex, UK
Mark Fox	University of Toronto, Canada
James Hardy	University of Derby, UK
Anju Johnson	University of Huddersfield, UK
Junhua Li	University of Essex, UK
Wenjia Li	New York Institute of Technology, USA
Zhi Li	Guangxi Normal University, China
Feng Mao	Walmart Labs, USA
Fanlin Meng	University of Essex, UK
Kun Niu	University of Posts and Communications, China
Doris Oesterreicher	University of Natural Resources and Life Sciences, Vienna, Austria
John Panneerselvam	University of Derby, UK
Sangeet Saha	University of Essex, UK
Minglai Shao	Beihang University, China
Dhiraj Srivastava	Indian Institute of Technology, India
Jinya Su	Loughborough University, UK
Peipei Sui	Shandong Normal University, China
Shuai Zhang	Ulster University, UK

Organizing Committee

Liming Chen	De Montfort University, UK
Huansheng Ning	University of Science and Technology Beijing, China
Chunming Rong	University of Stavanger, Norway
Chonggang Wang	InterDigital, USA
Changjun Jiang	Donghua University, China
Lu Liu	University of Leicester, UK
Faycal Bensaali	Qatar University, Qatar
Zhengchao Dong	Columbia University, USA
Colin Johnson	University of Kent, UK
Tan Jen Hong	National University of Singapore, Singapore
Rusdi Abd Rashid	University of Malaya Center for Addiction Sciences (UMCAS), Malaysia
Wenbing Zhao	Cleveland State University, USA
John Panneerselvam	University of Derby, UK
Po Yang	University of Sheffield, UK

Local Committee for CyberDI 2019 and CyberLife 2019

Huansheng Ning	University of Science and Technology Beijing, China
Rui Wang	University of Science and Technology Beijing, China
Bing Du	University of Science and Technology Beijing, China
Sahraoui Dhelim	University of Science and Technology Beijing, China
Qingjuan Li	University of Science and Technology Beijing, China
Feifei Shi	University of Science and Technology Beijing, China
Zhong Zhen	University of Science and Technology Beijing, China
Xiaozhen Ye	University of Science and Technology Beijing, China
Dawei Wei	University of Science and Technology Beijing, China
Yang Xu	University of Science and Technology Beijing, China

Contents – Part I

CyberDI 2019: Cyber Data, Information and Knowledge

Automatic Analysis and Reasoning Based on Vulnerability Knowledge Graph	3
<i>Shengzhi Qin and K. P. Chow</i>	
Application of Principal Component Analysis for Assessment the Behavior of Knowledge Management	20
<i>Na Ran</i>	
Information Extraction and Similarity Computation for Semi-/Un-Structured Sentences from the Cyberdata	38
<i>Peiying Zhang, Xingzhe Huang, Lei Zhang, and Weishan Zhang</i>	
An Approach for Semantic Web Discovery Using Unsupervised Learning Algorithms	56
<i>Yan Shen and Fangfang Liu</i>	
Direction-Aware Top- k Dominating Query	73
<i>Xue Miao, Xi Guo, Aziguli Wulamu, and Zhaoshun Wang</i>	
A Personalized Collaborative Filtering Recommendation System of Network Document Resource Based on Knowledge Graph.	94
<i>Yuezhong Wu, Rongrong Chen, Changyun Li, and Shuhong Chen</i>	
Short Text Representation Model Construction Method Based on Novel Semantic Aggregation Technology	107
<i>Dong Yi, Zhai Jia, Li Xin, and Chen Feng</i>	
FLSTM: Feature Pattern-Based LSTM for Imbalanced Big Data Analysis . . .	119
<i>Liang Xu, Xingjie Zeng, Weishan Zhang, Jiangru Yuan, Pengcheng Ren, Ruicong Zhang, Wuwu Guo, and Jiehan Zhou</i>	
A Construction Method of Author Influence Map Based on Data Field Theory and Entropy Weight Method	130
<i>Jie Yu, Dongdong Wang, Lingyu Xu, and Rongrong Chen</i>	
Online Public Opinion Deduction Based on an Innovative Cellular Automata	141
<i>Xin Liu, Shuai Cao, Yang Cao, Jie He, Weishan Zhang, Xueli Wang, and Liang Zheng</i>	

Discretionary Access Control Method to Protect Blockchain Privacy 161
Jie Yang, Min-Sheng Tan, and Lin Ding

Secure Healthcare Data Aggregation Scheme for Internet of Things. 175
Muhammad Azeem and Ata Ullah

A Multi-location Defence Scheme Against SSDP Reflection Attacks
in the Internet of Things 187
*Xin Liu, Liang Zheng, Shuai Cao, Sumi Helal, Jiehan Zhou, Hunfu Jia,
and Weishan Zhang*

Remote Data Authentication Scheme Based Balance Binary
Sort Merkle Hash Tree 199
*Mengyu Shen, Meiliang Liu, Yang Li, Delgerbat Batbayar,
and Xuanxia Yao*

An Efficient Hybrid Encryption Scheme for Large Genomic Data Files 214
Yatong Jiang, Tao Shang, Jianwei Liu, Zongfu Cao, and Yunxiao Geng

Sentiment Analysis of Text Classification Algorithms
Using Confusion Matrix. 231
Babacar Gaye and Aziguli Wulamu

On the Constructions of Bigraphical Categories 242
Dong Xu and Xiaojun Li

A Distributed Data Collection System for Traffic Images 249
*Wen Bo, Hongju Yang, Jiaojiao Xiao, Liangyan Li,
and Changyou Zhang*

CyberDI 2019: Cyber and Cyber-Enabled Intelligence

Robot Path Planning in Dynamic Environments Based on Deep
Reinforcement Learning. 265
Yu Han, Yu Guo, Zhenqiang Mi, and Yang Yang

A Way to Understand the Features of Deep Neural Networks
by Network Inversion 284
Hong Wang, Xianzhong Chen, and Jiangyun Li

Detection of Weak Defects in Weld Joints Based on Poisson
Fusion and Deep Learning 296
*Xinli Chen, Hongbing Wang, Li Li, Jingyi Liu, Shuqi Wei, Haihua Li,
and Jinxin Lv*

CARNet: Densely Connected Capsules with Capsule-Wise Attention Routing	309
<i>Zhi-Xuan Yu, Ye He, Chao Zhu, Shu Tian, and Xu-Cheng Yin</i>	
A Malware Identification and Detection Method Using Mixture Correntropy-Based Deep Neural Network.	321
<i>Xiong Luo, Jianyuan Li, Weiping Wang, Yang Gao, and Wenbing Zhao</i>	
An Improved Algorithm for Recruitment Text Categorization	335
<i>Hui Zhao, Xin Liu, Wenjie Guo, Keke Gai, and Ying Wang</i>	
Seizure Prediction Using Bidirectional LSTM.	349
<i>Hazrat Ali, Feroz Karim, Junaid Javed Qureshi, Adnan Omer Abuassba, and Mohammad Farhad Bulbul</i>	
Hybrid Machine Learning Models of Classifying Residential Requests for Smart Dispatching	357
<i>Tianen Chen, Jincheng Sun, Hongyi Lin, and Yan Liu</i>	
Data Driven Faster R-CNN for Transmission Line Object Detection	379
<i>Xin Zhou, Bin Fang, Jiye Qian, Gangwen Xie, Bangfei Deng, and Jide Qian</i>	
A Deep Learning-Based Hybrid Data Fusion Method for Object Recognition.	390
<i>Weishan Zhang, Zongchao Zheng, Yuanjie Zhang, Liang Xu, and Jiehan Zhou</i>	
Feature Fusion Detection Network for Multi-scale Object Detection	403
<i>Weishan Zhang, Xia Liu, Liang Xu, Zhaotong Li, Hongwei Zhao, and Jiehan Zhou</i>	
Post Profiles Research Based on Electric Power Major	413
<i>Wei Dai, Tao Xu, Jun Zhao, Rong Sun, Xin-dong Zhao, Yueran Wen, Hongfei Yuan, Shangxiu Song, and Haoyu Zong</i>	
Safety Analysis of Communication-Based Train Control System by STPA and Colored Petri Net	433
<i>Qian Xu and Juntong Lin</i>	
Location and Fusion Algorithm of High-Rise Building Rescue Drill Scene Based on Binocular Vision	450
<i>Jia Ma and Zhiguo Shi</i>	
Wear Debris Classification and Quantity and Size Calculation Using Convolutional Neural Network	470
<i>Hongbing Wang, Fei Yuan, Liyuan Gao, Rong Huang, and Weishen Wang</i>	

ArcGIS Services Recommendation Based on Semantic and Heuristic Optimization Algorithm	487
<i>Jiaqi Zheng, Jin Diao, Zhangbing Zhou, and Yongli Xing</i>	
Designing Public Digital Cultural Service Interactive System Based on Reality-Based Interaction Principles	502
<i>Jinhua Dou</i>	
Modeling and Verification of Resource-Oriented Internet of Things Services with Context Constraints	518
<i>Lei Yu, Yang Lu, BenHong Zhang, Ya Li, FangLiang Huang, YuLian Shen, and TongPing Shen</i>	
Sc-Ge: Multi-Factor Personalized Point-of-Interest Recommendation Model	534
<i>Wen Hu and Yuhai Jing</i>	
RFT: An Industrial Data Classification Method Based on Random Forest	547
<i>Caiyun Liu, Xuehong Chen, Yan Sun, Shuai Feng Yang, and Jun Li</i>	
A New Non-smart Water Meter Digital Region Localization and Digital Character Segmentation Method	557
<i>Fei Lei, Zhimei Xiong, and Xueli Wang</i>	
Fault Prediction for Software System in Industrial Internet: A Deep Learning Algorithm via Effective Dimension Reduction	572
<i>Siqi Yang, Shuai Feng Yang, Zigang Fang, Xiuzhi Yu, Lanlan Rui, and Yucheng Ma</i>	
An Improved NSGA-II Algorithm and Its Application	581
<i>Xiaofei Zhang, Zhiqiu Liu, Chao Wang, and Yalin Shang</i>	
Correction to: Wear Debris Classification and Quantity and Size Calculation Using Convolutional Neural Network	C1
<i>Hongbing Wang, Fei Yuan, Liyuan Gao, Rong Huang, and Weishen Wang</i>	
Author Index	595

Contents – Part II

Communication and Computing

A Markov Approximation Algorithm for Computation Offloading and Resource Scheduling in Mobile Edge Computing	3
<i>Haowei Chen, Mengran Liu, Yunpeng Wang, Weiwei Fang, and Yi Ding</i>	
A Geographic Routing Protocol Based on Trunk Line in VANETs	21
<i>Di Wu, Huan Li, Xiang Li, and Jianlong Zhang</i>	
Sub-array Based Antenna Selection Scheme for Massive MIMO in 5G	38
<i>Hassan Azeem, Liping Du, Ata Ullah, Muhammad Arif Mughal, Muhammad Muzamil Aslam, and Muhammad Ikram</i>	
A Green SWIPT Enhanced Cell-Free Massive MIMO System for IoT Networks	51
<i>Meng Wang, Haixia Zhang, Leiyu Wang, and Guannan Dong</i>	
Non-orthogonal Multiple Access in Coordinated LEO Satellite Networks	65
<i>Tian Li, Xuekun Hao, Guoyan Li, Hui Li, and Xinwei Yue</i>	
Multi-sensor Data Fusion Based on Weighted Credibility Interval	79
<i>Jihua Ye, Shengjun Xue, and Aiwen Jiang</i>	
A Locality Sensitive Hashing Based Collaborative Service Offloading Method in Cloud-Edge Computing	92
<i>Wenmin Lin, Xiaolong Xu, Qihe Huang, Fei Dai, Lianyong Qi, and Weimin Li</i>	
A Testbed for Service Testing: A Cloud Computing Based Approach	105
<i>Qinglong Dai, Jin Qian, Jianwu Li, Jun Zhao, Weiping Wang, and Xiaoxiao Liu</i>	
Improve the Efficiency of Maintenance for Optical Communication Network: The Multi-factor Risk Analysis via Edge Computing	121
<i>Yucheng Ma, Yanbin Jiao, Yongqing Liu, Hao Qin, Lanlan Rui, and Siqi Yang</i>	
Edge Computing for Intelligent Transportation System: A Review	130
<i>Qian Li, Pan Chen, and Rui Wang</i>	

Consensus Performance of Traffic Management System for Cognitive Radio Network: An Agent Control Approach	138
<i>Muhammad Muzamil Aslam, Liping Du, Zahoor Ahmed, Hassan Azeem, and Muhammad Ikram</i>	
CyberLife 2019: Cyber Philosophy, Cyberlogic and Cyber Science	
An Efficient Concurrent System Networking Protocol Specification and Verification Using Linear Temporal Logic	149
<i>Ra'ed Bani Abdelrahman, Hussain Al-Aqrabi, and Richard Hill</i>	
Performance Evaluation of Multiparty Authentication in 5G IIoT Environments	169
<i>Hussain Al-Aqrabi, Phil Lane, and Richard Hill</i>	
PAM: An Efficient Hybrid Dimension Reduction Algorithm for High-Dimensional Bayesian Network	185
<i>Huiran Yan and Rui Wang</i>	
Indoor Activity Recognition by Using Recurrent Neural Networks	205
<i>Yu Zhao, Qingjuan Li, Fadi Farha, Tao Zhu, Liming Chen, and Huansheng Ning</i>	
Petal-Image Based Flower Classification via GLCM and RBF-SVM	216
<i>Zhihai Lu and Siyuan Lu</i>	
A Convolutional Neural Network-Based Semantic Clustering Method for ALS Point Clouds	228
<i>Zezhou Li, Tianran Tan, Yizhe Yuan, and Changqing Yin</i>	
Aligning Point Clouds with an Effective Local Feature Descriptor.	241
<i>Xialing Feng, Tianran Tan, Yizhe Yuan, and Changqing Yin</i>	
A Tutorial and Survey on Fault Knowledge Graph	256
<i>XiuQing Wang and ShunKun Yang</i>	
An Attention-Based User Profiling Model by Leveraging Multi-modal Social Media Contents	272
<i>Zhimin Li, Bin Guo, Yueqi Sun, Zhu Wang, Liang Wang, and Zhiwen Yu</i>	
Face Anti-spoofing Algorithm Based on Depth Feature Fusion	285
<i>Jingying Sun and Zhiguo Shi</i>	
Facial Micro-expression Recognition Using Enhanced Temporal Feature-Wise Model	301
<i>Ruicong Zhi, Mengyi Liu, Hairui Xu, and Ming Wan</i>	

Dynamic Facial Feature Learning by Deep Evolutionary Neural Networks . . . <i>Ruicong Zhi, Caixia Zhou, and Tingting Li</i>	312
Baseball Pitch Type Recognition Based on Broadcast Videos <i>Reed Chen, Dylan Siegler, Michael Fasko Jr., Shunkun Yang, Xiong Luo, and Wenbing Zhao</i>	328
Semi-automated Development of a Dataset for Baseball Pitch Type Recognition <i>Dylan Siegler, Reed Chen, Michael Fasko Jr., Shunkun Yang, Xiong Luo, and Wenbing Zhao</i>	345
Ford Vehicle Classification Based on Extreme Learning Machine Optimized by Bat Algorithm <i>Yile Zhao and Zhihai Lu</i>	360
Design and Implementation of a Wearable System for Information Monitoring <i>Qi Zhao and Tongtong Zhai</i>	371
A Review of Internet of Things Major Education in China. <i>Yuke Chai, Wei Huangfu, Huansheng Ning, and Dongmei Zhao</i>	389
CyberLife 2019: Cyber Health and Smart Healthcare	
Research on the Influence of Internet Use on Adolescents’ Self <i>Huimei Cao and Jiansheng Li</i>	407
Breast Cancer Risk Assessment Model Based on si-SDAE. <i>Xueni Li and Zhiguo Shi</i>	417
Prediction Model of Scoliosis Progression Bases on Deep Learning. <i>Xiaoyong Guo, Suxia Xu, Yizhong Wang, Jason Pui Yin Cheung, and Yong Hu</i>	431
A Hybrid Intelligent Framework for Thyroid Diagnosis <i>Zhuang Li, Jingyan Qin, Xiaotong Zhang, and Yadong Wan</i>	441
Geriatric Disease Reasoning Based on Knowledge Graph. <i>Shaobin Feng, Huansheng Ning, Shunkun Yang, and Dongmei Zhao</i>	452
Image Analysis Based System for Assessing Malaria. <i>Kyle Manning, Xiaojun Zhai, and Wangyang Yu</i>	466
Research in Breast Cancer Imaging Diagnosis Based on Regularized LightGBM <i>Chun Yang and Zhiguo Shi</i>	487

Segmentation-Assisted Diagnosis of Pulmonary Nodule Recognition Based on Adaptive Particle Swarm Image Algorithm 504
Yixin Wang, Jinshun Ding, Weiqing Fang, and Jian Cao

Auxiliary Recognition of Alzheimer’s Disease Based on Gaussian Probability Brain Image Segmentation Model 513
Xinlei Chen, Dongming Zhao, and Wei Zhong

Sleep Stage Classification Based on Heart Rate Variability and Cardiopulmonary Coupling. 521
Wangqilin Zhao, Xinghao Wu, and Wendong Xiao

sEMG-Based Fatigue Detection for Mobile Phone Users 528
Li Nie, Xiaozhen Ye, Shunkun Yang, and Huansheng Ning

Research on the Effect of Video Games on College Students’ Concentration of Attention 542
Zhixin Zhu and Jiansheng Li

Study on Cardiovascular Disease Screening Model Based-Ear Fold Crease Image Recognition 550
Xiaowei Zhong

Author Index 557

CyberDI 2019: Cyber Data, Information and Knowledge



Automatic Analysis and Reasoning Based on Vulnerability Knowledge Graph

Shengzhi Qin^(✉) and K. P. Chow

The University of Hong Kong, Hong Kong, China
{szqin, chow}@cs.hku.hk

Abstract. In the security community, it is valuable to extract and store the vulnerability knowledge. Many data sources record vulnerability in unstructured data and semi-structured data which are hard for machine-understanding and reuse. Security expert need to analyze the description, link to related knowledge and reason out the hidden connection among various weakness. It is necessary to analyze the vulnerability data automatically and manage knowledge in a more intelligent method. In this paper, we propose a model for automatic analysis and reasoning based on the vulnerability knowledge graph. The vulnerability knowledge graph is extracted from several widely used vulnerability databases and stored in the graph database. Natural language processing technique is used to process and analyze the latest vulnerability description. The extracted entity will be linked to the vulnerability knowledge graph and added as new knowledge. Reasoning function can find hidden relationships among weaknesses based on the knowledge graph. Finally, we present sample cases to demonstrate the practical usage of the model.

Keywords: Cybersecurity · Knowledge graph · Vulnerability · Knowledge graph reasoning · Knowledge extraction

1 Introduction

With the development and popularity of the Internet, a variety of software and products have been developed. People are increasingly relying on the Internet and these products. Although this does bring convenience to people's lives, network security issues follow. Attacks and exploits against cybersecurity vulnerabilities have also developed rapidly in recent years, and the security of the Internet is facing challenges. For cybersecurity community, obtaining and managing a large amount of high-quality vulnerability data is very valuable, which provides a reference for checking the system for known vulnerabilities.

There are many widely used vulnerability datasets and collection platforms, one of the best known is National Vulnerability Database (NVD) [1]. NVD is a vulnerability management data repository used by U.S. government. NVD is not a separate data set. Instead, NVD links a series of vulnerability-related data sets including Common Vulnerabilities and Exposures (CVE) [2], Common Weakness Enumeration (CWE) [3], Common Vulnerability Scoring System (CVSS) [4] and Common Platform Enumeration (CPE) [5]. NVD manages a large amount of security-related information

as a high-quality vulnerability database and provides the JavaScript Object Notation (JSON) feed for public reference.

The high-quality data from NVD is produced by security expert: after collecting vulnerability data from CVE, the expert will analyze the vulnerabilities described in natural language, and then connect the specific CVE to the other dataset like CPE, CVSS, CWE. However, as the number of vulnerabilities increases, the workload of security expert grows rapidly. In addition, there are many other data sources that use natural language to describe vulnerabilities such as blogs, security news, and cyber threat intelligence subscribed by email. They also need to be automatically analyzed.

In order to realize automatically analyzing and reasoning vulnerability, we proposed the Automatic Analysis and Reasoning Vulnerability (AARV) model. This model has three key components which are natural language processing (NLP) part, vulnerability knowledge graph (VulKG) and Reasoning function.

The purpose of NLP is using computers to process, understand human language. The main task of natural language processing includes Part-of-speech tagging, Information extraction, and Named Entity Recognition (NER). The unstructured data such as text data can be processed by NLP tools and get the key information out of the sentences.

As mentioned earlier, many vulnerability data sources including CVE are unstructured data. Unstructured data is described by natural language in text form. The NLP technique can process the source data and do the NER task. With the use of NLP, the AARV model can automatically analyze and extract named entity from the vulnerability description.

In order to manage vulnerability data in a more intelligent way, we use knowledge graph and try to store the data as knowledge. Knowledge graph can link the data from different sources together, which is what NVD does to other vulnerability-related databases. With knowledge graph, the AARV model can manage the vulnerability data from the graph perspective and support reasoning function.

More specific, the VulKG stores the entities and relationships in Resource Description Framework (RDF). For one specific vulnerability, VulKG will store the weakness objects, the attack properties and product objects. These objects are connected by relationships which are defined in the VulKG ontology.

The relationship links the entities and contains hidden information which can be revealed by reasoning. Knowledge graph-based reasoning is a function that can do reasoning according to the knowledge in VulKG. This technique can help to mine some hidden rules in the VulKG, which is hard for traditional databases to do so.

The combination of these parts forms the AARV model. We can use the AARV model as a knowledge base and do many complicated queries. In this paper, we discuss each key component and give a sample case of this model. Our contributions in this paper are as follows:

1. Propose a state-of-the-art model for automatic vulnerability analysis.
2. Develop the VulKG based on VulKG ontology.
3. Extract knowledge from vulnerability description.
4. Reason out weakness chain based on VulKG.

The rest of the paper is organized as follows: Sect. 2 shows some related research in automatic analysis and reasoning in vulnerability domain. Section 3 introduces the AARV model in detail. Section 4 presents a sample case to show how does the model work. Finally, Sect. 5 draws the conclusions and outlines the possible future research direction.

2 Related Work

In order to realize automatic analysis and reasoning based on vulnerability knowledge graph, the AARV model combines three parts including knowledge graph development, vulnerability description analysis, and security-domain knowledge graph reasoning. Many significant works have been done in above areas.

Some researchers focus on designing the security-domain ontology for knowledge graph development. Iannacone et al. [6] develop an ontology for cybersecurity knowledge graphs. The ontology describes different security concepts which can facilitate the data integration from various data sources including CVE and NVD. The ontology is more focused on containing more concepts in cybersecurity domain. The definition related to vulnerability is not complete and detailed.

Intrusion Detection System (IDS) ontology is designed by Undercoffer et al. [7] and improved by More et al. [8] in order to be more compatible with diverse security-related data. Syed et al. [9] further develop the IDS ontology, which is valuable in describing security standards and mapping other security-domain ontologies. The VulKG ontology is inspired by above works. We adjust the structure and details of the ontology and make it more suitable for our datasets.

Some researchers develop the security domain knowledge graph from different perspective and models. Du et al. [10] propose a software vulnerability knowledge graph which focuses on integrating three different data sources including CVE, Maven and GitHub. The knowledge graph aligns the open source software component used in different datasets and makes the vulnerability recorded in CVE more usable. The difference between this knowledge graph and VulKG is the data sources. Jia et al. [11] demonstrate a framework for constructing a cybersecurity knowledge graph. They build a cybersecurity knowledge base with an ontology and use Stanford NER to extract security-related entities. But there are not too much implementation details about the security knowledge graph.

Liao et al. [12] propose a solution for fully automated Indicators of Compromise (IOC) extraction. The IOC Automatic Extractor combines NER and RE steps together and tries to extract the relationship between unstructured threat information. They claim that the performance of the solution is beyond what the state-of-the-art NLP technique and industry IOC tool can achieve. Gasmi et al. [13] present the LSTM-CRF model to do NER task in cybersecurity domain. The evaluation corpora contain vulnerability descriptions from CVE and NVD entries which is the data source of VulKG. Joshi et al. [14] utilize the CRF model combining with the DBpedia spotlight to extract entities and link entities to DBpedia. The extracted result is stored as linked data collection. Pingle et al. [21] use RelExt, a Feed-Forward Neural Network (FFNN) classifier, to

predict the relationship between the security-related named entity pairs which are converted into vectors by Word2Vec model.

There is also some progress on knowledge graph reasoning in cybersecurity domain. More et al. [8] build a knowledge base and develop reasoning logic. The reasoning logic is a set of rules predefined in knowledge base. They configure different reasoning logic rules against different cases and try to reason out risk alert. Alqahtani et al. [15] present a vulnerability analysis framework. The well-defined ontology is the core component of the framework. The reasoning function is supported by OWL which contains various relationship characteristics such as owl:sameAs. The reasoning result is used to trace vulnerabilities across knowledge boundaries.

Narayanan et al. [16] propose a system with knowledge graph reasoning function. The core components of reasoning include OWL reasoner and predefined rules using Semantic Web Rule Language. The reasoning function could derive actionable intelligence. Han et al. [17] develop a knowledge graph embedding method for embedding CWE and CWE relationships in a low-dimensional vector space. The reasoning function attempts to predict the relationship between CWE pairs and common consequences of CWE.

In summary, there is some progress in developing security knowledge graph and some related research area including automatic analyzing security data and do reasoning task. However, most existing work is relatively independent and lacks integration. In the security reasoning part, most research use symbolic logic-based method, which is inflexible and rigid, and cannot take advantage of the large amount of data. Some reasoning research use statistic-based method, and the reasoning results is not that practical.

In our opinion, it is better to combine the idea of above parts and form a more intelligent automated analysis framework. Therefore, we propose the AARV model to realize automatic analysis and reasoning vulnerability data based on VulKG.

3 AARV Model

The idea of AARV model is using several techniques to realize automatic analysis and reasoning against vulnerability-related information. Figure 1 shows the framework of AARV Model. The core component of this model is the VulKG which stores and manages the vulnerability knowledge. The main body of the VulKG is extracted from NVD which is a high-quality semi-structured data source. The extracted knowledge is represented in RDF and stored in graph database after conversion. NLP part takes unstructured data like latest vulnerability description as input, and the output is the result of NER. The output entity will try to align with the entity in VulKG. If the VulKG does not contain the entity from NLP output, the model will identify it as a new entity and allocate the entity an URI. The relationship between entities is predefined in the VulKG ontology. The Reasoning function is based on the knowledge stored in VulKG, and try to find some hidden weakness relationships behind the knowledge.

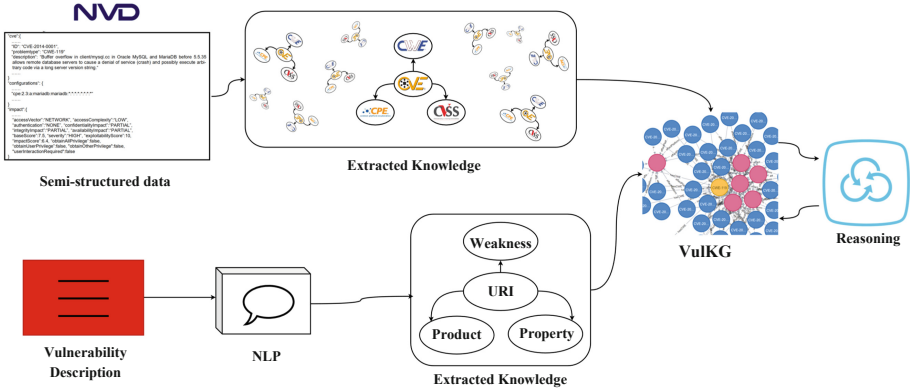


Fig. 1. Automatic analysis and reasoning vulnerability model

Section 3 contains three parts and each part shows one key component of the AARV model. The first part presents the knowledge extraction detail of semi-structured data. The second part briefly discusses the automatic analysis process using NER model. The third part introduces VulKG reasoning function shows the reasoning result.

3.1 Knowledge Extraction from Semi-structured Data

Semi-structure Data. The development of VulKG is based on several high-quality data sources. The NVD is one of the best public databases in vulnerability domain and it connects to several widely used resources including CVE, CWE, CVSS, and CPE.

The sample NVD entry is shown in Fig. 2. Each NVD entry has three parts including CVE, Configurations and Impact. CVE is a data set which record publicly known cybersecurity vulnerabilities. Each CVE item records a specific vulnerability using description and has a unique id: CVE-ID. The CVE part in NVD entry not only contains the description with CVE-ID, but also the weakness type recorded by CWE.

CWE is a category system for software weaknesses and vulnerabilities and allocates each type of weakness a CWE-ID. CWE data in NVD contains the weakness information and classify the specific CVE into a vulnerability type. Configuration field uses CPE to describe the products affected by specific CVE. CPE is a structured naming scheme for information technology systems, software, and packages based upon the generic syntax for Uniform Resource Identifiers (URI). So, CPE is very suitable to store product information as knowledge. Impact field records the CVSS information. CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. NVD uses CVSS to assess the specific CVE vulnerability. In NVD, each CVE-ID represent for a specific vulnerability and link other dataset together.

```

"cve":{
  .....
  "ID": "CVE-2014-0001",
  "problemtype": "CWE-119"
  "description": "Buffer overflow in client/mysql.cc in Oracle MySQL and MariaDB before 5.5.35
  allows remote database servers to cause a denial of service (crash) and possibly execute arbitrary
  code via a long server version string."
  .....
}
"configurations": {
  .....
  "cpe:2.3:a:mariadb:mariadb:*.:*:*:*:*:*"
  .....
}
"impact":{
  .....
  "accessVector":"NETWORK", "accessComplexity":"LOW", "authentication":"NONE",
  "confidentialityImpact":"PARTIAL", "integrityImpact":"PARTIAL", "availabilityImpact":"PARTIAL",
  "baseScore":7.5, "severity":"HIGH", "exploitabilityScore":10, "impactScore":6.4,
  "obtainAllPrivilege":false,"obtainUserPrivilege":false, "obtainOtherPrivilege":false,
  "userInteractionRequired":false
}
}

```

Fig. 2. Sample entry in NVD JSON feed data

VulKG Ontology. The relationships among different vulnerability-related concepts are predefined in VulKG ontology. The ontology is described by Web Ontology Language (OWL). The development of VulKG Ontology is inspired by Unified Cybersecurity Ontology [9] and the IDS ontology [7]. We adjusted some details to make the ontology more suitable for our data sources. For example, CPE divides products into three different types including hardware, operating system and application, which is different from the reference ontologies. The main relationship among core concepts is shown in Fig. 3.

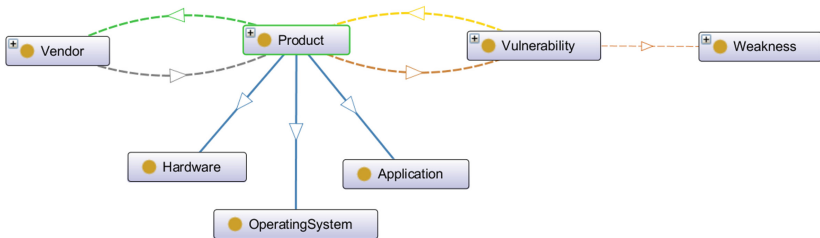


Fig. 3. Part of the VulKG ontology used for extracting VulKG

Product & Vendor. The Product class is the abstraction of all specific product objects. It can also be divided into three subclasses according to the type of product, including Hardware, Operating System and Application. The CPE objects are the instances of Product class. Each URI in CPE represents for a specific product containing detailed

information including product type, vendor, product name and version. For example, a CPE object is like this: “cpe:2.3:a:oracle:mysql:5.5.12:*:*:*:*:*”. Letter ‘a’ means that this product is an instance of the Application class. ‘Oracle’ shows the vendor information. ‘Mysql’ is the name of the product. Version data is recorded in ‘5.5.12’. There are two kinds of relationships between Product class and the Vendor class including ‘hasVendor’ and ‘hasProduct’, which are defined as the inverse relationship in OWL.

Vulnerability & Weakness. The Vulnerability class is the abstraction of all specific vulnerability object. In VulKG ontology, the CVE objects are the instances of Vulnerability class. The relationships between Vulnerability class and Product class are ‘hasVulnerability’ and ‘affectProduct’, which is a pair of inverse relationships. CVSS information is recorded in the data property of Vulnerability class.

The Weakness class is the abstraction of all specific weakness object. The CWE objects are the instance of Weakness class. In VulKG ontology, ‘hasCWE’ is the relationship from Vulnerability class to Weakness class.

Knowledge Extraction. Knowledge is extracted based on the corresponding relationship between the NVD data feed and the VulKG ontology. The extracted output is expressed by RDF. In RDF, knowledge is described as triples including subject, predicate and object. In VulKG, we use N-triples to serialize the RDF knowledge. The resources and properties in RDF are identified by URIs. The format of URIs in VulKG is designed according to the source website URIs and predefined in the VulKG ontology. For details, please refer to Fig. 4.

Figure 4 shows the extraction result from sample CVE object shown in Fig. 2. The content in Fig. 4 is separated into four parts by dotted lines. In the first part, we define several prefixes for clearer demonstration. The second part records the relationships between CVE and CWE, CVE and CPE. Third part records the CVE data properties containing CVSS data. The second and third parts are extracted from the NVD data source directly. The final part is the background knowledge which contains the links from instances to VulKG ontology and the vendor entity linking with DBpedia.

DBpedia spotlight [18] is a tool for automatically annotating mentions of DBpedia resources in text, and link unstructured data sources to the Linked Open Data cloud through DBpedia. In AARV, we use DBpedia spotlight to recognize the vendor so that we can reuse the URI about the vendor information and link our knowledge to the DBpedia. We take Arnav Joshi work [14] as reference for this part.

RDF is also a graph model and link different resources. In our implementation, we use RDF to represent extracted knowledge and use Neo4j to manage the VulKG. Neo4j is one of the most popular graph databases and support several functions including graph visualization, property graph and Select, Delete, Update, Insert operations. In Neo4j, knowledge is organized as a property graph, which is another perspective on knowledge.

```

@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix cve: <http://nvd.nist.gov/vuln/detail/> .
@prefix cwe: <http://cwe.mitre.org/data/definitions/> .
@prefix cpe: <http://nvd.nist.gov/products/cpe#> .
@prefix dbpedia: <http://dbpedia.org/resource/> .
@prefix vulontology:
<http://github.com/Brian-hku/VulKG/blob/master/VulOntology.owl#> .
.....
cve:CVE-2014-0001 vulontology:hasCWE cwe:119.
cve:CVE-2014-0001 vulontology:affectProduct
cpe:cpe:2.3:a:mariadb:mariadb:*:*:*:*:*:*.*
.....
cve:CVE-2014-0001 vulontology:hasAccessComplexity "LOW".
cve:CVE-2014-0001 vulontology:hasAccessVector "NETWORK".
cve:CVE-2014-0001 vulontology:hasAuthentication "NONE".
cve:CVE-2014-0001 vulontology:hasAvailabilityImpact "PARTIAL".
cve:CVE-2014-0001 vulontology:hasBaseScore "7.5".
cve:CVE-2014-0001 vulontology:hasConfidentialityImpact "PARTIAL".
cve:CVE-2014-0001 vulontology:hasExploitabilityScore "10".
cve:CVE-2014-0001 vulontology:hasImpactScore "6.4".
cve:CVE-2014-0001 vulontology:hasIntegrityImpact "PARTIAL".
cve:CVE-2014-0001 vulontology:hasObtainAllPrivilege "false".
cve:CVE-2014-0001 vulontology:hasObtainOtherPrivilege "false".
cve:CVE-2014-0001 vulontology:hasObtainUserPrivilege "false".
cve:CVE-2014-0001 vulontology:hasSeverity "HIGH".
cve:CVE-2014-0001 vulontology:hasUserInteractionRequired "false".
.....
cpe:cpe:2.3:a:mariadb:mariadb:*:*:*:*:*:*.* vulontology:hasVendor
dbpedia:MariaDB.
cpe:cpe:2.3:a:mariadb:mariadb:*:*:*:*:*:*.* rdf:type
dbpedia:Application_software.
dbpedia:MariaDB rdf:type vulontology:Vendor.
cve:CVE-2014-0001 rdf:type vulontology:Vulnerability.
cwe:119 rdf:type vulontology:Weakness.

```

Fig. 4. Extracted knowledge in RDF from demo CVE

3.2 Automatic Analysis Vulnerability Description Using NLP

Based on VulKG which is extracted from high-quality semi-structured knowledge base, we can perform automatic analysis on the latest vulnerability description and extract new knowledge by using NLP. In this section, we present our idea about using NER model to extract knowledge from unstructured data and integrating the recognized entities with VulKG.

The input of this process is vulnerability description in natural language, then we will perform NER against vulnerability description. The output is the entities recognized by NER. NER is mainly used to identify proper noun or special meaning phrases in the text. The commonly used NER technology mainly identifies entities like

organization, person, place or time. However, in the field of cybersecurity, the commonly used NER technology cannot meet the above task requirements.

In AARV model, the vulnerability text data set is from CVE description which is high-quality unstructured data source. According to VulKG and VulKG ontology, we create five types of entities for the NER task, including ACCESSVECTOR, AUTHENTICATION, WEAKNESS, PRODUCT and VERSION.

In the vulnerability description, the most valuable information is the weakness detail and the vulnerable product. The weakness detail can align with the weakness objects in CWE data while product name and version information can identify the CPE objects in VulKG. So, we define WEAKNESS, PRODUCT and VERSION to extract the weakness entities and product entities. There is also some information about the attack detail in description. We define ACCESSVECTOR and AUTHENTICATION to extract some of the attack detail. ACCESSVECTOR entities describe the attack vector such as ‘local user’ or ‘remote attacker’ which could be recognized by NER model. AUTHENTICATION entities record the detail about whether the attackers need authentication.

In AARV, we select BiLSTM-CRF model to do NER task in security vulnerability domain. The model selection refers to the research result proposed by Gasmi et al. [13] which is one of the most advanced methods for doing NER tasks in cybersecurity domain. The model architecture is shown in Fig. 5. As for labeling the description data, we adopt BIOES method. B represents the beginning of the entity, I represent the middle part of the entity, E represents the end of the entity, S represents the entity which is a single character, and non-entity part is represented by O.

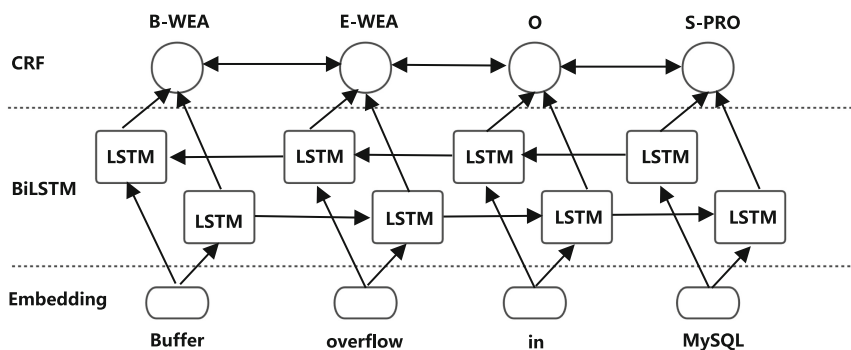


Fig. 5. BiLSTM-CRF model

After recognizing the named entity, we need to align the NER result with VulKG and VulKG ontology. The Entity-VulKG alignment relationship is shown in Table 1. Each entity type will align with corresponding property or objects in VulKG. ‘hasAccessVector’ and ‘hasAuthentication’ are properties in VulKG ontology. WEAKNESS, PRODUCT, and VERSION entities will be aligned with the objects in CWE and CPE dictionary. The alignment process detail will be shown in Sect. 4.1.

Table 1. Entity-VulKG alignment relationship

Entity type	Accessvector	Authentication	Weakness	Product&version
Align with	'hasAccessVector'	'hasAuthentication'	CWE objects	CPE objects

We also consider that NER could identify new entities. If new WEAKNESS entities are identified by NER model, we will use 'CWE-New' to match them. If the NER model identify new PRODUCT and VERSION entities, we will create new CPE objects and label it as 'new'. The naming pattern of new CPE objects refer to official naming specification [19].

The matching result will be converted into knowledge expressed by RDF in the same way as Knowledge Extraction part shown in Sect. 3.1. This process can help security experts reduce the workload, automatically label and analyze the latest vulnerability description, and align with VulKG, so that the extracted knowledge can be reused.

3.3 VulKG Reasoning

VulKG-based reasoning function focuses on mining hidden rules. We want to reason out the hidden relationship between different weakness types. In this section, we define the VulKG reasoning problem, and give the reasoning result with evaluation.

Reasoning Problem Definition. The reasoning method used in VulKG is inspired by Association Rule Mining (ARM) and try to reason out hidden rules and knowledge. Based on VulKG, we define the reasoning task: Mining hidden CWE Chain. A CWE Chain is a sequence of two or more separate weaknesses that can be closely linked together within software. One weakness, X, can directly create the conditions that are necessary to cause another weakness, Y, to enter a vulnerable condition. When this happens, CWE refers to X as "primary" to Y, and Y is "resultant" from X [20].

More specific, the statistic-based VulKG reasoning focuses on mining CWE Chain which contains two different weaknesses. The key indicator of chain mining is Chain Confidence, which is used to identify CWE Chain Candidate. Chain Confidence calculates the conditional probability of a pair of weaknesses existing together in the same product. More formally, the Chain Confidence is formally defined as:

$$\text{Chain Confidence} = C(\text{Pr with CWE1} \cap \text{Pr with CWE2})/C(\text{Pr with CWE1}) \quad (1)$$

$C(\text{Pr with CWE1})$ is the number of product Pr which has specific weakness CWE1. $C(\text{Pr with CWE1} \cap \text{Pr with CWE2})$ represents the number of product Pr which has specific weaknesses CWE1 and CWE2. In short, we will use C_1 and C_{12} to represent these two parameters.

Chain Confidence indicates the hidden relationship between weakness and the products. We calculate Chain Confidence based on data in VulKG, and set the thresholds against the indicators including C_1 , C_{12} , and Chain Confidence. If C_1 and C_{12} are too small, statistical errors will make a huge effect on Chain Confidence. So, when mining the CWE chain, products with weaknesses should be frequent. Chain

Confidence statistically reflects the strength of the relationship and should not be too small. After repetitious experiments, we set the threshold for VulKG reasoning function as C_1 (100), C_{12} (100), Chain Confidence (0.2). If the values of indicators are over the thresholds, then a CWE Chain Candidate will be identified as mining result.

The CWE Chain Candidate is not the final reasoning result and we manually validate the Chain Candidates and select the chains which we think is logically reasonable from the perspective of vulnerability analysis. More specifically, we classify the Chain Candidate with four different labels including 0, 0.5, 1, and S.

Reasoning Result and Evaluation. We calculate the indicators in VulKG which contains the vulnerability data including NVD, CVE, CPE, and CWE in 2018 and 2019. 52 CWE Chain Candidates are identified by threshold. The final result of VulKG reasoning is shown in Table 2. In Table 2, the expression of CWE Chain is CWE pair. For example, (362, 119) represents the CWE Chain $CWE-362 \rightarrow CWE-119$.

Table 2. CWE Chain Reasoning result with label

Label	CWE Chain
1	(362, 119), (362, 125), (362, 416), (362, 787), (362, 200), (362, 20), (362, 190), (125, 362), (125, 476), (125, 416), (125, 787), (125, 200), (125, 20), (125, 190), (476, 416), (476, 20), (416, 362), (416, 125), (416, 476), (416, 787), (416, 200), (400, 20), (787, 362), (787, 125), (787, 416), (787, 200), (787, 20), (787, 190), (287, 200), (287, 20), (918, 79), (20, 119), (190, 119), (190, 125), (190, 20)
0.5	(295, 20), (415, 119), (476, 200), (416, 119), (416, 20), (416, 190), (190, 416), (190, 200)
0	(77, 119), (476, 119), (476, 125), (400, 119), (287, 119), (326, 79)
S	(125, 119), (787, 119), (78, 77)

Label 1 means the Chain Candidate is commonly used to exploit vulnerabilities, or implies reasonable exploit logic. Label 0.5 means the Chain Candidate is ambiguous or not that common. Label 0 represents that the Chain Candidate has no obvious exploit logic and judge it as a fake CWE Chain. Label S means the Chain Candidate has strong relationship, but the relationship does not satisfy the definition of CWE Chain. For example, CWE-125 (Out-of-bounds Read) is subclass of CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer).

The statistical result of VulKG reasoning is shown in Table 3. We consider that CWE Chain Candidates labeled as 0.5 or 1 are the real CWE Chains, while 0 and S are fake CWE Chains. Overall, the accuracy of the reasoning function is 82.69%.

Table 3. Reasoning result evaluation

	1	0.5	0	S
Number	35	8	6	3
Ratio	67.31%	15.38%	11.54%	5.77%
Accuracy	82.69%		17.31%	

Section 4.2 will demonstrate a sample reasoning case which can show more reasoning detail including Chain Confidence calculation and validation process.

Mining CWE Chain can help security experts detect weaknesses in the system from a new perspective and provide a reference for checking composite vulnerabilities.

4 Case Study

In Sect. 4, we demonstrate several cases to display the different parts of AARV model further. Since the knowledge extraction against semi-structured data has been discussed with sample cases in Sect. 3.1, we focus on demonstrating two other parts of AARV model. The first part presents the NLP component and shows a knowledge extraction sample case from unstructured data. The second part describes the details of CWE Chain Reasoning based on VulKG.

4.1 Extract Knowledge from Unstructured Data by NLP Component

NER model can automatically analyze and process the latest vulnerability description. In this section, we present a sample case to show the workflow of the NLP component in AARV model. The sample vulnerability description is from CVE-2019-1881 which is shown in Fig. 6.

CVE-2019-1881:

A vulnerability in the web-based management interface of Cisco Industrial Network Director (IND) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on an affected device. For more information about CSRF attacks and potential mitigations, see Understanding Cross-Site Request Forgery Threat Vectors.

Fig. 6. Sample CVE vulnerability description

The first step is using NER model to process sample input description and try to recognize the entities. The recognized entity would be one of the five types including ACCESSVECTOR, AUTHENTICATION, WEAKNESS, PRODUCT and VERSION.

The result of NER processing sample CVE is shown in Fig. 7. In this case, NER model recognize four types of entities. VERSION entities are not recognized because there is no version information in sample vulnerability description.

The second step is aligning the recognized entities with VulKG. ‘Cisco Industrial Network Director’ is recognized as PRODUCT entity and we match it with the CPE dictionary. The matching result is the CPE object: ‘cpe:2.3:a:cisco:industrial_network_director:1.6.0:*:*:*:*:*:*’. In this sample case, the matching process is successful. If there is no CPE object that can match with recognized entities, we will create a new object following the naming specification.

```

CVE-2019-1881:
PRODUCT: ['Cisco Industrial Network Director']
AUTHENTICATION: ['Unauthenticated']
ACCESSVECTOR: ['remote attacker']
WEAKNESS: ['cross-site request forgery', 'CSRF', 'CSRF', 'CSRF', 'Cross-Site Request Forgery']
VERSION: []

```

Fig. 7. NER result of sample CVE

The identified ‘Unauthenticated’ is an AUTHENTICATION entity, which corresponds to ‘hasAuthentication’ property in VulKG ontology. ‘remote attacker’ is identified as an ACCESSVECTOR entity, which corresponds to ‘hasAccessVector’ property in VulKG ontology.

In the result list of WEAKNESS entity, five entities are identified. The entities will match with the CWE data and the result is CWE-352 [Cross-Site Request Forgery (CSRF)]. The final alignment output is shown in Fig. 8.

```

@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix cve: <http://nvd.nist.gov/vuln/detail/> .
@prefix cwe: <http://cwe.mitre.org/data/definitions/> .
@prefix cpe: <http://nvd.nist.gov/products/cpe#> .
@prefix dbpedia: <http://dbpedia.org/resource/> .
@prefix vulontology:
<http://github.com/Brian-hku/VulKG/blob/master/VulOntology.owl#> .

cve:CVE-2019-1881 vulontology:hasCWE cwe:352.
cve:CVE-2019-1881 vulontology:affectProduct
cpe:cpe:2.3:a:cisco:industrial_network_director:1.6.0:*:*:*:*:*.*.
cve:CVE-2019-1881 vulontology:hasAccessVector "NETWORK".
cve:CVE-2019-1881 vulontology:hasAuthentication "NONE".

```

Fig. 8. NER result align with VulKG

In this sample case, we process the latest vulnerability description by NLP component in AARV model and align the NER result with VulKG, which could partially replace the analysis and labeling work of security experts. VulKG can also be automatically extended and enriched based on the latest vulnerability reports.

4.2 CWE Chain Reasoning

In this section, we demonstrate the reasoning flow of the sample CWE Chain: CWE-918[Server-Side Request Forgery (SSRF)] → CWE-79[Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)] which is in the reasoning result list. The reasoning sample is based on VulKG which contains the vulnerability data including NVD, CVE, CPE, and CWE in 2018 and 2019. The first step of reasoning CWE Chain is to query in VulKG for calculating Chain Confidence. The

second step is comparing the calculation result with presetting threshold, which can identify whether the sample Chain is a CWE Chain Candidate. Finally, we will show a real vulnerability to support the logic behind the sample Chain.

The calculation of Chain Confidence needs to query in VulKG for two parameters C_1 and C_{12} . VulKG is stored in Neo4j which is a widely-used graph database. We use Cypher which is the query language of Neo4j to query for C_1 and C_{12} . More specific, we query for C_1 of sample Chain (CWE-918 \rightarrow CWE-79) as the first step. According to the definition, C_1 of sample Chain is the number of products which have weakness CWE-918. The Cypher query for C_1 is shown in Fig. 9a.

```
MATCH (a:Weakness {CWE_ID:"CWE-918"})--(b:Vulnerability)--(c:Product) return distinct(c)
```

Fig. 9a. Cypher query for calculating C_1 (CWE-918) in VulKG

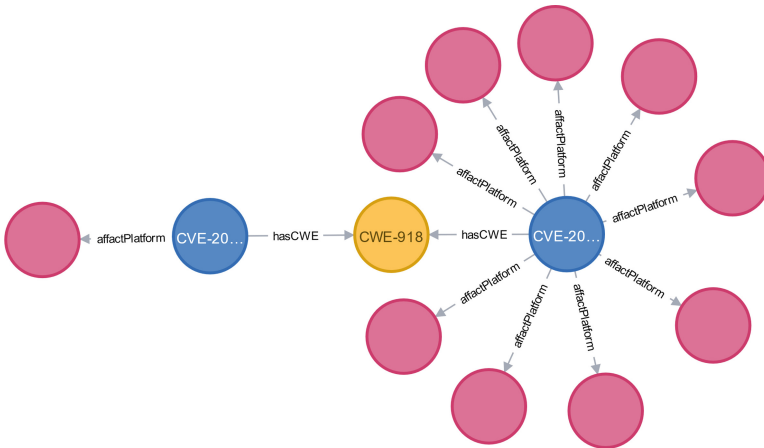


Fig. 9b. Cypher query result visualization [C_1 (CWE-918)]

Since the full version of the results is large and not easy to display clearly, Fig. 9b demonstrates a simplified version of the query result visualization. In the query result visualization, pink nodes represent for CPE objects. The yellow node represents for CWE objects. The blue nodes represent for CVE objects. From query result visualization, we can tell that the CWE-918 has several specific CVE as neighbor which will affect different CPE products. We count the CPE objects amount as C_1 of sample Chain.

Then we query for C_{12} of sample Chain. According to the definition, C_{12} of sample Chain is the number of products which have weaknesses CWE-918 and CWE-79. The Cypher query for C_{12} is shown in Fig. 10a.

```
MATCH (a:Weakness {CVE_ID:"CVE-918"})--(b:Vulnerability)--(c:Product)--
      (d:Vulnerability)--(e:Weakness {CVE_ID:"CVE-79"}) return distinct(c)
```

Fig. 10a. Cypher query for calculating C_{12} (CVE-918 & CVE-79)

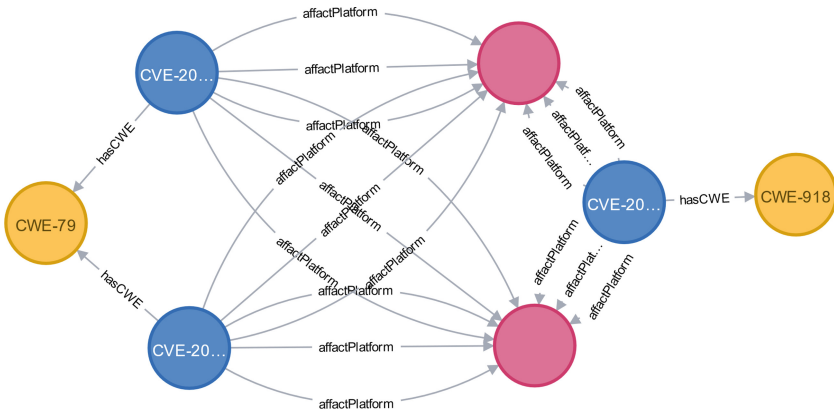


Fig. 10b. Cypher query result visualization [C_{12} (CVE-918 & CVE-79)]

From query result visualization in Fig. 10b, we can tell that there are different paths linking CVE-918 and CVE-79. We count the amount of CPE objects which are the nodes of the linking path as C_{12} of sample Chain. Result in Fig. 10b is also simplified.

Next step, we calculate the Chain Confidence using the query result. After getting the indicators of Chain reasoning, we compare them with the presetting threshold. The statistical result with threshold is shown in Table 4.

Table 4. Statistical results of Sample Chain with threshold

	Head CWE	C_1	Tail CWE	C_{12}	Chain Confidence
2018	CWE-918	213	CWE-79	102	0.478873239
2019	CWE-918	191	CWE-79	104	0.544502618
Threshold		100		100	0.2

In both 2018 and 2019, the reasoning indicators are over the threshold as shown in Table 4. So, the sample Chain is mined out as the CWE Chain Candidate.

Finally, we validate the CWE Chain Candidate, and try to judge whether this Candidate is a real CWE Chain. In the sample Chain, CVE-918 is commonly called SSRF while CVE-79 is commonly called XSS. In general, attackers can use SSRF to forge requests and control response packets. In some exploit scenarios, the contents of the response packets are displayed on the web page without filtering. If the malicious JavaScript code is inserted into response packet, the attackers will construct an XSS vulnerability successfully.

The SSRF to XSS attack chain is very common. We also found an actual vulnerability (CVE-2017-9506) to support the validation of the sample Chain. The description of the proof vulnerability is shown in Fig. 11.

CVE-2017-9506: The IconUriServlet of the Atlassian OAuth Plugin from version 1.3.0 before version 1.9.12 and from version 2.0.0 before version 2.0.4 allows remote attackers to access the content of internal network resources and/or perform an **XSS attack** via **Server Side Request Forgery (SSRF)**.

Fig. 11. Vulnerability description of CVE-2017-9506

In the description, it is said that the attacker could perform an XSS (CWE-79) attack via Server Side Request Forgery (CWE-918). So, the exploit logic behind the sample Chain Candidate is reasonable. Finally, we get one CWE Chain from the VulKG reasoning function.

5 Conclusions and Future Work

In this paper, we proposed the AARV model for automatic analysis and reasoning based on VulKG. VulKG is extracted from semi-structured data and extended by knowledge from unstructured data. The NLP component can automatically analyze and process the latest vulnerability description. The reasoning function based on VulKG can reason out valuable CWE Chain which reveals the hidden relationship between weaknesses. We also demonstrate sample cases of different part in AARV model.

Future work will focus on following research direction:

1. Improve the reasoning function. We will try to support more complicated reasoning task by using embedding-based methods.
2. Add more vulnerability detail to VulKG. With more detail, the VulKG could be the knowledge base of intrusion detection system.
3. Improve the entity-VulKG alignment algorithm. We will try to use deep learning method to improve the performance of alignment task.

References

1. NVD Homepage. <https://nvd.nist.gov/>. Accessed 14 Sept 2014
2. CVE Homepage. <https://cve.mitre.org/>. Accessed 14 Sept 2014
3. CWE Homepage. <https://cwe.mitre.org/>. Accessed 14 Sept 2014
4. CVSS Homepage. <https://www.first.org/cvss/>. Accessed 14 Sept 2014
5. CPE Homepage. <https://cpe.mitre.org/>. Accessed 14 Sept 2014
6. Iannacone, M.D., et al.: Developing an ontology for cyber security knowledge graphs. *CISR* **15**, 12 (2015)

7. Undercofer, J., Joshi, A., Finin, T., Pinkston, J.: A target-centric ontology for intrusion detection. In: Workshop on Ontologies in Distributed Systems, held at The 18th International Joint Conference on Artificial Intelligence (2003)
8. More, S., Matthews, M., Joshi, A., Finin, T.: A knowledge-based approach to intrusion detection modeling. In: 2012 IEEE Symposium on Security and Privacy Workshops, pp. 75–81. IEEE (2012)
9. Syed, Z., Padia, A., Finin, T., Mathews, L., Joshi, A.: UCO: a unified cybersecurity ontology. In: Workshops at the Thirtieth AAAI Conference on Artificial Intelligence (2016)
10. Du, D., et al.: Refining traceability links between vulnerability and software component in a vulnerability knowledge graph. In: Mikkonen, T., Klamma, R., Hernández, J. (eds.) ICWE 2018. LNCS, vol. 10845, pp. 33–49. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-91662-0_3
11. Jia, Y., Qi, Y., Shang, H., Jiang, R., Li, A.: A practical approach to constructing a knowledge graph for cybersecurity. *Engineering* **4**(1), 53–60 (2018)
12. Liao, X., Yuan, K., Wang, X.F., Li, Z., Xing, L., Beyah, R.: Acing the IOC game: toward automatic discovery and analysis of open-source cyber threat intelligence. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 755–766. ACM (2016)
13. Gasmi, H., Bouras, A., Laval, J.: LSTM recurrent neural networks for cybersecurity named entity recognition. In: ICSEA 2018, p. 11 (2018)
14. Joshi, A., Lal, R., Finin, T., Joshi, A.: Extracting cybersecurity related linked data from text. In 2013 IEEE Seventh International Conference on Semantic Computing, pp. 252–259. IEEE (2013)
15. Alqahtani, S.S., Eghan, E.E., Rilling, J.: SV-AF—a security vulnerability analysis framework. In: 2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE), pp. 219–229. IEEE (2016)
16. Narayanan, S.N., Ganesan, A., Joshi, K., Oates, T., Joshi, A., Finin, T.: Early detection of cybersecurity threats using collaborative cognition. In: 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), pp. 354–363. IEEE (2018)
17. Han, Z., Li, X., Liu, H., Xing, Z., Feng, Z.: DeepWeak: reasoning common software weaknesses via knowledge graph embedding. In: 2018 IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER), pp. 456–466. IEEE (2018)
18. Mendes, P.N., Jakob, M., García-Silva, A., Bizer, C.: DBpedia spotlight: shedding light on the web of documents. In: Proceedings of the 7th International Conference on Semantic Systems, pp. 1–8. ACM (2011)
19. Cheikes, B.A., Cheikes, B.A., Kent, K.A., Waltermire, D.: Common platform enumeration: naming specification version 2.3. US Department of Commerce, National Institute of Standards and Technology (2011)
20. Chains and Composites. https://cwe.mitre.org/data/reports/chains_and_composites.html. Accessed 14 Sept 2014
21. Pingle, A., Piplai, A., Mittal, S., Joshi, A.: RelExt: relation extraction using deep learning approaches for cybersecurity knowledge graph improvement. arXiv preprint [arXiv:1905.02497](https://arxiv.org/abs/1905.02497) (2019)



Application of Principal Component Analysis for Assessment the Behavior of Knowledge Management

Na Ran (✉)

University of Science and Technology Beijing, 30 Xueyuan Road,
Haidian District, Beijing 100083, People's Republic of China
ranna@ustb.edu.cn

Abstract. Most of the knowledge is first published in various types of journals in the form of articles. Better manage the knowledge in the form of articles will greatly benefit the development of economics, and society. It is difficult to assess the management of knowledge. Principal component analysis has been used to the knowledge management with the economic data, population data, educational data, research data for two developing countries and two developed countries. It is found that only the first two factors at the most are needed to replace the original variables. Larger fluctuations in the proportion of the loadings for different types of journals to the total loadings are found in the developing countries compared to those in the developed countries. And the largest loading for the journal is almost the same as for the population. The expressions between the factor and the standard formal variable obtained by the principal component analysis can be used to further study the effects of knowledge management on the development of society and economics. the GDP is found have a strong positive relationship with the population, education expenditure, researchers in R&D, the Industrial design applications, the Trademark applications, the Gross enrolment ratio, the Teachers in tertiary education, the Scientific and technical journal articles, different types of journals.

Keywords: Principal component analysis · Knowledge management · Knowledge share

1 Introduction

It is well known that the behavior of knowledge management (how to knowledge share, knowledge spread in the world) is very important to the rapid transformation of the knowledge to the productive force. After a knowledge dissemination mechanism has been built, knowledge can be spread in the society. And thus, people can use the knowledge to develop technology, promote social progress, and liberate productive forces. At the same time, knowledge owners also can get fast feedback information of knowledge application. The relationship between teachers and apprentices is the knowledge dissemination mechanism in early human society. And an agent for knowledge repository and the dissemination of knowledge-library has come [1]. Later,

a new knowledge dissemination mechanism-publishing scientific research in academic journals has appeared. In the second half of the last century, the beginning of the Internet has brought new characteristics of knowledge dissemination mechanism: more and more rapidly for cultural, academic exchanges, and even telemedicine activities that previously seemed impossible to implement has been developed. Such a transformation can be sped by letting the articles published in scientific journals are free to all readers. One can note that scientific researches especially basic scientific researches aim to seek the truth, understand the world promote social progress, and liberate productive forces. Its ultimate goal is to expand human knowledge and benefit mankind. The exchange of scientific researches will encourage scientific researchers to share their knowledge with others, so that knowledge can be transferred from individual ownership to group ownership. For example, the developing countries can benefit the most from free dissemination mechanism [2].

It is found that social sciences can be studied by information theory [3]. And a system in the social sciences can also be mathematically and computationally modeled [4]. Statistical methods have been applied to study the behavioral sciences [5]. The problem in social science can also be studied by statistical methods [6]. The statistical software has been widely used in social science such as business, economics, psychology, sociology, political science, and social networks [7, 8]. For a system, it often includes larger numbers of variables. Thus, it is difficult to interpret the behavior of a system. At the same time, these variables are somehow similar. This means that multicollinearity in these variables. Such a multicollinearity problem between the independent variables has a large effect on the prediction of dependent variables in the regression analysis [9]. The principal component analysis is just such a method that can help us find interrelationships between variables [10]. It has been used for early disease detection [11, 12], for analyzing the performance of semiconductor devices [13], socio-economic impact [14], the relationships between some pre- and post-slaughter traits of broilers [15], and many other fields of natural and Social Sciences. The aim of this paper is to study the correlation of the behavior of knowledge management (how to knowledge share, knowledge spread in the world) and national economic development by using principal component analysis. The data of two big developing countries (China and India) in Asia and two developed countries (USA and UK) have been studied by principal component analysis.

2 Method

For a given paired data (x_i, y_i) , the Pearson r correlation coefficient can be calculated by

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}} \quad (1)$$

where $\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$ and $\bar{y} = \frac{1}{n} \sum_{i=1}^n y_i$.

The variables are somehow similar, which means that the fluctuation of the variables is “approximately” the same. For interpreting a dataset with many variables, principal component analysis is most widely used to reduce the number of variables and reveal hidden variables. It is the general description of the common variance. If x is a vector of p random variables, define a linear function

$$\alpha'_1 x = \alpha_{11}x_1 + \alpha_{12}x_2 + \cdots + \alpha_{1p}x_p = \sum_{j=1}^p \alpha_{1j}x_j \quad (2)$$

the first step is to look for $\alpha'_1 x$ with the elements x having maximum variance. Next, look for a linear function $\alpha'_2 x$ that is uncorrelated with $\alpha'_1 x$ having a maximum variance. And so on, the k th step is finished. $\alpha'_k x$ is the k th principal component. Up to p principal component can be obtained. It is hoped that m ($m < p$) principal components can explain most of the variation in x . This is the key idea that complexity can be reduced by transforming the original variables into principal components.

If \sum is assumed to be the covariance matrix for vector x and α_k is assumed to be unit length, to maximize variance requires $\alpha'_1 \sum \alpha_1 = \alpha'_1 \lambda \alpha_1 = \lambda \alpha'_1 \alpha_1 = \lambda$. Here λ is a Lagrange multiplier, and α_1 is the eigenvector for the largest eigenvalue. λ should be as larger as possible.

The data of the number of access prestigious academic journals in natural science (indexed by SCI, the abbreviation of science citation index) and the number of prestigious academic journals in social science (indexed by SSCI, the abbreviation of social science citation index) in recently 21 years for China, India, USA (United States of America), and UK (the United Kingdom) come from the website of the Web of Science (www.isiknowledge.com). The GDP (Gross domestic product) data, population data, educational data, and research data of China, India, USA, and the UK come from the website of the World Bank (www.worldbank.org).

3 Results and Discussion

3.1 Qualitative Analysis

Figure 1 depicts how the GDP (constant 2010 US\$) data and the population data of China, India, USA, and the UK change with time for the recently 21 years. The data come from the website of the World Bank. One can easily found that the GDP of the developing countries (China and India) increases faster than the developed countries (USA and UK) did. One can also easily found the population in all four counties slowly increases with time. On the other hand, it can be found that the GDP growth is much faster than the population growth for all four countries.

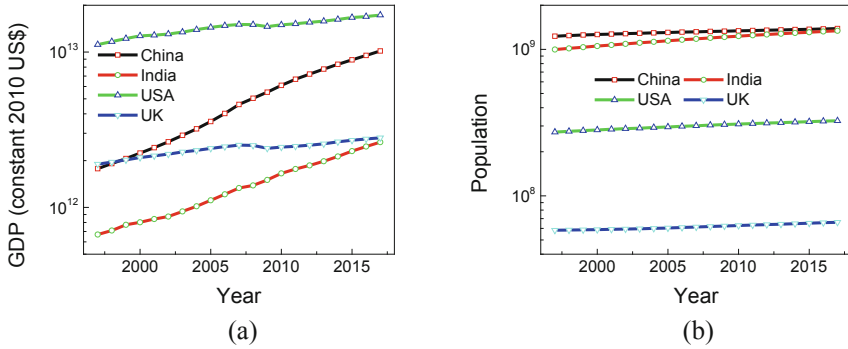


Fig. 1. (a) The GDP (constant 2010 US\$) and (b) the population of China, India, USA, and the UK as a function of time.

Figure 2 demonstrates how the education expenditure (% of GNI) and the education expenditure (current US\$) of China, India, USA, and the UK change with time for the recently 21 years. GNI is Gross national income. The data come from the website of the World Bank. It can easily be observed in both figures that there are no monotonous or decline relationships for all four countries. But there is a growing trend for education expenditure (current US\$). It means that the education expenditure (current US\$) is more relevant to the GDP than education expenditure (% of GNI).

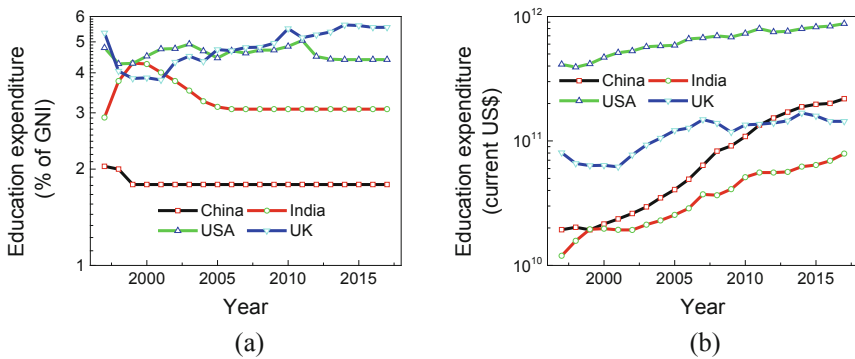


Fig. 2. (a) The education expenditure (% of GNI) (b) The education expenditure (current US\$) of China, India, USA, and the UK as a function of time.

Figure 3 shows how the Research and development expenditure (% of GDP) and the Researchers in Research and Development (per million people) of China, India, the USA, and the UK change with time for recently 21 years. The data come from the website of the World Bank. Both figures clearly illustrate that there is a complicated situation however a growth trend is often observed.

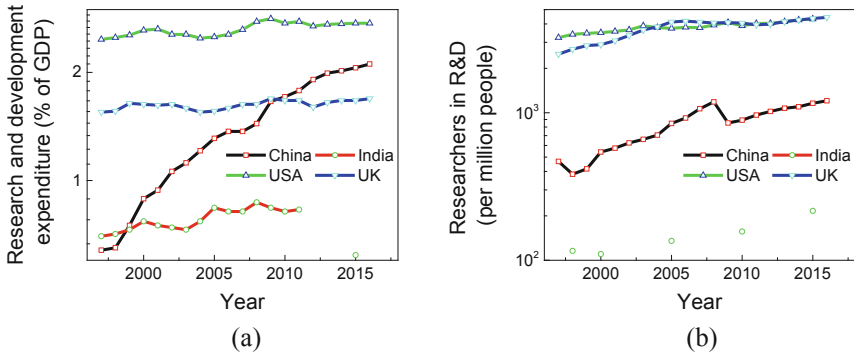


Fig. 3. (a) The Research and development expenditure (% of GDP) (b) the Researchers in Research and Development (per million people) of China, India, USA, and the UK as a function of time.

Figure 4 depicts how the Patent applications (residents) of China, India, the USA, and the UK change with time for recently 21 years. The data come from the website of the World Bank. It can be seen from both figures that both have a growth trend for China, India, USA.

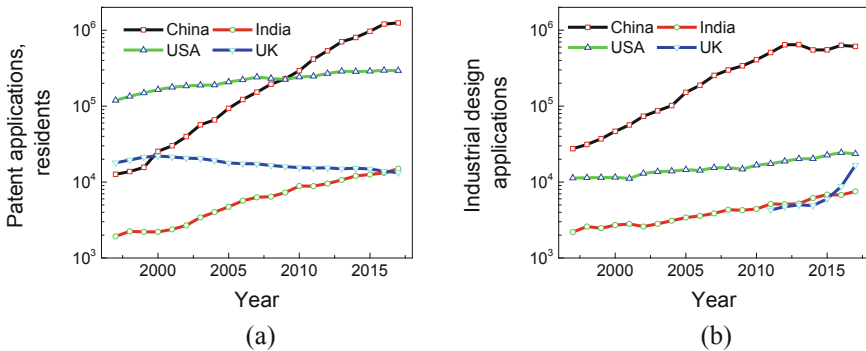


Fig. 4. (a) The Patent applications (residents) (b) The Industrial design applications (resident, by count) of China, India, USA, and the UK as a function of time.

Figure 5 shows how the total Trademark applications and the Gross enrolment ratio of China, India, USA, and the UK change with time for the recently 21 years. The data come from the website of the World Bank. It can be clearly seen in this figure that both have a growth trend for all four countries.

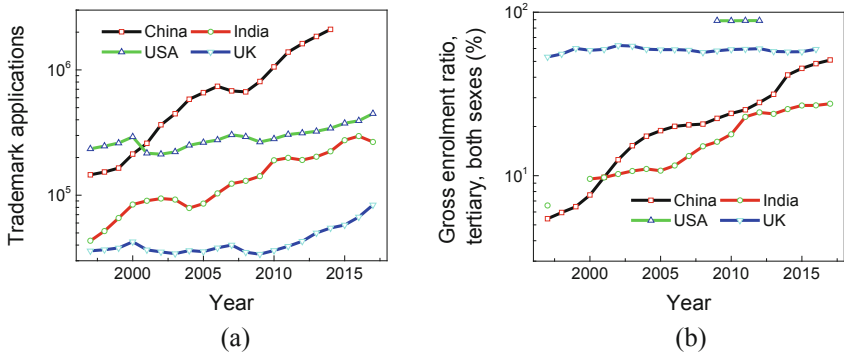


Fig. 5. (a) The total Trademark applications (b) The Gross enrolment ratio (tertiary, both sexes (%)) of China, India, USA, and the UK as a function of time.

Figure 6 depicts how the Teachers in tertiary education and how the Pupil-teacher ratio in tertiary education of China, India, USA, and the UK change with time for the recently 21 years. The data come from the website of the World Bank. Figure 6(a) clearly illustrates that there is a growing trend for all four countries. It can be clearly concluded from Fig. 6(b) that the Pupil-teacher ratio in tertiary education decreases with time for developed countries.

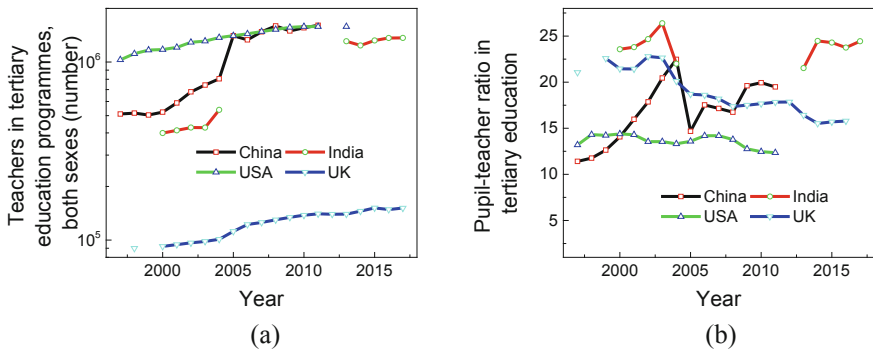


Fig. 6. (a) The Teachers in tertiary education programmes (both sexes) (b) The Pupil-teacher ratio in tertiary education, of China, India, USA, and the UK as a function of time.

Figure 7 demonstrates how the Scientific and technical journal articles of China, India, the USA, and the UK change with time for recently 21 years. The data come from the website of the World Bank. A growing trend for all four countries can be observed.

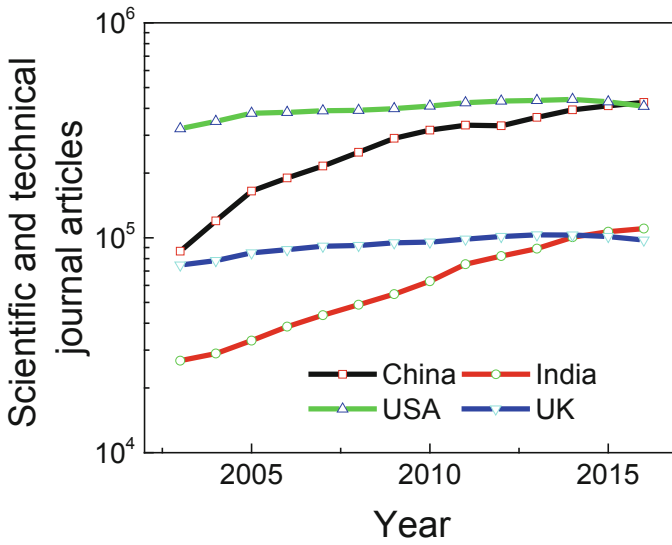


Fig. 7. The Scientific and technical journal articles of China, India, the USA, and the UK as a function of time.

Figure 8 depicts how the number of SCI-indexed journals and the number of SSCI-indexed journals published by China, India, the USA, and the UK change with time for the recently 21 years. The data come from the website of the World Bank. This figure clearly demonstrates that both have a growth trend for China, India, USA.

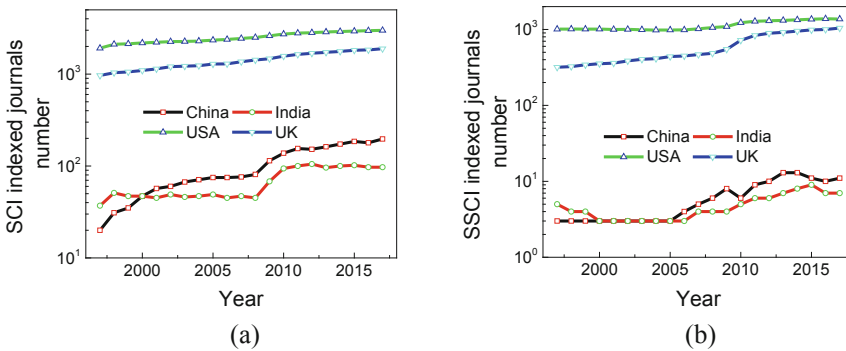


Fig. 8. (a) The number of SCI-indexed journals, and (b) The number of SSCI-indexed journals published by China, India, USA, and the UK as a function of time.

Figure 9 depicts how the number of open access SCI-indexed journals and the number of open access SSCI-indexed journals published by China, India, USA, and the UK change with time for the recently 21 years. The data come from the website of the

World Bank. This figure clearly demonstrates that both have a growth trend for China, India, USA.

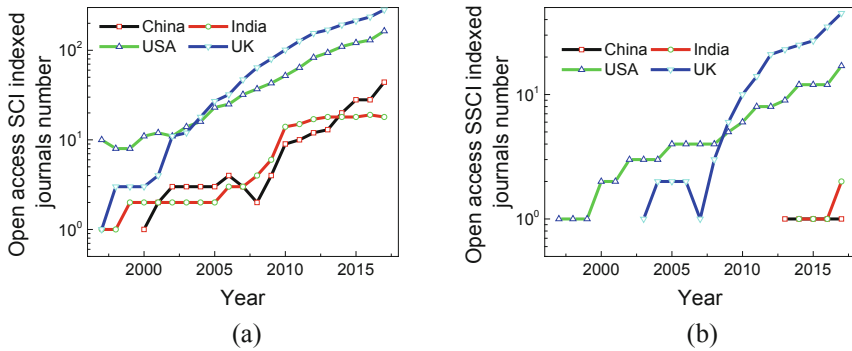


Fig. 9. (a) The number of open access SCI-indexed journals, and (b) the number of open access SSCI-indexed journals published by China, India, USA, and the UK as a function of time.

3.2 Correlation Coefficient Analysis

Table 1 shows the Pearson r correlation coefficient between the GDP (constant 2010 US\$) and population data, educational data, research data, and the prestigious journal data.

The results for China in the Table 1 demonstrate: there is a significant positive linear relationship between the population and the GDP because $r(19) = 0.967$, $p < 0.01$; there is not a significant negative linear relationship between the education expenditure (% of GNI) and the GDP because $r(19) = -0.392$, $p > 0.01$; there is a significant positive linear relationship between the education expenditure (current US\$) and the GDP because $r(19) = 0.992$, $p < 0.01$; there is a significant positive linear relationship between the Research and development expenditure (% of GDP) and the GDP because $r(18) = 0.992$, $p < 0.01$; there is a significant positive linear relationship between the Research and Researchers in R&D (per million people) and the GDP because $r(18) = 0.981$, $p < 0.01$; there is a significant positive linear relationship between the Research and Patent applications (nonresidents) and the GDP because $r(19) = 0.954$, $p < 0.01$; there is a significant positive linear relationship between the Industrial design applications (nonresident, by count) and the GDP because $r(19) = 0.968$, $p < 0.01$; there is a significant positive linear relationship between the total Trademark applications and the GDP because $r(16) = 0.971$, $p < 0.01$; there is a significant positive linear relationship between the Gross enrolment ratio in tertiary education for both sexes (%) and the GDP because $r(19) = 0.974$, $p < 0.01$; there is a significant positive linear relationship between the teachers in tertiary education for both sexes and the GDP because $r(13) = 0.992$, $p < 0.01$; there is not a significant positive linear relationship between the Pupil-teacher ratio in tertiary education and the GDP because $r(13) = 0.610$, $p > 0.01$; there is a significant positive linear relationship

between the Scientific and technical journal articles and the GDP because $r(12) = 0.980, p < 0.01$; there is a significant positive linear relationship between the SCI-indexed journals and the GDP because $r(19) = 0.982, p < 0.01$; there is a significant positive linear relationship between the SSCI-indexed journals and the GDP because $r(19) = 0.933, p < 0.01$; there is a significant positive linear relationship between the open access SCI-indexed journals and the GDP because $r(19) = 0.894, p < 0.01$; there is a significant positive linear relationship between the open access SSCI-indexed journals and the GDP because $r(19) = 0.810, p < 0.01$.

Table 1. Correlation coefficient matrix.

		China	India	USA	UK
Population	Pearson	0.967	0.973	0.983	0.936
	Sig.	0.000	0.000	0.000	0.000
Education expenditure (% of GNI)	Pearson	-0.392	-0.593	-0.171	0.736
	Sig.	0.078	0.005	0.457	0.000
Education expenditure (current US\$)	Pearson	0.992	0.992	0.977	0.916
	Sig.	0.000	0.000	0.000	0.000
R&D expenditure (% of GDP)	Pearson	0.974	-0.558	0.726	0.561
	Sig.	0.000	0.013	0.000	0.000
Researchers in R&D (per million people)	Pearson	0.881	0.982	0.942	0.964
	Sig.	0.000	0.003	0.000	0.000
Patent applications	Pearson	0.954	0.997	0.985	-0.835
	Sig.	0.000	0.000	0.000	0.000
Industrial design applications	Pearson	0.968	0.992	0.935	0.787
	Sig.	0.000	0.000	0.000	0.036
Trademark applications	Pearson	0.971	0.980	0.842	0.680
	Sig.	0.000	0.000	0.000	0.000
Gross enrolment ratio	Pearson	0.974	0.977	0.591	0.161
	Sig.	0.000	0.000	0.409	0.499
Teachers in tertiary education	Pearson	0.931	0.983	0.972	0.943
	Sig.	0.000	0.000	0.000	0.000
Pupil-teacher ratio in tertiary education	Pearson	0.610	-0.070	-0.405	-0.887
	Sig.	0.016	0.847	0.135	0.000
Scientific and technical journal articles	Pearson	0.980	0.994	0.820	0.775
	Sig.	0.000	0.000	0.000	0.000
Number of SCI-indexed journals	Pearson	0.982	0.892	0.951	0.936
	Sig.	0.000	0.000	0.000	0.000
Number of SSCI-indexed journals	Pearson	0.933	0.852	0.810	0.855
	Sig.	0.000	0.000	0.000	0.000
Number of open access SCI-indexed journals	Pearson	0.894	0.941	0.883	0.864
	Sig.	0.000	0.000	0.000	0.000
Number of open access SSCI-indexed journals	Pearson	0.810	0.757	0.904	0.801
	Sig.	0.000	0.000	0.000	0.000

The results for India in the Table 1 demonstrate: there is a significant positive linear relationship between the population and the GDP because $r(19) = 0.973$, $p < 0.01$; there is a significant negative linear relationship between the education expenditure (% of GNI) and the GDP because $r(19) = -0.593$, $p < 0.01$; there is a significant positive linear relationship between the education expenditure (current US\$) and the GDP because $r(19) = 0.992$, $p < 0.01$; there is a significant positive linear relationship between the Research and development expenditure (% of GDP) and the GDP because $r(17) = 0.992$, $p < 0.01$; there is not a significant negative linear relationship between the Research and Researchers in R&D (per million people) and the GDP because $r(3) = 0.982$, $p < 0.01$; there is a significant positive linear relationship between the Research and Patent applications (nonresidents) and the GDP because $r(19) = 0.997$, $p < 0.01$; there is a significant positive linear relationship between the Industrial design applications (nonresident, by count) and the GDP because $r(19) = 0.992$, $p < 0.01$; there is a significant positive linear relationship between the total Trademark applications and the GDP because $r(19) = 0.980$, $p < 0.01$; there is a significant positive linear relationship between the Gross enrolment ratio in tertiary education for both sexes (%) and the GDP because $r(17) = 0.977$, $p < 0.01$; there is a significant positive linear relationship between the teachers in tertiary education for both sexes and the GDP because $r(8) = 0.983$, $p < 0.01$; there is not a significant negative linear relationship between the Pupil-teacher ratio in tertiary education and the GDP because $r(8) = -0.070$, $p > 0.01$; there is a significant positive linear relationship between the Scientific and technical journal articles and the GDP because $r(12) = 0.994$, $p < 0.01$; there is a significant positive linear relationship between the SCI-indexed journals and the GDP because $r(19) = 0.892$, $p < 0.01$; there is a significant positive linear relationship between the SSCI-indexed journals and the GDP because $r(19) = 0.852$, $p < 0.01$; there is a significant positive linear relationship between the open access SCI-indexed journals and the GDP because $r(19) = 0.941$, $p < 0.01$; there is a significant positive linear relationship between the open access SSCI-indexed journals and the GDP because $r(19) = 0.757$, $p < 0.01$.

The results for USA in the Table 1 demonstrate: there is a significant positive linear relationship between the population and the GDP because $r(19) = 0.983$, $p < 0.01$; there is not a significant negative linear relationship between the education expenditure (% of GNI) and the GDP because $r(19) = -0.171$, $p > 0.01$; there is a significant positive linear relationship between the education expenditure (current US\$) and the GDP because $r(19) = 0.977$, $p < 0.01$; there is a significant positive linear relationship between the Research and development expenditure (% of GDP) and the GDP because $r(18) = 0.726$, $p < 0.01$; there is a significant positive linear relationship between the Research and Researchers in R&D (per million people) and the GDP because $r(17) = 0.942$, $p < 0.01$; there is a significant positive linear relationship between the Research and Patent applications (nonresidents) and the GDP because $r(19) = 0.985$, $p < 0.01$; there is a significant positive linear relationship between the Industrial design applications (nonresident, by count) and the GDP because $r(19) = 0.935$, $p < 0.01$; there is a significant positive linear relationship between the total Trademark applications and the GDP because $r(16) = 0.842$, $p < 0.01$; there is not a significant positive linear relationship between the Gross enrolment ratio in tertiary education for both sexes (%) and the GDP because $r(2) = 0.591$, $p > 0.01$; there is a significant positive

linear relationship between the teachers in tertiary education for both sexes and the GDP because $r(14) = 0.972$, $p < 0.01$; there is not a significant positive linear relationship between the Pupil-teacher ratio in tertiary education and the GDP because $r(13) = -0.405$, $p > 0.01$; there is a significant negative linear relationship between the Scientific and technical journal articles and the GDP because $r(12) = 0.820$, $p < 0.01$; there is a significant positive linear relationship between the SCI-indexed journals and the GDP because $r(19) = 0.951$, $p < 0.01$; there is a significant positive linear relationship between the SSCI-indexed journals and the GDP because $r(19) = 0.810$, $p < 0.01$; there is a significant positive linear relationship between the open access SCI-indexed journals and the GDP because $r(19) = 0.883$, $p < 0.01$; there is a significant positive linear relationship between the open access SSCI-indexed journals and the GDP because $r(19) = 0.904$, $p < 0.01$.

The results for UK in the Table 1 demonstrate: there is a significant positive linear relationship between the population and the GDP because $r(19) = 0.936$, $p < 0.01$; there is a significant negative linear relationship between the education expenditure (% of GNI) and the GDP because $r(19) = 0.736$, $p < 0.01$; there is a significant positive linear relationship between the education expenditure (current US\$) and the GDP because $r(19) = 0.936$, $p < 0.01$; there is a significant positive linear relationship between the Research and development expenditure (% of GDP) and the GDP because $r(18) = 0.561$, $p = 0.01$; there is a significant positive linear relationship between the Research and Researchers in R&D (per million people) and the GDP because $r(18) = 0.964$, $p < 0.01$; there is a significant positive linear relationship between the Research and Patent applications (nonresidents) and the GDP because $r(19) = -0.835$, $p < 0.01$; there is not a significant negative linear relationship between the Industrial design applications (nonresident, by count) and the GDP because $r(5) = 0.787$, $p > 0.01$; there is a significant positive linear relationship between the total Trademark applications and the GDP because $r(19) = 0.680$, $p < 0.01$; there is not a significant positive linear relationship between the Gross enrolment ratio in tertiary education for both sexes (%) and the GDP because $r(18) = 0.161$, $p > 0.01$; there is a significant positive linear relationship between the teachers in tertiary education for both sexes and the GDP because $r(17) = 0.943$, $p < 0.01$; there is not a significant negative linear relationship between the Pupil-teacher ratio in tertiary education and the GDP because $r(17) = -0.887$, $p < 0.01$; there is a significant positive linear relationship between the Scientific and technical journal articles and the GDP because $r(12) = 0.775$, $p < 0.01$; there is a significant positive linear relationship between the SCI-indexed journals and the GDP because $r(19) = 0.936$, $p < 0.01$; there is a significant positive linear relationship between the SSCI-indexed journals and the GDP because $r(19) = 0.855$, $p < 0.01$; there is a significant positive linear relationship between the open access SCI-indexed journals and the GDP because $r(19) = 0.864$, $p < 0.01$; there is a significant positive linear relationship between the open access SSCI-indexed journals and the GDP because $r(19) = 0.801$, $p < 0.01$.

In summary, only the Population, the Education expenditure (current US\$), the Researchers in R&D, the Industrial design applications, the Teachers in tertiary education, the Scientific and technical journal articles, the SCI-indexed journals, the SSCI-indexed journals, the open-access SCI-indexed journals, and the open-access SSCI-indexed journals are always positively correlated to the GDP for all four countries.

3.3 Principal Component Analysis

In order to use principal component analysis, only the data of the GDP, the population, the Education expenditure (current US\$), the Researchers in R&D, the Industrial design applications, the Scientific and technical journal articles, the SCI-indexed journals, the SSCI-indexed journals, the open-access SCI-indexed journals, and the open-access SSCI-indexed journals have been chosen. Table 2 shows the statistics, which are used to verify and to ensure the correlation matrix is appropriate for principal component analysis. Table 2 clearly shows all KMO-statistics are larger than 0.5, and all Bartlett significance is less than 0.001. It demonstrates that the data are indeed quite appropriate for principal component analysis. Additionally, both the initial communalities—the amount of common variance and the extraction communalities are 1.0 for all four countries.

Table 2. KMO-statistics and Bartlett significance.

	China	India	USA	UK
KMO-statistics	0.736314	.874	.639	.797
Bartlett significance	1.2079E-42	7.7812E-38	1.8058E-38	1.9363E-37

Tables 3, 4, 5 and 6 show the cumulative percentage of variance explained. Usually, a cumulative percentage of approximately 90% be enough to explain. Factor 1 explains 87.62%, 93.46%, 91.83%, and 78.67% of total variants for the data of China, India, USA, and the UK, respectively. Factor 2 explains 5.08%, 6.54%, 3.85%, and 17.89% of total variants for the data of China, India, USA, and the UK, respectively. One main component is needed for China, India, and the USA, two components are needed for the UK.

Table 3. Total variance explained for the data of China.

Component	Initial Eigenvalues			Extraction sums of squared loading			Rotation sums of squared loading		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	8.762	87.617	87.617	8.762	87.617	87.617	4.769	47.694	47.694
2	.508	5.075	92.692	.508	5.075	92.692	2.062	20.620	68.315
3	.444	4.439	97.131	.444	4.439	97.131	1.869	18.692	87.007
4	.208	2.080	99.210	.208	2.080	99.210	1.197	11.970	98.977
5	.045	.450	99.661	.045	.450	99.661	.058	.581	99.558
6	.023	.231	99.892	.023	.231	99.892	.031	.311	99.869
7	.009	.085	99.977	.009	.085	99.977	.010	.101	99.970
8	.002	.018	99.995	.002	.018	99.995	.002	.017	99.987
9	.000	.004	99.999	.000	.004	99.999	.001	.011	99.998
10	.000	.001	100.00	.000	.001	100.00	.000	.002	100.00

Table 4. Total variance explained for the data of India.

Component	Initial Eigenvalues			Extraction sums of squared loading			Rotation sums of squared loading		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	9.346	93.456	93.456	9.346	93.456	93.456	5.076	50.762	50.762
2	.654	6.544	100.00	.654	6.544	100.00	4.924	49.238	100.00
3	7.461E-16	7.461E-15	100.00	7.461E-16	7.461E-15	100.000	1.183E-15	1.183E-14	100.00
4	5.375E-16	5.375E-15	100.00	5.375E-16	5.375E-15	100.000	9.724E-16	9.724E-15	100.00
5	3.199E-16	3.199E-15	100.00	3.199E-16	3.199E-15	100.000	7.443E-16	7.443E-15	100.00
6	7.257E-17	7.257E-16	100.00	7.257E-17	7.257E-16	100.000	4.839E-16	4.839E-15	100.00
7	-8.357E-17	-8.357E-16	100.00	8.357E-17	8.357E-16	100.000	3.982E-16	3.982E-15	100.00
8	-1.728E-16	-1.728E-15	100.00	1.728E-16	1.728E-15	100.000	3.000E-16	3.000E-15	100.00
9	-4.514E-16	-4.514E-15	100.00	4.514E-16	4.514E-15	100.000	1.560E-16	1.560E-15	100.00
10	-1.463E-15	-1.463E-14	100.00	1.463E-15	1.463E-14	100.000	1.414E-16	1.414E-15	100.00

Table 5. Total Variance Explained for the data of the USA.

Component	Initial Eigenvalues			Extraction sums of squared loading			Rotation sums of squared loading		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	9.183	91.831	91.831	9.183	91.831	91.831	3.603	36.033	36.033
2	.385	3.849	95.680	.385	3.849	95.680	2.816	28.157	64.190
3	.201	2.007	97.688	.201	2.007	97.688	2.225	22.251	86.441
4	.122	1.216	98.903	.122	1.216	98.903	1.178	11.783	98.224
5	.065	.646	99.549	.065	.646	99.549	.120	1.197	99.420
6	.038	.381	99.930	.038	.381	99.930	.049	.490	99.910
7	.005	.046	99.977	.005	.046	99.977	.006	.058	99.968
8	.002	.019	99.996	.002	.019	99.996	.003	.026	99.994
9	.000	.004	99.999	.000	.004	99.999	.000	.003	99.997
10	6.6E-5	.001	100.00	6.6E-5	.001	100.00	.000	.003	100.00

Table 6. Total variance explained for the data of the UK.

Component	Initial Eigenvalues			Extraction sums of squared loading			Rotation sums of squared loading		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	7.867	78.667	78.667	7.867	78.667	78.667	7.413	74.129	74.129
2	1.789	17.892	96.559	1.789	17.892	96.559	1.377	13.772	87.900
3	.286	2.863	99.422	.286	2.863	99.422	1.140	11.404	99.305
4	.039	.389	99.812	.039	.389	99.812	.047	.474	99.778
5	.019	.188	100.000	.019	.188	100.000	.022	.222	100.000
6	1.111E-15	1.111E-14	100.000	1.111E-15	1.111E-14	100.000	1.652E-15	1.652E-14	100.000
7	1.331E-16	1.331E-15	100.000	1.331E-16	1.331E-15	100.000	4.522E-16	4.522E-15	100.000
8	2.571E-17	2.571E-16	100.000	2.571E-17	2.571E-16	100.000	1.885E-16	1.885E-15	100.000
9	-1.722E-16	-1.722E-15	100.000	1.722E-16	1.722E-15	100.000	1.676E-16	1.676E-15	100.000
10	-3.835E-16	-3.835E-15	100.000	3.835E-16	3.835E-15	100.000	3.100E-17	3.100E-16	100.000

Figure 10, the Scree plot, further demonstrates that one main component is needed for China, India, and the USA, two components are needed for the UK.

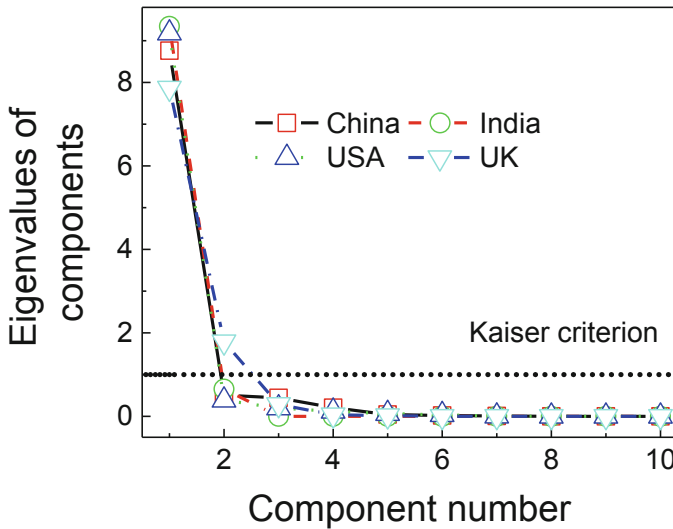


Fig. 10. The Scatter Plot generated through principal component analysis for the data of China, India, the USA, and the UK.

Table 7 shows the varimax rotated factor loading for the data of China, India, the USA, and the UK. For the data of China, Factor 1 explains 87.62% of total variants, the

Number of SCI-indexed journals with the strongest positive loading, the Researchers in R&D (per million people) with the lowest loading. For the data of India, Factor 1 explains 93.46% of total variants, the Number of open access SSCI-indexed journals with the strongest positive loading, the Number of SCI-indexed journals with the lowest loading. For the data of USA, Factor 1 explains 91.83% of total variants, the Scientific and technical journal articles with strongest positive loading, the Researchers in R&D (per million people) with the lowest loading. For the data of UK, Factor 1 explains 78.67% of total variants, the Number of open access SSCI-indexed journals with the strongest positive loading, the Scientific and technical journal articles with the lowest loading; Factor 2 explains 17.89% of total variants, the Scientific and technical journal articles with the strongest positive loading, the Researchers in R&D (per million people) with the lowest loading.

Table 7. Varimax rotate factor loadings.

	China	India	USA	UK	
	Factor 1	Factor 1	Factor 1	Factor 1	Factor 2
Number of open access SCI-indexed journals	.469	.447	.482	.975	-.050
Number of open access SSCI-indexed journals	.366	.955	.448	.985	-.057
Number of SCI-indexed journals	.810	.354	.673	.961	.027
Number of SSCI-indexed journals	.827	.805	.562	.963	.087
GDP	.722	.713	.618	.946	-.111
Population	.733	.655	.693	.968	-.074
Scientific and technical journal articles	.768	.756	.850	-.113	.974
Researchers in R&D (per million people)	.351	.847	.348	.943	-.038
Industrial design applications	.863	.829	.427	.885	-.438
Education expenditure (current US\$)	.747	.528	.717	.355	.451

Table 8 shows the ratio of each Varimax Rotate Factor Loading to the total loadings. The proportion of the loadings for different types of journals to the total loadings in the developed countries is relative uniform, whereas larger fluctuations come in the developing countries. On the other hand, The largest proportion of the loadings for journals in component 1 is compared to that for population and GDP.

Table 8. The ratio of varimax rotate factor loadings.

	China	India	USA	UK	
	Factor 1 (%)	Factor 1 (%)	Factor 1 (%)	Factor 1 (%)	Factor 2 (%)
Number of open access SCI-indexed journals	7.046274	6.488605	8.056957	12.39197	-6.48508
Number of open access SSCI-indexed journals	5.498798	13.86268	8.687815	12.51906	-7.393
Number of SCI-indexed journals	12.16947	5.138627	8.074982	12.21403	3.501946
Number of SSCI-indexed journals	12.42488	11.6853	12.1305	12.23945	11.28405
GDP	10.84736	10.34983	10.12978	12.02339	-14.3969
Population	11.01262	9.507911	11.13915	12.303	-9.59792
Scientific and technical journal articles	11.53846	10.97402	12.49099	-1.4362	126.3294
Researchers in R&D (per million people)	5.273438	12.29496	15.32084	11.98526	-4.92866
Industrial design applications	12.96575	12.03368	6.272531	11.24809	-56.8093
Education expenditure (current US\$)	11.22296	7.664393	7.696467	4.511947	58.49546

Table 9 shows the component score coefficient (or weight) matrix. Table 9 clearly gives the scientific and technical article published in the USA has the largest component score coefficient in component 1. Similarly, the population of the USA has the largest component score coefficient in component 1. Thus, the main component can be determined by the following equation

$$F_1 = a_1x_1 + a_2x_2 + \cdots + \alpha_{10}x_{10} \quad (3)$$

Table 9. The component score coefficient (or weight) matrix.

	China	India	USA	UK	
	Factor 1	Factor 1	Factor 1	Factor 1	Factor 2
Number of open access SCI-indexed journals (x_1)	-.537	-.245	-.286	.197	.056
Number of open access SSCI-indexed journals (x_2)	-.262	.685	-.330	.191	.053
Number of SCI-indexed journals (x_3)	.337	-.241	.241	.169	.034
Number of SSCI-indexed journals (x_4)	.411	.200	-.272	.172	.024
GDP (x_5)	.065	.000	-.104	.141	.051
Population (x_6)	.098	-.092	.366	.183	.057
Scientific and technical journal articles (x_7)	.181	.085	1.266	.215	1.197
Researchers in R&D (per million people) (x_8)	-.447	.317	-.065	.122	.038
Industrial design applications (x_9)	.601	.265	-.464	.024	-.039
Education expenditure (current US\$) (x_{10})	.153	-.215	.323	-.363	-.376

4 Conclusion

There are eleven strong positive correlation: the population and the GDP, the Education expenditure (current US\$) and the GDP, Researchers in R&D (per million people) and the GDP, the Industrial design applications and the GDP, the Trademark applications and the GDP, the Teachers in tertiary education and the GDP, the Scientific and technical journal articles and the GDP, the number of SCI-indexed journals and the GDP, the number of SSCI-indexed journals and the GDP, the number of open access SCI-indexed journals and the GDP, the number of open access SSCI-indexed journals and the GDP.

The knowledge management data with the economic data, population data, educational data, research data for two developing countries and two developed countries have been studied by using the principal component analysis. The results of the principal component analysis show only the first factor is needed to replace the original variables for the data of China, India, and the USA, whereas two factors are needed for the data of the UK. at the most Such factors contain almost all the information of the original variables. Larger fluctuations in the proportion of the loadings for different types of journals to the total loadings (5%–12% for China, and 5%–12% for India) are found in the developing countries compared to those in the developed countries (8%–12% for the USA, and 12%–13% for the UK). And the largest loading for the journal is almost the same as for the population. Lastly, the expression between the factor and the

standard formal variable is given. This article shows that the principal component analysis can be used to further study how knowledge management can help us improve our productivity and life, understand the world, improve society and economics.

References

1. Branin, J.J.: Knowledge management in academic libraries: building the knowledge bank at the Ohio State University. *J. Libr. Adm.* **39**(4), 41–56 (2003)
2. Kirsop, B., Chan, L.: Transforming access to research literature for developing countries. *Ser. Rev.* **31**(4), 246–255 (2005)
3. Bowden, R.: *The Information Theory of Comparisons: With Applications to Statistics and the Social Sciences*. Springer, Singapore (2018). <https://doi.org/10.1007/978-981-13-1550-3>
4. Melnik, R.: *Mathematical and Computational Modeling: With Applications in Natural and Social Sciences, Engineering, and the Arts*. Wiley, Hoboken (2015)
5. Nesselroade, K.P., Grimm, L.G.: *Statistical Applications for the Behavioral Sciences*. Wiley, Hoboken (2019)
6. Mukherjee, S.P., Sinha, B.K., Chattopadhyay, A.K.: *Statistical Methods in Social Science Research*. Springer, Singapore (2018). <https://doi.org/10.1007/978-981-13-2146-7>
7. Ho, R.: *Understanding Statistics for the Social Sciences with IBM SPSS*. Chapman and Hall/CRC, London (2017)
8. Yockey, R.D.: *SPSS Demystified*. Taylor & Francis, Oxford (2017)
9. Sharma, S.: *Applied Multivariate Techniques*. Wiley, New York (1996)
10. Sousa, S.I.V., Martins, F.G., Alvim-Ferraz, M.C.M., Pereira, M.C.: Multiple linear regression and artificial neural Networks based on principal components to predict ozone concentrations. *Environ. Model. Softw.* **22**(1), 97–103 (2007)
11. Papi, M., Caracciolo, G.: Principal component analysis of personalized biomolecular corona data for early disease detection. *Nano Today* **21**, 14–17 (2018)
12. Karouzakis, E., et al.: Analysis of early changes in DNA methylation in synovial fibroblasts of RA patients before diagnosis. *Sci. Rep.* **8**(1), 7370 (2018)
13. Fadhel, S., et al.: PV shading fault detection and classification based on IV curve using principal component analysis: application to isolated PV system. *Sol. Energy* **179**, 1–10 (2019)
14. Ali, A., Shang, J., Saif, U.: Socio-economic impact of CPEC on agricultural productivity of Pakistan: a Principal Component Analysis. *Int. J. Food Agric. Econ. (IJFAEC)* **6**, 47–57 (2018)
15. Mendes, M.: Multivariate multiple regression analysis based on principal component scores to study relationships between some pre-and post-slaughter traits of broilers. *J. Agric. Sci.* **17**, 77–83 (2011)



Information Extraction and Similarity Computation for Semi-/Un-Structured Sentences from the Cyberdata

Peiyong Zhang¹, Xingzhe Huang¹, Lei Zhang², and Weishan Zhang¹(✉)

¹ College of Computer Science and Technology,
China University of Petroleum (East China), Qingdao 266580, China
25640521@qq.com, 1776366729@qq.com, zhangws@upc.edu.cn

² Petroleum Engineering Technology Research Institute,
Shengli Oilfield, Sinopec, Beijing, China
zhanglei976.slyt@sinopec.com

Abstract. With the popularization of network and the improvement of network speed, social network application plays an increasingly important role in people's social life. People express their opinions and ask their own questions on social software, and these huge amounts of data drive researchers to propose various algorithms to extract the information in sentences and classify them. In this paper, we proposed a novel method of sentence similarity computation, which purpose is to extract the syntactic and semantic information of semi-structured and structured sentences and calculate their similarity. We mainly consider the subject predicate and object of sentence pairs, and use Stanford parser to classify Dependency Relation Triples to calculate the syntactic and semantic similarity between two sentences. Extensive simulations demonstrated that our method outperforms the other state-of-the-art methods in terms of correlation coefficient and mean deviation.

Keywords: Sentence similarity computation · Information extraction and computation · Syntactic similarity · Semantic similarity · Type of sentence pair

1 Introduction

The task of cyberdata extraction and computation is to extract useful information from semi-structured and unstructured data. With the help of the model, better decisions can be made and work can be done better. At present, there are various opinions, questions and answers on social networks, and people are accustomed to looking for answers on the Internet. How to classify data with high similarity and give better answers to users' questions is an important research direction. Natural Language Processing (NLP), as a branch of artificial intelligence, is widely used in sentence classification text summarization [1] and semantic analysis to deal with social network data. As a basic task of natural language

processing, sentence similarity computation is also widely used in text summary, semantic analysis, question answering systems, recommendation systems [2], automatic summarization [3,4] and so on. In the field of automatic question answering system, sentence similarity computation is used to match the question sentences so as to return the correct answer correspond to the user question. In the recommendation systems, sentence similarity computation is used to improve classical collaborative filtering methods for a site with the aim of matching people who are looking for expert advice on a specific topic. In the automatic summarization applications, sentence similarity computation is applied to eliminate sentences with similar meanings. In the field of sentence classification, sentence similarity analysis is used to classify sentences with the same emotion. In this paper, we propose a sentence similarity computation model that integrates both grammatical and semantic features, which will make the mining and calculation of social network data more accurate.

These aforementioned applications require model to understand human language and hidden meanings. Although the opinions, questions and so on of people on social networks are mostly semi-structured or unstructured, semantics are still an important factor in understanding the meaning of sentences. Therefore, semantic extraction of sentences is still crucial to the calculation of sentence similarity on social networks. Measuring sentence similarity on social networks is a challenge task because people express their opinions online more casually than in written language, which results in sentences that may not have correct grammatical information or even misspelled words. The traditional document similarity approaches is not efficient to measure the similarity between sentences. In addition to aforementioned reasons, there are other reasons is that the sentences may not contain any words or the co-occurrence of words is rarely appear, and two sentences may have an equivalent meanings with totally different structures in terms of word forms, word orders as well as the grammatical relations. In this context, the researchers have been introduced various short text similarity computation methods. There is still some room for improvement due to the complexity of human language.

This paper assumes that the approximate similarity between two sentences is determined by their subjects, verbs, and objects are the same or different, i.e., the sentence pattern. This paper also presumes that the accurate similarity between two sentences is determined by the syntactic structure similarity and the semantic similarity according to their syntactic kernels and semantic kernels. We summarized the main contributions of this paper as follows.

1. We divided all of the sentence pairs into eight cases according to their contained subjects, predicate verbs, and objects, and determined the coarse sentence similarity interval by their type of sentence pattern for each sentence pair.
2. This paper proposed a novel syntactic kernel to measure the syntactic similarity between two sentences in terms of their syntactic structures of the two sentences.

3. This paper proposed a novel semantic kernel to measure the semantic similarity between two sentences in terms of their expressed meanings of the two sentences.
4. This paper proposed a novel method of sentence similarity computation based on sentence pattern, syntactic and semantic, which imitates human thinking manner. Extensive simulations demonstrated that our method is better than the other state-of-the-art methods in terms of correlation coefficient and mean deviation.

The remainder of this paper is organized as follow. Section 2 describes the existing methods for computing sentence similarity. Section 3 introduces the coarse-grained sentence similarity computation on the aspect of sentence similarity interval. Section 4 introduces the fine-grained sentence similarity computation on aspects of syntactic and semantic. In Sects. 5 and 6, we present and discuss the experimentation evaluation for our method. The conclusions and future works are discussed in Sect. 7.

2 Related Works

Recent literatures on sentence similarity computation have shown abundantly proposed methods [5–14]. Most research studies exploited semantic similarity between two words for measuring how similar two input sentences are. Some of these methods utilized bag-of-words (BOW) techniques to calculate the sentence similarity. These BOW techniques based on the assumption that the more similar two sentences are the more common words they share. Over the past three years, there are many sentence similarity methods utilizing the convolutional neural networks and recurrent neural networks [15–17]. These sentence similarity computation methods can be roughly divided into three categories: the statistical-based methods, the regulation-based methods, and the hybrid methods.

2.1 The Statistical-Based Methods

These statistical-based methods compute sentence similarity usually by counting the number of the co-occurring words to measure the sentence similarity. In 2008, Islam Aminul and Inkpen Diana [5] proposed a corp-based algorithm to measure semantic word similarity. This paper mainly concentrated on computing the similarity between two sentences or two short textual segments, and applied to applications of textual knowledge representation and knowledge discovery, experimental results on two different datasets indicated that the proposed method is better than several other methods.

Several years later, the authors of [10] proposed a hybrid Sinhala sentence similarity computation method using a semantic similarity measurement technique (corpus-based similarity measurement plus knowledge-based similarity measurement), which used word order similarity and lexical resources in calculating the semantic similarity between two words. Experimental results indicated

that the proposed method achieved a Pearson correlation factor of 0.832 on 4000 sentence pairs.

Over the past three years, there is increasing concern that some researchers use convolutional neural network to model the sentences with the aim of improving the accuracy of sentence similarity computation. The authors of [16] proposed convolutional neural network models for matching two sentences by adapting the convolutional strategy in vision and speech. Hua He et al. [15] adopted convolutional neural networks to model the sentences from the multiple perspectives. They compared the proposed sentence representations at several granularities using multiple similarity metrics. The authors of [17] used convolutional neural network to compute the sentence semantic similarity. This work proposed a parallel convolutional neural network model. The model not only represents a single sentence in a sentence pair as a sentence vector, but also does similarity measurement of sentences after convolution pooling. Finally, they evaluate the proposed method using two different textual similarity related tasks.

2.2 The Regulation-Based Methods

From the perspective of syntax, there are a number of literature on sentence similarity computation. In literature, the authors proposed a method that based on semantic dependency relationship analysis to calculate sentence similarity, this method took advantage of semantic level and dependency syntactic level to measure the sentence similarity, and achieved satisfactory experimental results. The authors of [18] proposed a similarity measure based on manually-crafted lexico-syntactic patterns, the proposed method was evaluated on five ground truth datasets and on the task of semantic relation extraction, and achieved comparable performance without requiring semantic resources. Xiong et al. [7] investigated the various characteristics of dependency syntactic tree including word, the part-of-speech (POS) of word and the dependency type, this paper presented a similarity computation method between two dependency relationship triples which is made up of dominant, dependent and dependency type. The proposed sentence similarity computation method is based on the comprehensive analyzing of all these features, and the experimental results indicated that the sentence similarity computation method based on dependency syntactic tree is more comprehensive and accurate.

From the perspective of semantic, some researchers employ the syntactic and semantic analysis to compute the sentence similarity. The most representatives of these studies are as follows. The authors of [8] introduced a novel method of sentence similarity computation by incorporating the semantic information and syntactic information into the computing process. This paper firstly obtained the semantic information from a structural lexical database and corpus statistics, secondly measured the word order similarity between two sentences according to their position of word appearance in each sentence, and finally combined semantic similarity and word order similarity so as to propose a new algorithm which is applied to the conversational agents. The authors of [9] proposed a

novel sentence similarity computation method by exploiting both syntactic and semantic features to measure their similarity.

2.3 The Hybrid Methods

There are a number of literature on sentence similarity computation from the perspective of sentence level. Li et al. [6] proposed an approach of sentence similarity computation with a hybrid method by combing knowledge and corpus based semantic similarity measures and word order based similarity measures. The proposed algorithm exploited WordNet and Brown corpus to calculate the semantic similarity, and took advantage of word similarity to improve the sentence similarity computation accuracy. Liu et al. [19] presented a novel method for sentence similarity computation which utilized the semantic information, word order similarity, and the contributions of different part-of-speech in a sentence to calculate the sentence similarity. The experimental results on the selected sentence pairs indicated that the proposed method can improve the accuracy of sentence similarity computation.

For the sentence or short-text level, numerous methods have been proposed to address this issue. The authors of [11] presented a new method for measuring short-text and sentence semantic similarity. The proposed method captured and combined syntactic and semantic information to compute the semantic similarity between two sentences. Mihalcea et al. [12] proposed a hybrid unsupervised method that used two corpus-based metrics and six knowledge-based different metrics and combined the results to present a short-text similarity method. The weakness of this approach is that is utilized the eight different similarity methods, which causes the computational process inefficient. The authors of [13] introduced a semantic similarity measure for short-text based corpus and knowledge, and used different measures to calculate the word similarity, on the one hand, this paper exploited some relevant features of corpus-based semantic similarity to compute the sentence similarity, on the other hand, this paper described an approach based on the knowledge-based semantic similarity to perform the sentence similarity computation.

3 Coarse-Grained Sentence Similarity Computation

Generally, people obtain the meaning from a sentence on three aspects, including subject, predicate verb, and object. A general sentence consists of these three parts. We divided sentence pairs into several types according to their subjects, predicate verbs, and objects are the same or not. The types of sentence pattern is terms of subject, predicate verb, and object are the same or not are illustrated in Table 1. The lowest and highest columns are the lowest similarity values and the highest similarity values according to the human judgement similarity values for 30 sentence pairs, respectively. Note that the process of computing the maximum and minimum values is as follows, this is a method of sentence similarity computation from coarse-grained perspective with the aim of obtaining an approximate interval for each sentence pair.

Table 1. The types of sentence pattern

Type	Subject	Predicate	Object	Lowest	Highest
Case1	Same	Same	Same	0.348	0.955
Case2	Same	Same	Different	0.293	0.773
Case3	Same	Different	Same	-	-
Case4	Same	Different	Different	-	-
Case5	Different	Same	Same	0.063	0.283
Case6	Different	Same	Different	0.005	0.405
Case7	Different	Different	Same	-	-
Case8	Different	Different	Different	0	0.36

Step 1: Extract the subjects, verbs, and objects from the standard benchmark dataset which is comprised of 30 sentence pairs constructed by Li et al. [6] using the same method that presented in literature [20].

Step 2: Here each sentence may contain one or several of subjects, only one predicate verb, and one or several of objects. As long as any pair of subjects is the same or their similarity value is more than a predefined threshold (here we use 0.8), we consider their subjects are the same, otherwise different. The objects of two sentences are the same or different is also determined in the same way. In this step, we determined the type of sentence pattern for each sentence pair according to their subjects, predicate verbs, and objects are the same or not.

Step 3: Through the statistics of these values from 30 sentence pairs, we can obtain the maximum and minimum values for each sentence pair, and these values are obtained from the training dataset that consists of 30 sentence pairs which constructed by Li et al. [6].

Note: The mark ‘-’ in Table 1 denotes that there is not this situation in these sentence pairs in the standard benchmark dataset.

4 Fine-Grained Sentence Similarity Computation

In this section, we use the Stanford Parser to obtain the grammatical relation triples and compute the syntactic similarity and semantic similarity between two sentences; this is a method of sentence similarity computation from a fine-grained perspective. The Stanford Parser is a lexicalized dependency parser based on Probabilistic Context Free Grammar (PCFG). We can express the structure of a sentence as two forms in dependency grammatical theory, one is the syntactic tree and the other is the set of dependency relationships. Here we use the set of dependency relationships to represent the syntactic structure of the sentence.

Table 2. The set of dependency relationships returned by Stanford Parser

No.	Dependency relation
1	nsubj(like-2, I-1)
2	root(ROOT-0, like-2)
3	amod(technique-6, natural-3)
4	nn(technique-6, language-4)
5	nn(technique-6, process-5)
6	dobj(like-2, technique-6)

Table 3. The set of dependency relationships using their POS tags

No.	Dependency relationship
1	nsubj(VBP, PRP)
2	root(ROOT, VBP)
3	amod(NN, JJ)
4	nn(NN, NN)
5	nn(NN, NN)
6	dobj(VBP, NN)

4.1 Dependency Relationship Triples Extraction

We use the Stanford Parser to obtain the set of dependency relationships from each sentence. Each of dependency relationship is composed of three parts including the relationship type, the dominant and the dependent. For instance, the set of dependency relationships for the sentence *I like the natural language process technique.* is illustrated in Table 2.

For the sake of computing syntactic similarity between two sentences, we use the Part-Of-Speech (*POS*) of the word to substitute for the specific word. This paper adopts Stanford Tagger to perform the *POS* annotation, and obtain the set of dependency relationships expressed by their *POS* as illustrated in Table 3.

4.2 Syntactic Similarity Computation

Let the set of dependency relationships derived from sentence A be $A = \{a_1, a_2, \dots, a_n\}$, let the set of dependency relationships derived from sentence B be $B = \{b_1, b_2, \dots, b_m\}$. Where a_i represents the each of dependency relationship triple obtained from sentence A , b_j represents the each of dependency relationship triple obtained from sentence B .

Before calculating the similarity of two sets of dependency relationship triples, we must determine how to calculate the similarity between two dependency relationship triples. Here we calculate the similarity between two dependency relationship triples only when their dependency relationship types are the

Table 4. The cases of similarity computation between two dependency relationship triples

No.	POS	Dominant part	Dependent part	Similarity
1	Same	Same	Furlan2011Comparable same	1.0
2	Same	Same	Different	0.5
3	Same	Different	Same	0.5
4	Same	Different	Different	0
5	Different	*	*	0

same, otherwise we set the similarity value to 0. When their dependency relationship types are the same, we assign equal weights to both the dominant part and the dependent part. When their *POS* are the same, the similarity value between two *POS* parts is set to 1, otherwise the similarity value is set to 0. In this manner, the similarity between two dependency relationship triples can only be 1, 0.5 or 0. All of the cases for similarity computation between two dependency relationship triples are illustrated in Table 4.

Based on the similarity computation method between two dependency relationship triples, we can define the syntactic similarity between two sets of dependency relationship triples by Eq. (1).

$$Sim(a_i, B) = \max_{1 \leq j \leq m} Sim(a_i, b_j) \quad (\forall b_j \in B) \quad (1)$$

$$Sim(A, b_j) = \max_{1 \leq i \leq n} Sim(a_i, b_j) \quad (\forall a_i \in A) \quad (2)$$

The similarity values between two dependency relationship triples are given in Table 4. Therefore, we can calculate the syntactic similarity between two sentences using the formula (2).

4.3 Semantic Similarity Computation

In order to measure the semantic similarity between two sentences, we mainly concentrate on the similarity of semantic kernels for two sentences. The authors of [20] proposed a semantic kernel based approach which based on the assumption that the sentence meaning can be expressed in terms of its semantic kernels, they expressed each sentence as several subjects, verbs and objects. In our work, we divided each sentence into several of dependency relationship triples returned by Stanford Parser, and through computing the similarity between two set of typed dependency relationship triples, proposed a semantic kernel for measuring the semantic similarity between two compared sentences.

In this work, we use the Stanford Parser to parse each sentence into a series of dependency relationship triples which denoted by $S = \{T_1, T_2, \dots, T_n\}$, where S denotes the sentence, T_i denotes the i -th typed dependency relationship triple for the sentence S , n denotes the number of dependency relationship triples,

Table 5. The unimportant dependency relationship type lists

No.	Type abbreviation	Type name
1	det	determiner
2	expl	expletive
3	goeswith	goes with
4	possessive	possessive modifier
5	preconj	preconjunct
6	predet	predeterminer
7	prep	prepositional modifier
8	punct	punctuation
9	ref	referent

$T_i = \{g^i, t^i, d^i\}$, where g^i denotes the governor of the i -th typed dependency relationship triple for the sentence S , t^i denotes the type of the i -th typed dependency relationship triple for the sentence S , d^i denotes the dependent of the i -th typed dependency relationship triple for the sentence S . The computing procedure of semantic similarity between two typed dependency relationship triples can be described as follows.

Step 1. We first filter the unimportant dependency relationship types which lists in Table 5, the unimportant dependency relationship type lists are constructed by referring to the literature [4].

Step 2. We use an Improved Approximate Semantic Kernel (*IASK*) to compute the semantic similarity between two typed dependency relationship triples. The semantic similarity between two typed dependency relationship triples can be defined as:

$$\text{sim}(S_1^i, S_2^j) = \{\alpha \times s(g_1^i, g_2^j) + \beta \times s(d_1^i, d_2^j)\} \times q(t_1^i, t_2^j) \quad (3)$$

Where $\text{sim}(S_1^i, S_2^j)$ denotes the similarity between two triples S_1 and S_2 , α and β are two balance coefficients to adjust the weights of two parts $s(g_1^i, g_2^j)$ and $s(d_1^i, d_2^j)$, and they must satisfy the equation $\alpha + \beta = 1.0$. s is a function of semantic similarity between two English words, according to the literature [21], The Wu and Palmer’s algorithm is becoming a standard measure of similarity. Therefore, we adopt Wu and Palmer’s method [22] to evaluating semantic similarity between words. The formula as follows:

$$s(w_1, w_2) = \frac{2 * LCS^{depth}}{w_1^{depth} + w_2^{depth} + 2 * LCS^{depth}} \quad (4)$$

Where LCS denotes the Least Common Subsumer of w_1 and w_2 , LCS^{depth} denotes the number of nodes from LCS to the root node, w_1^{depth} and w_2^{depth} respectively represent the number of nodes on the path of the LCS .

q is a binary function:

$$q(a, b) = \begin{cases} 1 & \text{if } (a = b) \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

Based on the formulas (3), (4) and (5), we define the Improved Approximate Semantic Kernel (*IASK*) as follows:

$$IASK(S_1, S_2) = \frac{\sum_{i=1}^m \max_{1 \leq j \leq n} \{sim(T_1^i, T_2^j)\} + \sum_{j=1}^n \max_{1 \leq i \leq m} \{sim(T_1^i, T_2^j)\}}{m + n} \quad (6)$$

Step 3. We compute the semantic similarity between two sentences by using the *IASK* kernel function. The semantic similarity between two sentences can be computed by Formula 7.

$$Sem(S_1, S_2) = IASK(S_1, S_2) \quad (7)$$

5 The Overall Sentence Similarity Computation

Based on the coarse-grained sentence similarity computation and fine-grained sentence similarity computation, the coarse-grained sentence similarity computation determines the interval of sentence pair according to the types of sentence pattern for the sentence pair, the fine-grained sentence similarity computation determines the accurate similarity value based on the syntactic similarity computation and semantic similarity computation. The overall sentence similarity computation formula can be defined as follows:

$$SS(S_1, S_2) = lowest + \{highest - lowest\} \times \{\alpha \times Syn(S_1, S_2) + (1 - \alpha) \times Sem(S_1, S_2)\} \quad (8)$$

Where $SS(S_1, S_2)$ represents the overall sentence similarity between sentence S_1 and S_2 , *lowest* and *highest* represent the lowest and highest similarity values according to the type of sentence pairs, respectively. $Syn(S_1, S_2)$ and $Sem(S_1, S_2)$ represent the syntactic similarity and semantic similarity between two sentences S_1 and S_2 , respectively. α represents the balance coefficient to determine the contributions of syntactic similarity and semantic similarity. In our work, we set $\alpha = 0.35$ according to the study of literature [21].

6 Experimental Results and Analysis

In this section, we first describe the dataset, which used for measuring our method and the other methods, and then give the experimental results and analysis regarding to our method.

6.1 Datasets

We evaluate the proposed method of sentence similarity computation using two different datasets. The first dataset is the preliminary benchmark dataset which constructed by Li et al. [6], the author of [6] extracted 30 pairs of nouns from 65 pairs of nouns which presented in literature [23], and translated these 30 pairs of nouns into 30 pairs of sentences using the Collins Cobuild Dictionary, only these 30 pairs of sentences are considered relevant for sentence similarity measurement purpose. We used the Pearson’s correlation coefficient (r) to evaluate the proposed method compared with other state-of-the-art sentence similarity methods. The second dataset is some of sentence pairs which extracted from the Microsoft Research Paraphrase corpus (*MSRP*) [24] which is a part of the SemEval 2012 competition dataset [25]. The *MSRP* dataset consists of 4076 pairs of training sentences and 1725 pairs of testing sentences, and each sentence pair is assessed by two people to determine whether the two sentences convey the same meaning or not. We randomly select four positive and four negative pairs of sentences and calculate their similarity using out proposed method to validate our method.

6.2 Experimental Results and Analysis

To evaluate the performance of the proposed method, two experiments are designed with an aim to validate the proposed method in two different applications. The first experiment aims to evaluate the accuracy of sentence similarity computation. The second experiment aims to assess the performance of judging two sentences whether have the same meanings.

Experiment 1: In order to evaluate our method against the other state-of-the-art approaches described in literature [26] on benchmark dataset, we used the Pearson’s correlation coefficient between each method and human judgement as well as the mean deviation from the human judgement to perform the comparison. LSS [27] is a method of sentence similarity which utilize WordNet as lexical database to determine the word semantic similarity, and it is capable of identifying highly similar meanings regard of their details. Latent Semantic Analysis (LSA) is one of the most used in the literature [28] which is based on the statistical computing and singular value decomposition techniques. The method of Sentence Similarity based on Semantic Nets and Corpus Statistics is denoted by *STASIS* is presented by literature [6], this method use the word order similarity and word semantic similarity to measure the overall sentence similarity. Omiotis [29] is another sentence similarity computation method based on WordNet, it can deal with synonymy and polysemy issues due to its capability of semantic similarity. STS [5] is an modified version of the Longest Common Sub-sequence (*LCS*) string matching algorithm, it is considered to be the most accurate algorithm in terms of proximity to human judgement. Le et al. [30] proposes a model based on attention of Constituency Vector tree (ACV-tree) to analyze the sentence similarity. In addition to the syntactic structure and semantic relationship of the sentence, the model also adds the weight information of words in the sentence to

Table 6. The comparison of six methods on standard benchmark dataset

SP	Human	LSS	STASIS	LSA	Omiotis	STS	SS
1	0.010	0.180	0.329	0.510	0.1062	0.06	0.0399
5	0.005	0.198	0.287	0.530	0.1048	0.11	0.0683
9	0.005	0.280	0.209	0.505	0.1046	0.07	0.0329
13	0.108	0.166	0.530	0.535	0.3028	0.16	0.0682
17	0.063	0.324	0.356	0.575	0.2988	0.26	0.1353
21	0.043	0.324	0.512	0.530	0.2430	0.16	0.1014
25	0.065	0.220	0.546	0.595	0.2995	0.33	0.1274
29	0.013	0.220	0.335	0.505	0.1074	0.12	0.0677
33	0.145	0.324	0.590	0.810	0.4946	0.29	0.0820
37	0.130	0.280	0.438	0.580	0.1085	0.20	0.0920
41	0.283	0.324	0.428	0.575	0.1082	0.09	0.1066
47	0.348	0.198	0.721	0.715	0.2164	0.30	0.4567
48	0.355	1.000	0.641	0.615	0.5295	0.34	0.4210
49	0.293	1.000	0.739	0.540	0.5071	0.15	0.3872
50	0.470	0.800	0.685	0.675	0.5502	0.49	0.4877
51	0.138	0.800	0.649	0.725	0.5026	0.28	0.0952
52	0.485	1.000	0.493	0.695	0.5987	0.32	0.3055
53	0.483	0.471	0.394	0.830	0.4965	0.44	0.3972
54	0.360	0.800	0.517	0.610	0.4255	0.41	0.0454
55	0.405	0.800	0.550	0.700	0.4287	0.19	0.0728
56	0.588	0.800	0.759	0.780	0.9308	0.47	0.3828
57	0.628	1.000	0.700	0.750	0.6120	0.26	0.3740
58	0.590	0.800	0.753	0.830	0.7392	0.51	0.5604
59	0.863	1.000	1.000	0.985	0.9982	0.94	0.8643
60	0.580	0.800	0.663	0.830	0.9309	0.60	0.4332
61	0.523	0.800	0.662	0.630	0.3466	0.29	0.3746
62	0.773	1.000	0.729	0.740	0.7343	0.51	0.5179
63	0.558	1.000	0.639	0.870	0.7889	0.52	0.4477
64	0.955	1.000	0.998	1.000	0.9291	0.93	0.9284
65	0.653	1.000	0.831	0.860	0.8194	0.65	0.3597

the leaf node of the tree, which makes the model more similar to human thinking manner. The author [31] uses word embedding to generate the three-dimensional vector of sentences as the input of convolutional neural network (CNN), which makes the model well extract the grammatical and semantic information of sentences. Compared with the other models mentioned in the paper, only Le and Yao considered the semantic and syntactic information of the sentence as well

as our work. Therefore, we deliberately compare Pearson’s performance of the three models in Fig. 1. We denote our proposed method by *SS*, the similarity values of sentence pairs are listed in Table 6, the correlation of the compared methods to human judgement is illustrated in Fig. 1, the mean deviation of the compared methods from human judgement is illustrated in Fig. 2.

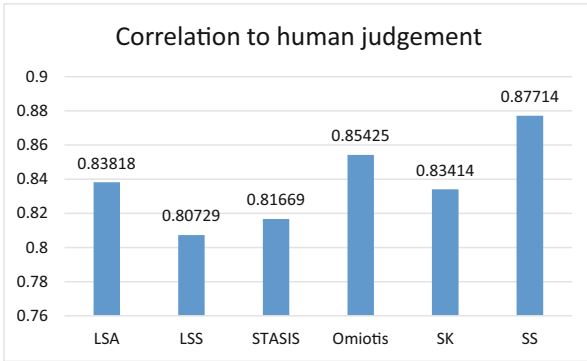


Fig. 1. The correlation of the compared six methods

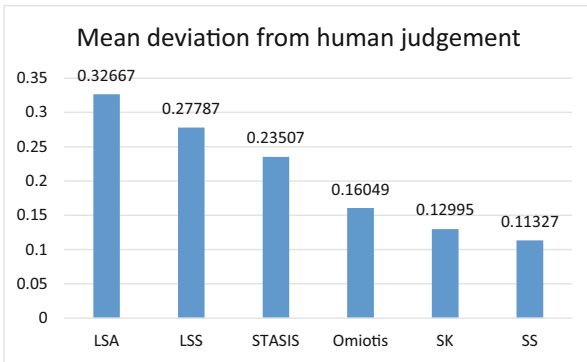


Fig. 2. The mean deviation of the compared six methods

From the Table 6, it can be seen that the similarity values of sentence pairs are in accordance with the human judgement similarity values due to the fact that our method use the type of sentence pair to determine the maximum and minimum similarity value between each sentence pair. The proposed method can guarantee that the calculated similarity value can further converge to the human judgement similarity, therefore the computing results are more close to the human judgement.

As illustrated by Fig. 1, the correlation of our method denoted by *SS* with the human judgement reaches to 0.87714, which is the best method in the compared six methods. Due to our method take into account of the syntactic and semantic kernel in computing the sentence similarity, furthermore, using the type of sentence pair to further make the calculated similarity value close to human judgement similarity value so as to improve the sentence similarity accuracy.

As illustrated by Fig. 2, our method *SS* can achieve the best results among the six methods in terms of mean deviation between each method and human judgement similarity. The main reason is that syntactic and semantic kernel make contributions to the sentence similarity computation, moreover, the type of sentence pairs can helpful to further amend for improving the sentence similarity

Table 7. The selected eight sentence pairs

No.	Sentence pair
1	“Amrozi accused his brother, whom he called the witness; of deliberately distorting his evidence.” “Referring to him as only the witness; Amrozi accused his brother of deliberately distorting his evidence”
2	“They had published an advertisement on the Internet on June 10, offering the cargo for sale, he added.” “On June 10, the ship’s owners had published an advertisement on the Internet, offering the explosives for sale”
3	“The stock rose \$2.11, or about 11%, to close Friday at \$21.51 on the New York Stock Exchange.” “PG& E Corp. shares jumped \$1.63 or 8% to \$21.03 on the New York Stock Exchange on Friday”
4	“Revenue in the first quarter of the year dropped 15% from the same period a year earlier.” “With the scandal hanging over Stewart’s company, revenue the first quarter of the year dropped 15% from the same period a year earlier”
5	“Yucaipa owned Dominick’s before selling the chain to Safeway in 1998 for \$2.5 billion.” “Yucaipa bought Dominick’s in 1995 for \$693 million and sold it to Safeway for \$1.8 billion in 1998”
6	“That compared with \$35.18 million, or 24 cents per share, in the year-ago period.” “Earnings were affected by a non-recurring \$8 million tax benefit in the year-ago period”
7	“Gyorgy Heizler, head of the local disaster unit, said the coach was carrying 38 passengers.” “The head of the local disaster unit, Gyorgy Heizler, said the coach driver had failed to heed red stop lights”
8	“Rudder was most recently senior vice president for the Developer & Platform Evangelism Business.” “Senior Vice President Eric Rudder, formerly head of the Developer and Platform Evangelism unit, will lead the new entity”

Table 8. The similarity values of eight sentence pairs extracted from MSRP corpus

Sentence pair	Equivalent	$Syn(S_1, S_2)$	$Sem(S_1, S_2)$	$SS(S_1, S_2)$
SP1	YES	0.6923	0.6875	0.6892
SP2	YES	0.4667	0.6638	0.5948
SP3	YES	0.2778	0.4024	0.3588
SP4	YES	0.7429	0.7423	0.7425
SP5	NO	0.0714	0.4157	0.2952
SP6	NO	0.2400	0.3554	0.3150
SP7	NO	0.3529	0.4444	0.4124
SP8	NO	0.0645	0.3380	0.2423

computation accuracy. The more our method is close to human judgement, the lesser the mean deviation is.

Experiment 2: Since sentence similarity computation strongly depends on the examined data. We randomly select four positive and four negative pairs of sentences from the Microsoft Paraphrase Corpus, adopt the proposed method to calculate the sentence similarity for each pair of sentences aim at demonstrating the feasibility and validity of our method. The goal of this experiment is to find some shortcomings of our method so as to improve it in the future works. The eight sentence pairs selected are shown in Table 7. The sentence similarity values are listed in Table 8.

For positive samples, we can observe that except for the sentence pair3, the sentence similarity values of the other three sentence pairs are more than 0.5. For positive sentence pair1, the syntactic structure and semantic information of the two sentences are very similar, therefore the syntactic similarity and semantic similarity between the two sentences are higher. For positive sentence pair2, the syntactic structure of the two sentences are not very similar, but the semantic information of the two sentences are very similar, the overall sentence similarity are very high. For positive sentence pair3, the syntactic structure and semantic information of the two sentences are lower according to the syntactic and semantic kernels, due to the fact that the two sentences contain several of different numbers which interfere with the syntactic and semantic kernel computation. For positive sentence pair4, not only the syntactic structure of two sentences are very similar, but also the semantic information of two sentences are very similar, moreover, both of two sentences contain the same number “15” to further increase the overall similarity.

For negative samples, we can observe that all of the sentence pairs obtain a relatively low similarity, due to these pairs express different meanings from each other. For negative sentence pair5, although they have several common words, their predicate verbs are different, one is “owned”, the other is “bought”, their different verbs make their relation types which returned by Stanford Parser

different, thus cause lower overall sentence similarity. For negative sentence pair6, all of their subjects, predicate verb, and objects are different each other, although they contain several of the same words such as “in the year-ago period”, the overall similarity of two sentences are still low. For sentence pair7, compared with sentence pair6, the number of common words of two sentences is more than sentence pair6, thus their overall similarity value is more than sentence pair6 similarity, but their objects are different each other, this situation cause the syntactic and semantic similarity of two sentences low. For sentence pair8, because their predicate verbs are different, both of syntactic similarity and semantic similarity are relatively low, and we obtain the overall similarity of 0.2423.

7 Conclusions and Future Works

This paper presents a novel method to compute the sentence similarities through imitating human thinking manner. We mainly use the Stanford Parser to obtain the Typed Dependency Relation Triples, use the types of sentence pattern to determine their maximum and minimum similarity values aim at approximately computing sentence similarity from a coarse-grained perspective, and measure their structure similarity by means of syntactic kernels and evaluate their semantic similarity by means of semantic kernels which utilize the Wu and Palmer similarity measure to calculate word similarity between two words from a fine-grained perspective. Experiment 1 has demonstrated that our method is better than the state-of-the-art methods in terms of Pearson’s correlation coefficient and mean deviation, Experiment 2 only use the syntactic and semantic kernels to compute the sentence similarity on part of MSRP corpus to validate our method is effective and feasible.

Our method of sentence similarity computation agrees with human intuition that firstly we determine if sentence pairs have the same sentence patterns, and give them a interval value, secondly determine their structure similarity and semantic similarity by means of syntactic and semantic kernels to obtain the more accurate similarity value. The limitation of our method is the overall similarity computation accuracy decreases with the increase of the number of their contained digital numbers, just as illustrated in sentence pair3 in Experiment 2. This shortcoming will be amended in our future work.

In the future, we intend to collect more information associated with the semantic or syntactic of the sentences. Based on these information, convolutional neural networks and recurrent neural networks are utilized in the process of sentence similarity computation.

Acknowledgments. This work is supported by “the Fundamental Research Funds for the Central Universities” of China University of Petroleum (East China) (Grant No. 18CX02139A), the Shandong Provincial Natural Science Foundation, China (Grant No. ZR2014FQ018). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

1. Rani, R., Tandon, S.: In: 2018 4th International Conference on Computing Sciences (ICCS) (2018)
2. Spaeth, A., Desmarais, M.C.: Combining collaborative filtering and text similarity for expert profile recommendations in social websites. In: Carberry, S., Weibelzahl, S., Micarelli, A., Semeraro, G. (eds.) UMAP 2013. LNCS, vol. 7899, pp. 178–189. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38844-6_15
3. Aliguliyev, R.M.: *Expert Syst. Appl.* **36**(4), 7764 (2009)
4. Ozates, S.B., Ozgur, A., Radev, D.R.: In: Language Resources and Evaluation Conference (2016)
5. Aminul, I., Diana, I.: *ACM Trans. Knowl. Discov.* **2**(2, article 10), 1 (2008)
6. Li, Y., Mclean, D., Bandar, Z.A., O’Shea, J.D.: *IEEE Trans. Knowl. Data Eng.* **18**(8), 1138 (2006)
7. Xiong, J., Liu, Y.T., Yuan, D.: *Inf. Technol. J.* **12**(20), 5685 (2013)
8. Li, Y., Bandar, Z., Mclean, D., O’Shea, J.: In: Seventeenth International Florida Artificial Intelligence Research Society Conference, Miami Beach, Florida, USA (2004)
9. Nguyen, H.T., Duong, P.H., Le, T.Q.: Springer (2015)
10. Kadupitiya, G.D.J., Ranathunga, S.: In: Proceedings of the 6th Workshop on South and Southeast Asian Natural Language Processing, pp. 44–53 (2016)
11. Oliva, J., Serrano, J.I., Del Castillo, M.D., Iglesias, A.: *Data Knowl. Eng.* **70**(4), 390 (2011)
12. Mihalcea, R., Corley, C., Strapparava, C.: In: National Conference on Artificial Intelligence and the Eighteenth Innovative Applications of Artificial Intelligence Conference, 16–20 July 2006, Boston, Massachusetts, USA, pp. 775–780 (2006)
13. Furlan, B., Sivavcki, V., Jovanovi, C.B., Nikoli, C.: *JITA - J. Inf. Technol. Appl. (Banja Luka) - APEIRON* **1**(1), 65 (2011)
14. Peiying, Z., Qiuming, L., Huayu, L.: *Int. J. Database Theory Appl.* **9**(10), 379 (2016)
15. He, H., Gimpel, K., Lin, J.: In: Conference on Empirical Methods in Natural Language Processing, pp. 1576–1586 (2015)
16. Hu, B., Lu, Z., Li, H., Chen, Q.: *Adv. Neural Inf. Process. Syst.* **3**, 2042 (2015)
17. Huang, J.P., Ji, D.H.: *Huanan Ligong Daxue Xuebao/J. S. China Univ. Technol.* **45**(3), 68 (2017)
18. Panchenko, A., Morozova, O., Naets, H.: pp. 174–178 (2012)
19. Liu, X., Zhou, Y., Zheng, R.: In: International Conference on Semantic Computing, pp. 250–256 (2007)
20. Amir, S., Tanasescu, A., Zighed, D.A.: *J. Intell. Inf. Syst.* 1–15 (2016)
21. Ming, C.L.: *Expert Syst. Appl.* **38**(5), 6392 (2011)
22. Wu, Z., Palmer, M.: In: Meeting on Association for Computational Linguistics, pp. 133–138 (1994)
23. Rubenstein, H., Goodenough, J.B.: *Commun. ACM* **8**(10), 627 (1965)
24. Dolan, B., Quirk, C., Brockett, C.: In: International Conference on Computational Linguistics, p. 350 (2004)
25. Agirre, E., Diab, M., Cer, D., Gonzalez-Agirre, A.: In: Joint Conference on Lexical and Computational Semantics, pp. 385–393 (2012)
26. O’Shea, J., Bandar, Z., Crockett, K., McLean, D.: A comparative study of two short text semantic similarity measures. In: Nguyen, N.T., Jo, G.S., Howlett, R.J., Jain, L.C. (eds.) KES-AMSTA 2008. LNCS (LNAI), vol. 4953, pp. 172–181. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78582-8_18

27. Croft, D., Coupland, S., Shell, J., Brown, S.: In: UK Workshop on Computational Intelligence, pp. 221–227 (2013)
28. Landauer, T.K., Foltz, P.W., Laham, D.: *Discourse Process*. **25**(2–3), 259 (1998)
29. Tsatsaronis, G., Varlamis, I., Vazirgiannis, M.: *J. Artif. Intell. Res.* **37**(4), 1 (2014)
30. Le, Y., Wang, Z.J., Quan, Z., He, J., Yao, B.: In: Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, IJCAI-18 (International Joint Conferences on Artificial Intelligence Organization), pp. 4137–4143 (2018). <https://doi.org/10.24963/ijcai.2018/575>
31. Yao, H., Liu, H., Zhang, P.: *Concurr. Comput. Pract. Exp.* **30**(1), e4415 (2018)



An Approach for Semantic Web Discovery Using Unsupervised Learning Algorithms

Yan Shen and Fangfang Liu^(✉)

School of Computer Engineering and Science, Shanghai University,
Shanghai 200444, China
ffliu@shu.edu.cn

Abstract. With the huge amount of available web services, it becomes increasingly difficult to find target web services for users accurately and effectively. For this reason, research in web service clustering has recently gained much attention. Most existing clustering methods perform well when dealing with long text documents. However, the textdescriptions of web services are in the form of short text. Meanwhile, it is meaningful to consider word order information in the textdescriptions of web services. Hence, we presented a service discovery approach based on web service clustering considering this issue. In our approach, web service discovery was divided into two parts: web service clustering and web service selection. In the process of web service clustering, the textdescriptions of web services were represented as vectors. In order to make vector representations reflect as much as possible the semantic information contained in the web service textdescriptions, we tried four different unsupervised sentence representations. In another part, LDA was used to mine topic semantic information of web services after user's web request was placed into a specific cluster according to its web service textdescription vector. The final efficiency of web service discovery was used to measure the effectiveness of our approach.

Keywords: Web service discovery · Web service description · Unsupervised learning algorithm · Web services clustering · Semantic information

1 Introduction

With the development of web technologies, the number of web services is increasing rapidly. Hence, finding suitable web services for users quickly and efficiently has become the content of many scholars. In recent years, the development of semantic web and machine learning algorithms have injected a lot of new vitality into the field of web service discovery [1–4]. Semantic web makes it possible to access web resources by content rather than just by keywords. OWL-S is a set of mark up language constructs that can be used to define properties and capabilities of web services in computer understandable way. It aims at providing an ontological description of web services to facilitate dynamic and automated discovery. Several machine learning algorithms have been applied in the field of web service discovery. However, it is still an open problem and can be further improved.

Using the definition of OWL-S language, each web service has a `textDescription` attribute, as shown in Fig. 1. This attribute offers the function of web service in the form of a sentence or short text, which provides a short but clear description of web service. The previous methods usually consider this attribute as a lexical vector or further introduce an external knowledge base to expand the lexical vector. However, the word order information in them is also important which contains rich semantic information.

Web service clustering [5] is an important step in web service discovery. A suitable method of web service clustering can improve the efficiency of web service discovery. The relevant web services are able to be returned to users if similar web services are placed into the same cluster. Most existing clustering methods perform well when dealing with long text documents. However, `textDescription` of web service is in the form of short text. In this paper, we attempt to represent the `textDescriptions` of web services as vectors for the purpose of more suitable web service clustering.

In this paper, we proposed an approach of semantic web service discovery which considered word order information in the `textDescription` of web service. The `textDescriptions` of web services were expressed as vectors which were used for web services clustering. These vectors not only contain the information of words, but also fully consider word order. We tried four different unsupervised vector representation methods to express the `textDescriptions` of web services. In our approach, web service discovery was divided into two parts: web service clustering and web service selection. In the process of web service clustering, `textDescriptions` of web services were first represented as vectors. And then these vectors were used to cluster web services by using K-means. In another part, LDA was applied to mine topic semantic information of web service request and each web service in cluster which was located in before. At last, the final web services were selected to be returned to user by calculating the similarity of their document-topic distribution. We measured the effectiveness of our approach through the final web service discovery. More details are shown in Sect. 4.

Our approach needs to answer two critical questions: (i) which unsupervised sentence representation methods are used to represent the `textDescriptions` of web services, and (ii) what these value of parameters should be, including cluster numbers, topic numbers in LDA and some similarity thresholds.

```
<profile:textDescription xml:lang="en">
This service is a recommended service to know about Heidelberg's, a
</profile:textDescription>
```

Fig. 1. `TextDescription` attribute of web service.

As to the first question, four different methods were used to represent `textDescriptions` of web services in our approach, including TF-IDF weighted `word2vec`, mean of `word2vec`, skip-thought and `doc2vec`. All of them are unsupervised sentence representation methods.

In terms of the second question, the best value of parameters, including cluster numbers, topic numbers in LDA and some similarity thresholds, were selected according to the final result of web service discovery. See more details in Sect. 5. Recall and Precision were used as evaluation metrics in our approach, which will be described in detail later.

In the reminder of this paper, we discuss related works in Sect. 2 and introduce some techniques used in our method in Sect. 3, including LDA model and the four different unsupervised sentence vector methods used in our paper. We describe the process of our web service discovery approach in detail in Sect. 4. And then we elaborate our experimental study in Sect. 5. The future work and conclusion are presented in Sect. 6.

2 Related Work

As mentioned before, web service clustering [6] is an effective solution to enhance the performance of web service discovery. Many researchers focus on web service clustering by applying various methods. There are a number of approaches proposed in recent years for web service clustering.

Some relevant works have been presented by using information retrieval techniques. Helmy et al. [7] proposed a text mining approach to automatically group services to specific domains and identify key concepts inside service textual documentation. Heyam et al. [8] presented an intensive investigation on the impact of incorporating feature selection methods (filter and wrapper) on the performance of four state-of-the-art machine learning classifiers. The purpose of employing feature selection is to find a subset of features that maximizes classification accuracy and improves the speed of traditional machine learning classifiers. Similarly, Elgazzar et al. [9] cluster web services based on content, types, messages, ports, and service name from WSDL documents. Approaches based on matrix factorization are also adopted to find relations between services and operations by co-clustering them since the duality relationship can help achieve better quality.

In order to enhance the accuracy of web services clustering, external knowledge and predefined ontologies are also applied in many existing works, which are utilized to compute the semantic similarity between Web services. More specifically, Pop et al. [10] proposed an approach of web services clustering by using an ant-based method based on semantic similarity. Du et al. [11] grouped web services into functionally similar service clusters by calculating semantic similarity with wordnet. Towards the sparseness of useful information in web services, Tian et al. [12] proposed a web service clustering approach based on transfer learning from auxiliary long text data obtained from Wikipedia. And they presented a topic model in order to handle the inconsistencies in semantics and topics between service descriptions and auxiliary data. Due to depend on ontologies and external knowledge, these approaches can accurately cluster services.

In addition, probabilistic topic model Latent Dirichlet Allocation (LDA) receives the attention of some scholars due to it can extract latent topic features of web services. Chen et al. [13] proposed an approach that integrated tagging data and WSDL

documents through augmented Latent Dirichlet Allocation (LDA). And further, three strategies were presented to preprocess tagging data before they were integrated into the LDA framework for clustering. Similar utilizing both WSDL documents and tags, Wu et al. [6] proposed a hybrid Web service clustering strategy which extracted five features from WSDL documents and computing the WSDL-level similarities and the tag-level similarities among Web services. WSDL-level similarity and tag-level similarity were combined into composite similarities for clustering Web services. Shi et al. [14] proposed an augmented LDA model using the high-quality word vectors which were obtained by Word2vec and then clustered into word clusters by K-means algorithm. These word clusters were integrated into the LDA training process. The results of experiment showed their approach had an average improvement of the clustering accuracy with metrics they used.

Zhao et al. [15] proposed a clustering method based on the heterogeneous service network model considering the relationship between service, user and provider for web service classification to improve the accuracy of service recommendation. Based on ontology and SVM, Rupasingha et al. [16] proposed a hybrid approach combining the summary of hybrid term similarity (HTS) and summary of context-aware similarity (CAS) methods to cluster WSDL files. SVM was used to calculate the semantic similarity in a generated ontology of web services. Liu et al. [17] used the Naive Bayes model to classify web services which can enhance service classification accuracy.

3 The Techniques Used in Our Method

3.1 Latent Dirichlet Allocation

Latent Dirichlet Allocation (LDA) [18] is a generative probabilistic model of a corpus based on Bayesian theory, which views documents as bags of words. In LDA [18], documents are represented as a set of latent topics, where each topic is characterized by a distribution over words. LDA [18] generates the distribution of word-document-topic and maps words and documents into a semantic space according to the analysis of the co-occurrence information of words. The training process of the LDA model combined with Gibbs sampling is shown in Fig. 2. The Gibbs sampling formula is shown in [18].

-
- 1: random initialization: randomly assign a topic number z to each word w in each document in the corpus.
 - 2: rescan the corpus, resample its topic according to the Gibbs sampling formula for each word w , and update it in the corpus.
 - 3: repeat the resampling process of the above corpus until the Gibbs sampling converges.
 - 4: the LDA model is the topic-word co-occurrence frequency matrix in the statistical corpus.
-

Fig. 2. The training process of the LDA model.

After the training process, the trained LDA model can be used to generate the distribution of topic for new documents following the steps of Fig. 3.

-
- 1: random initialization: randomly assign a topic number z to each word w in current document.
 - 2: rescan the corpus, resample its topic according to the Gibbs sampling formula for each word w .
 - 3: repeat the resampling process until the Gibbs sampling converges.
 - 4: obtain the topic distribution of current document.
-

Fig. 3. The inference process of the LDA model.

3.2 Word2vec

Word2vec [19] produces a distributed representation of words learned by two-layer neural networks. Word2vec takes a large amount of text as its input and produces a vector space, usually several hundred dimensions, in which each unique word in the corpus is assigned a corresponding vector. Word vectors are located in the vector space, which make words that share common context in the corpus very close to each other in the space. Two model architectures (CBOW and skip-gram) are proposed for learning continuous vector representations of words from huge data sets. In the CBOW architecture, the model predicts current word from a window of surrounding context words. In the skip-gram architecture, the model uses current word to predict surrounding window of the context word. For word2vec in our approach, we focus on the skip-gram architecture.

3.3 Doc2vec

Inspired by word2vec, doc2vec [20] is proposed to achieve phrase-level or sentence-level representations, which can consider the ordering of the words and semantics of the words. Doc2vec is an unsupervised framework that learns continuous distributed vector representations for pieces of texts. Two model architectures (PV-DM and PV-DBOW) are proposed for learning continuous vector representations of texts from huge data sets. The architecture of PV-DM is similar to the architecture of CBOW in word2vec. The only one change is the additional paragraph token that is mapped to a vector and can be thought of as another word. In PV-DM, the paragraph vector is concatenated with several word vector from a paragraph to predict the next word in the given many contexts sampled from the paragraph. Because paragraph vectors are learned from unlabeled data, they can work well for tasks that do not have enough labeled data. The architecture of PV-DBOW is also similar to the skip-gram model in word2vec. In PV-DBOW, the paragraph vector is used to predict the words from the text window.

3.4 Skip-Thought

Skip-thought [21] is an unsupervised learning approach of a generic, distributed sentence encoder. Combining the vocabulary expansion method proposed by [21], the off-the-shelf encoder is proposed to produce highly generic sentence representations. And further, the experimental result in [21] shows these generic sentence representations are

robust and perform well in practice. The skip-thought model is based on the skip-gram model in word2vec model, which encodes a sentence to predict the sentences around it instead of using a word to predict its surrounding context. A large collection of novels written by yet unpublished authors were used for training the skip-thought model. Three separate models including uni-skip, bi-skip and combine-skip were trained on dataset. The uni-skip model is an unidirectional encoder with 2400 dimensions and the bi-skip is a bidirectional model with forward and backward encoders of 1200 dimensions each. The combine-skip model consists of the concatenation of the vectors from uni-skip and bi-skip, having 4800 dimensions. After training on the dataset, the learned encoder was used as a feature extractor to extract skip-thought vectors for arbitrary sentences. Experiment shows that combine-skip is better than the uni-skip and bi-skip. Hence, we use the combine-skip model to learn the skip-thought vectors of the textdescriptions in web service.

4 Our Method

In this section, we introduce our web service discovery approach based on web service clustering considering word order information in the textdescriptions of web services. The architecture of our approach is shown in Fig. 4. As shown in Fig. 4, web service discovery is divided into two parts: web service clustering and web service selection. In the process of web service clustering, the owl-s web service documents are first parsed to get the textdescriptions of web services which provide a short but clear description of web services. And four different unsupervised sentence representations are used to represent the textdescriptions of web services, including TF-IDF weighted word2vec, mean of word2vec, skip-thought and doc2vec. TF-IDF is term frequency-inverse document frequency, which is a statistical measure used to evaluate how important a word is to a document in corpus. TF-IDF is composed by two terms: the normalized Term Frequency (TF) and the Inverse Document Frequency (IDF). The Term Frequency (TF) measures how frequently a term occurs in a document. The function of TF is defined as:

$$TF(t) = \frac{\text{Number of times term } t \text{ appears in a document}}{\text{Total number terms in the document}} \quad (1)$$

The Inverse Document Frequency (IDF) measures how important a term is. All terms in documents are considered equally important. As we all known, some terms, such as “am”, “are” and “that”, may appear a lot of times but have little importance. Hence, it is necessary to weigh down the frequent terms while scale up the rare ones. The function of IDF is defined as:

$$IDF(t) = \log \frac{\text{Total number of documents}}{\text{Number of documents with term } t \text{ in corpus}} \quad (2)$$

And the function of TF-IDF is defined as:

$$TF-IDF(t) = TF(t) * IDF(t) \tag{3}$$

After obtaining the representing vectors for the textdescriptions of web services, they are clustered using K-Means algorithm. And the clusters of web services are obtained at this stage. When a web service request coming, it can be quickly located in a particular service cluster by calculating the similarity of the vector of textdescription between web service request and cluster centers. In this way, web service selection can be performed only in the specific cluster, which can greatly reduce the selection space and improve the speed of overall web service discovery.

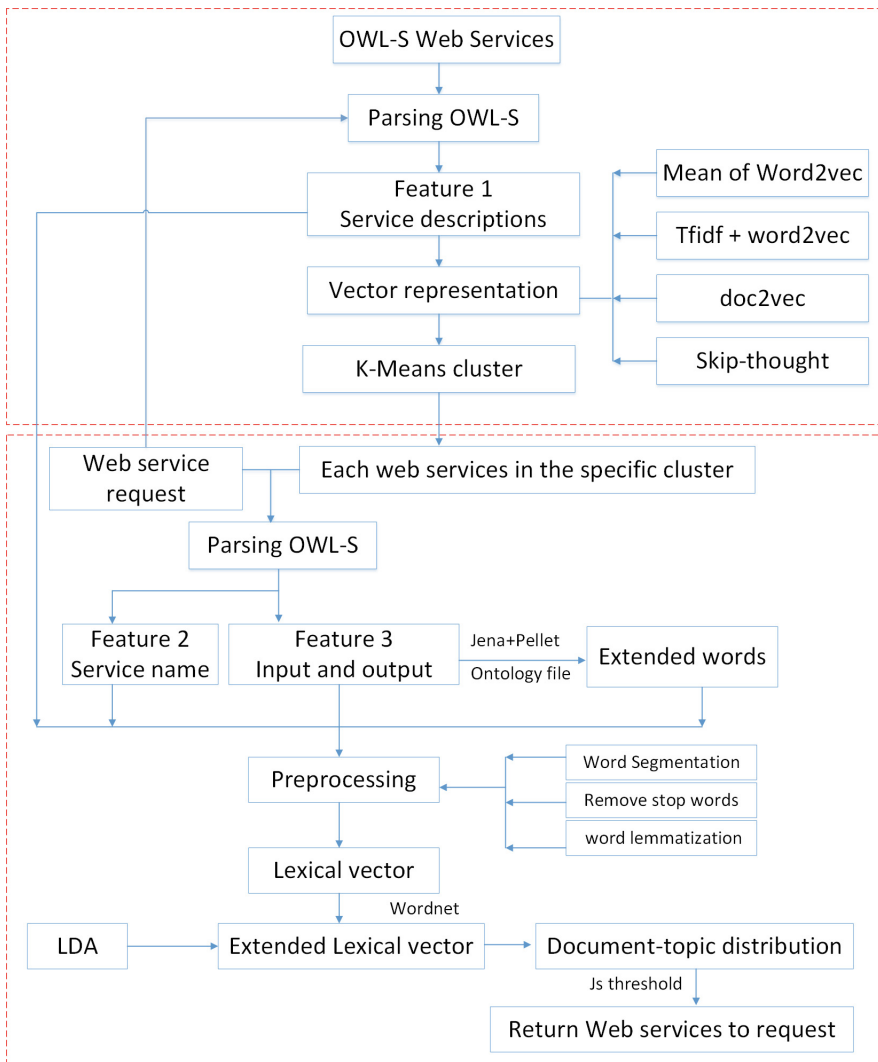


Fig. 4. The architecture of our approach

In the process of web services selection, the selection operation is performed only in the specific cluster. For all web services in the specific cluster, the owl-s web service documents are first parsed to get the information of service name, input and output. For input and output vocabularies, their parent class vocabularies, ancestor class vocabularies and subclass vocabularies are reasoned by using relevant ontology file. Service descriptions which are obtained in the process of web service clustering and service name undergo a series of pre-processing operations, including word segmentation, word lemmatization and removing stop words etc., to obtain the initial vocabulary vector. And then these initial vocabulary vectors are expanded by the wordnet dictionary, adding the top 10 vocabularies of each vocabulary. The expanded vocabularies, input vocabularies, output vocabularies, and the reasoned ontology vocabularies are combined to obtain the final lexical vector. LDA is used to mine topic semantic information according to the final lexical vector of web services in the specific cluster. Finally, we calculate the similarity of document-topic distribution between web service request and web services in the specific cluster. At last, some web services are returned to the web service request which meet a certain threshold.

5 Experiment

5.1 Experiment Data

OWLS-TC4 is the fourth version of the OWL-S service retrieval test collection which is intended to support the evaluation of the performance of OWL-S service match-making algorithms. OWLS-TC4 provides 1083 semantic web services and 42 test queries written in OWL-S 1.1 from nine different domains (education, food, medical care, economy, weapons, simulation, travel, geography and communication). The collection also provides ontology files used by web services and service requests. And all relevance sets created for OWLS-TC4 in test collection are available. These relevance sets are used to measure the effectiveness of our approach.

5.2 Evaluation Metrics

As mentioned before, web service discovery is divided into two parts: web service clustering and web service selection in our approach. In the process of web service clustering, we need to calculate the similarity between the vectors of web service textdescriptions and the similarity between web service requests and cluster centers. We use euclidean distance to measure this similarity. The euclidean distance between $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$ is defined as follows:

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \dots + (x_n - y_n)^2} \quad (4)$$

In the process of web services selection, LDA is used to mine topic semantic information. Hence, Jensen-Shannon (JS) is used to measure the similarity between the

document-topic distribution. The JS similarity between two probability distributions P_1 and P_2 is defined as follows:

$$JS(P_1||P_2) = \frac{1}{2}KL(P_1||\frac{P_1+P_2}{2}) + \frac{1}{2}KL(P_2||\frac{P_1+P_2}{2}) \quad (5)$$

And KL is defined as follows:

$$D_{KL}(P||Q) = \sum_{x \in X} P(x) \log \frac{P(x)}{Q(x)} \quad (6)$$

And for evaluation, we use Recall, Precision, F1 to measure the final web service discovery in our approach. These evaluation indicators are defined as follows:

$$Precision = \frac{TP}{TP + FP} \quad (7)$$

$$Recall = \frac{TP}{TP + FN} \quad (8)$$

$$F1 = \frac{2 * Precision * Recall}{Precision + Recall} \quad (9)$$

TP is true positive, FP is false positive, FN is false negative. They are elements in confusion matrix. For a binary classification problem, the confusion matrix can be obtained as shown in Table 1. As shown in Table 1, row represents predicted class and column represents actual class.

Table 1. Confusion matrix.

	Positive	Negative
True	True positive (TP)	True negative (TN)
False	False positive (FP)	False negative (FN)

5.3 Baselines

For our approach, it is important to make the vector representations reflect the semantic information contained in the web service text descriptions as much as possible. Hence, we measure the performance of the four unsupervised sentence representations (mean of word2vec, TF-IDF weighted word2vec, doc2vec and skip-thought) according to the efficiency of the final web service discovery.

5.4 Implementation

In our approach, K-Means and LDA methods are used to mine semantic information of web services. Hence, the value of some parameters is critical to the efficiency of the

final web service discovery, including cluster numbers, topic numbers in LDA, JS threshold and the parameter values of α and β in LDA. Some experiments were performed to select the optimal values of these parameters according to the efficiency of the final web service discovery. In these experiments, skip-thought was used to represent textdescriptions of web service as vectors. Next we will describe these experiments in detail.

Impact of Cluster Numbers (K). In our approach, K-Means is used to cluster vectors of web service textdescriptions. The number of clusters (K) is important for web service clustering and discovery. The best value of K was selected from 5 to 20 according to the efficiency of the final web service discovery. And other parameters were randomly set according to experience. The results are shown in Fig. 5. Obviously, Fig. 5 shows that the precision reach its highest point when the number of clusters K is 17. Therefore, we set K as 17 in our paper.

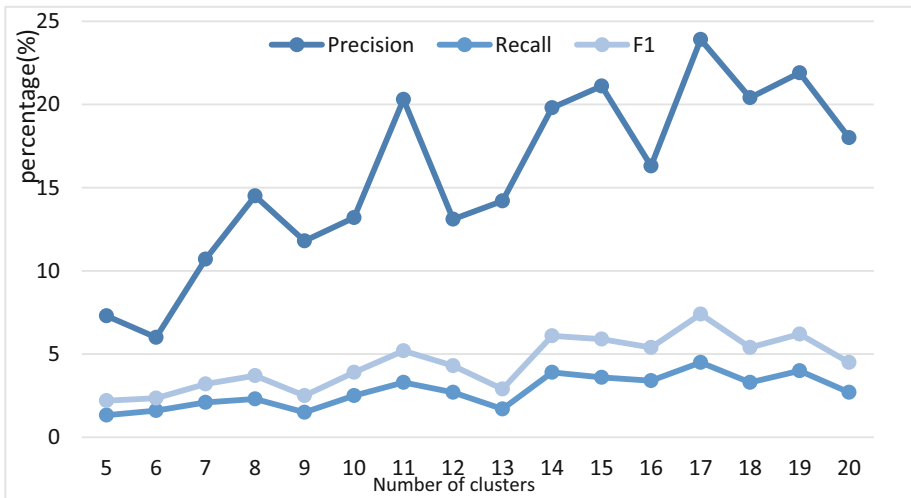


Fig. 5. The result with different cluster numbers (K).

Impact of Topic Numbers (T). In our approach, LDA is used to mine topic semantic information of web services after the user's web request is placed into the specific cluster. The number of topics (T) is important for LDA. The best value of T was selected from 10 to 20 when the number of clusters (K) was 17. And other parameters were randomly set according to experience. The results are shown in Fig. 6. Obviously, Fig. 6 shows that the Precision, Recall and F1 reach their highest point when the number of topics T is 15. Therefore, T was set as 15 in our paper.

Impact of JS Threshold. After the best value of T and K, the best value of JS threshold was selected among (0.01, 0.02, 0.03, 0.04, 0.05). The JS is used to measure the similarity of document-topic distribution between web service request and web services in the specific cluster. And further, web services which satisfy the JS thresh-

old are returned to user request. The results are shown in Fig. 7. As Fig. 7 shown, the performance of Precision, Recall and F1 are better than other values when JS is 0.04 though overall performance changes gently. Hence, JS threshold was set 0.04 in our paper.

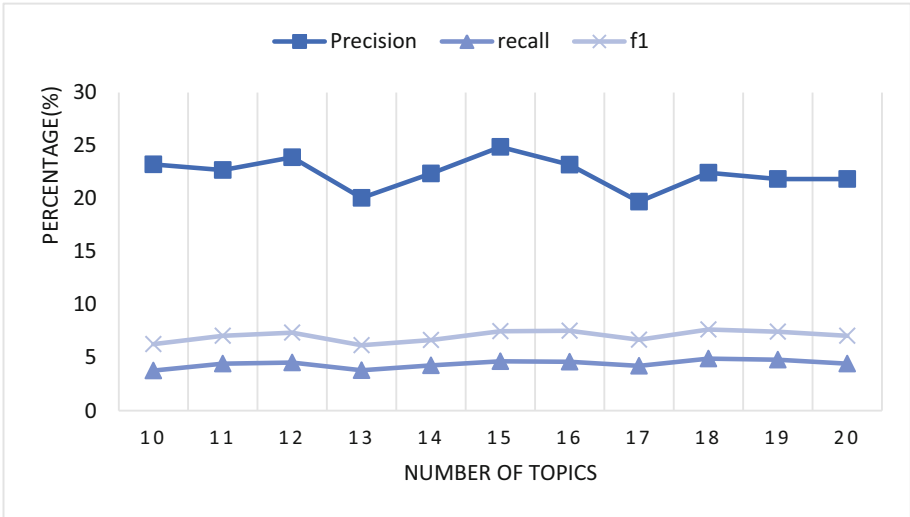


Fig. 6. The result with different topic numbers (T).

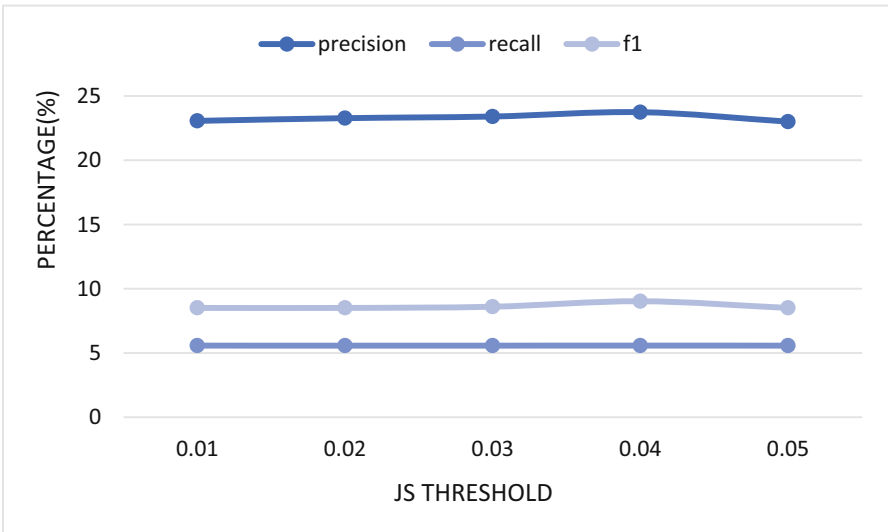


Fig. 7. The result with different JS threshold.

Impact of α and β in LDA. α and β are hyperparameters in LDA. α represents document-topic density and β represents topic-word density. The larger the α value, the more the document is composed of more topics. Similarly, the larger the β value, the more words make up the topic. Hence, the values of α and β are important for LDA. After the best value of T, K and JS threshold, the best value of α and β was selected among {1, 2, 3, 4} and the best value of β was selected among {0.4, 0.5, 0.6}. The results are shown in Fig. 8. As Fig. 8 shown, the precision reach their highest point when the α is 2 and β is 0.5. Therefore, we set α to 2 and set β to 0.5.

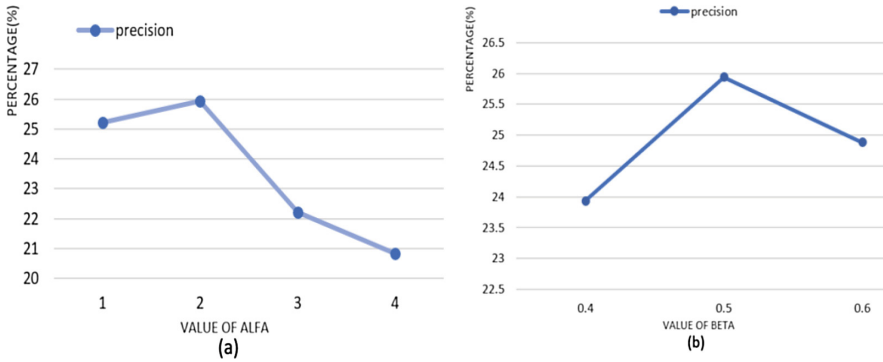


Fig. 8. The result with different α and β .

5.5 Results and Analysis of Web Service Discovery

We performed experiments in accordance with the procedure described in Fig. 4. After preprocessing web services, four different unsupervised sentence representations were used to represent the text descriptions of web services as vectors. And then K-Means algorithm was performed to cluster these vectors for web service selection. When facing a web service request, LDA was used to mine topic semantic information according to the final lexical vector of web services in the specific cluster. At last, some web services are returned to the web service request which meet a certain threshold. Results on experiments are demonstrated in Figs. 9, 10 and 11. We separately list the each value of Precision, Recall and F1 of the final web service discovery for 42 web service requests which are provided from data collection. The four different unsupervised sentence representations include mean of word2vec, TF-IDF weighted word2vec, doc2vec and skip-thought.

Figures 9, 10 and 11 show that the final performance of different web service requests fluctuates greatly. Although the Precision, Recall and F1 of some web service requests are very good, some web service requests have zero value. And all of the four unsupervised sentence representation methods have zero value. Obviously, the performance of web service discovery using skip-thought is the worst among four unsupervised methods. We believe that this generic sentence representation

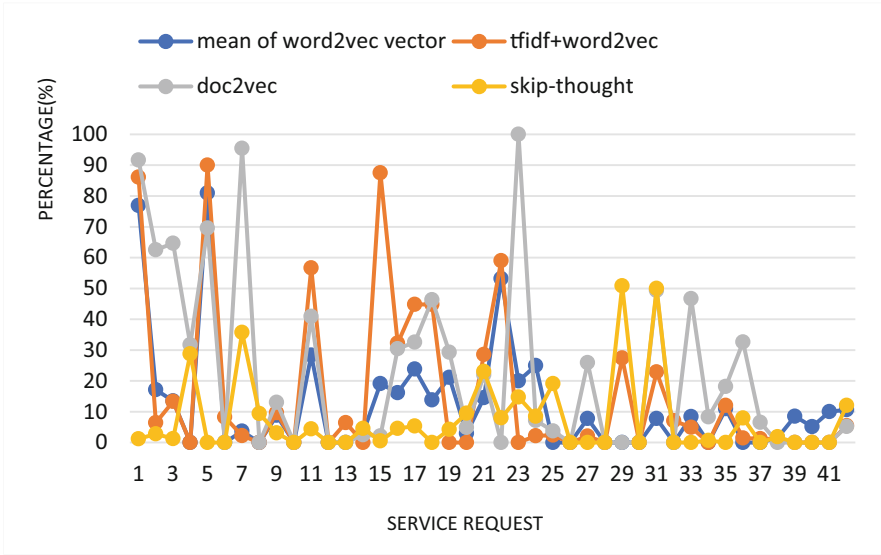


Fig. 9. The result of precision on web service discovery experiment.

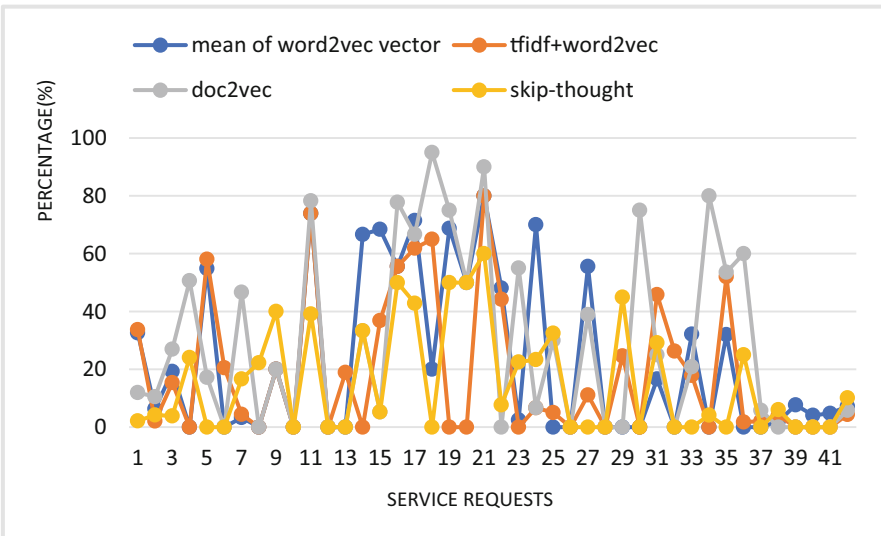


Fig. 10. The result of recall on web service discovery experiment.

skip-thought does not apply to the domain of web service. The skip-thought model was trained with a large collection of novels written by yet unpublished authors. Although vocabulary expansion method in skip-thought model can encode words that not seen as

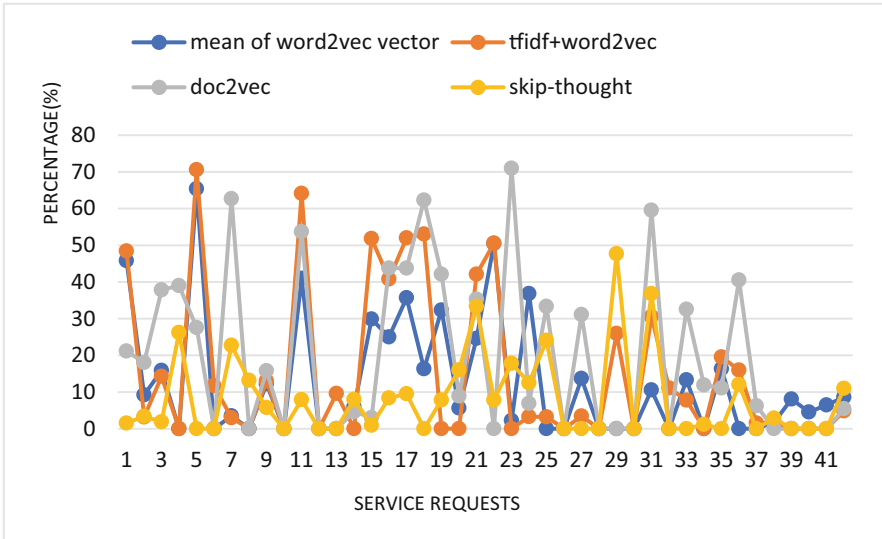


Fig. 11. The result of F1 on web service discovery experiment.

part of training. But the filed of novel and web services is quite different, which makes the vocabulary expansion method not effective. In addition to this, the performance of web service discovery using TF-IDF weighted word2vec is better than using word2vec. We believe that the TF-IDF method can highlight important words and make them have higher weights which are important for the expression of semantic information. We can see that the performance of web service discovery using doc2vec is the best among four unsupervised methods. Because the doc2vec method takes into account word order, the vector representations contain more semantic information than other methods.

In order to further analysis the experimental results, we select some different number of web service request subsets among 42 service requests and use average Precision, average Recall and average F1 to describe the final experimental results. We select four web service request subsets and the number of web service requests is 10, 14, 17, 19 respectively. There are duplicate web service requests in these subsets. Due to the performance of skip-thought is the worst, we only compare the remaining three methods (word2vec, doc2vec and TF-IDF weighted word2vec). Results are demonstrated in Fig. 12. The results shown in Fig. 12 are the same as those we summarized. The performance of web service discovery using doc2vec is the best. Meanwhile, the performance of web service discovery using TF-IDF weighted word2vec is better than using word2vec. Because the doc2vec method can capture the word order information of a sentence, while TF-IDF can highlight important words.



Fig. 12. Results of subsets with different web service requests.

6 Conclusion and Future Work

We proposed a web service discovery approach using unsupervised learning algorithms which is mainly divided into two parts: web service clustering and web service selection. In the process of web service clustering, the textdescriptions of web services are represented as vectors using four unsupervised sentence representation methods, including word2vec, TF-IDF weighted word2vec, doc2vec and skip-thought. Meanwhile, K-Means is used to cluster these vectors. In the process of web service selection, LDA is used to mine topic semantic information in a specific cluster when facing a web service request. At last, some web services are returned to the web service request which meet a certain threshold. In experiment, we selected the best value of K, T, JS threshold, α , β according to the final performance of web service discovery. And then we performed the experiment of whole web service discovery. The results indicate the performance of web service discovery using doc2vec is the best among TF-IDF weighted word2vec, doc2vec, word2vec and skip-thought. The performance of TF-IDF weighted word2vec is better than word2vec. The reason we analyzed is that doc2vec can capture the word order information of a sentence and TF-IDF can highlight important words. Meanwhile, the performance of web service discovery using skip-thought is the worst. The reason we analyzed is that the training data of skip-thought is mainly focus on novels rather than words in web service fields. Hence, this generic sentence representation model skip-thought model does not apply to the web service discovery.

In future, we will concentrate on reducing web service discovery time and discovering unsupervised sentence representations which are more suitable for web

services. Meanwhile, semantic web service described by owl-s also contains a lot of other information. In this paper, we only use the common information (service name, service description, input and output) in web services. Hence, we will focus on adding other useful information in web service to improve the efficiency of service discovery.

References

1. Mier, P.R., Pedrinaci, C., Lama, M.: An integrated semantic web service discovery and composition framework. *IEEE Trans. Serv. Comput.* **2015**, 537–550 (2015)
2. Cheng, B., Zhao, S., Li, C.: A web services discovery approach based on mining underlying interface semantics. *IEEE Trans. Knowl. Data Eng.* **29**(5), 950–962 (2017)
3. Fuzan, C., Chenghua, L., Harris, W.: A semantic similarity measure integrating multiple conceptual relationships for web service discovery. *Expert Syst. Appl.* **67**, 19–31 (2017)
4. Pawar, S., Chiplunkar, N.: Discovery and invocation of web services using multi-dimensional data model with WSDL. *Indian J. Sci. Technol.* **10**(17), 1–11 (2017)
5. Helmy, A., Salah, A.I., Geith, M.H.: Web services clustering approaches: a review. *IOSR J. Eng. (IOSRJEN)* **6**, 38–44 (2016)
6. Wu, J., Chen, L., Zheng, Z.: Clustering web services to facilitate service discovery. *Knowl. Inf. Syst.* **38**(1), 207–229 (2014)
7. Helmy, A., Geith, M.H.: An enhanced approach for web services clustering using supervised machine learning techniques. *Int. J. Sci. Eng. Res.* **1**(8), 158–170 (2017)
8. Albaity, H., Alshowiman, N.: Towards effective service discovery using feature selection and supervised learning algorithms. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* **10**(5), 191–200 (2019)
9. Elgazzar, K., Hassan, E., Martin, P.: Clustering WSDL documents to bootstrap the discovery of web services. In: *International Conference on Web Services*, pp. 147–154 (2010)
10. Pop, C.B., Chifu, V.R., Salomie, I., Dinsoreanu, M., David, T., Acretoae, V.: Semantic web service clustering for efficient discovery using an ant-based method. In: *Essaaidi, M., Malgeri, M., Badica, C. (eds.) Intelligent Distributed Computing IV. SCI*, vol. 315, pp. 23–33. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-15211-5_3
11. Du, Y., Zhang, Y., Zhang, X.: A semantic approach of service clustering and web service discovery. *Inf. Technol. J.* **12**(5), 967–974 (2013)
12. Tian, G., Wang, J., He, K.: Leveraging auxiliary knowledge for web service clustering. *Chin. J. Electron.* **25**(5), 858–865 (2016)
13. Chen, L., Wang, Y., Yu, Q., Zheng, Z., Wu, J.: WT-LDA: user tagging augmented LDA for web service clustering. In: *Basu, S., Pautasso, C., Zhang, L., Fu, X. (eds.) ICSOC 2013. LNCS*, vol. 8274, pp. 162–176. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-45005-1_12
14. Shi, M., Liu, J., Zhou, D.: WE-LDA: a word embeddings augmented LDA model for web services clustering. In: *International Conference on Web Services (ICWS)*, pp. 9–16 (2017)
15. Zhao, H., Wen, J., Zhao, J.: A new model-based web service clustering algorithm. In: *IEEE Region 10 Conference*, pp. 3468–3472 (2016)
16. Rupasingha, R., Paik, I., Kumara, B.: Calculating web service similarity using ontology learning with machine learning. In: *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1–8 (2015)
17. Liu, J., Tian, Z., Liu, P.: An approach of semantic web service classification based on naive bayes. In: *IEEE International Conference on Services Computing*, pp. 356–362 (2016)

18. Blei, D., Ng, A., Jordan, M.: Latent dirichlet allocation. *J. Mach. Learn. Res.* **3**, 993–1022 (2003)
19. Mikolov, T., Chen, K., Corrado, G.: Efficient estimation of word representations in vector space. In: *International Conference on Learning Representations*, pp. 1–12 (2013)
20. Le, Q., Mikolov, T.: Distributed representations of sentences and documents. In: *International Conference on Machine Learning*, pp. 1188–1196 (2014)
21. Kiros, R., Zhu, Y., Salakhutdinov, R.: Skip-thought vectors. In: *Advances in Neural Information Processing Systems*, pp. 3294–3302 (2015)



Direction-Aware Top- k Dominating Query

Xue Miao, Xi Guo, Aziguli Wulamu^(✉), and Zhaoshun Wang^(✉)

Beijing Key Laboratory of Knowledge Engineering for Materials,
University of Science and Technology Beijing, Beijing, China
xuemiao@xs.ustb.edu.cn, xiguo@ustb.edu.cn, 13911983933@163.com,
zhswang@sohu.com

Abstract. Traditional location-based services (LBSs) only consider the distance of the spatial object w.r.t the user. However, a spatial object has not only the distance attribute but also the direction attribute. In this paper, we propose a new spatial object query, i.e., the direction-aware top- k dominating query (DirDom query). Given a user's position and his favorite direction, the DirDom query finds the top- k objects with the highest dominant capabilities. The dominant capability of an object is the number of the objects it can dominate. An object can dominate another object if it is better considering both the distance and the direction. Here "better" means it is closer to the user and it is more consistent with the user's favorite direction. We design R-tree-based algorithms to answer DirDom queries. We evaluate the correctness and the efficiency of the algorithms by using real and synthetic datasets.

Keywords: Top- k dominating query · Direction-aware · Spatial queries · Location-based services

1 Introduction

The existing direction-aware spatial queries either find the nearest points of interests (POIs) in a specific direction range [3, 10–13, 15] or find the nearest POIs distributing around the user [1, 9, 14, 16]. Based on these existing work, we propose a new spatial query, i.e., the direction-aware top- k dominating query (DirDom query). The DirDom query recommends POIs according to the dominant capabilities of the POIs. Given the user's position and his favorite direction, if a POI p_i is closer to the user and it is more consistent with the user's favorite direction than another POI p_j , p_i dominates p_j . The number of POIs that p_i can dominate is the dominant capability of the POI p_i . The top- k POIs with the highest dominant capabilities are the query answers.

Example 1. There are some coffee shops around the user in Fig. 1. The user wants to buy a cup of coffee on his way home. The red arrow shows his favorite direction. The user wants to find the best three coffee shops that are closer to him

and more consistent with the direction towards home. As Fig. 1 shows, because coffee shops p_1 , p_2 and p_3 have the highest dominant capabilities, the DirDom query recommends them to the user. Details of all POIs are shown in the table in Fig. 1 and let's take p_1 as an example to explain the table. The distance from p_1 to q is 1.5 km and p_1 deviates from user's favorite direction by 3.2° , which is p_1 's direction deviation. The dominant capability of the POI p_1 is 17 and it is the highest among all POIs. The area dominated by p_1 is the shadow area in Fig. 1. There are 17 POIs in the shadow area, all of which are dominated by p_1 . POIs p_2 and p_3 aren't in the shadow area and their respective dominant capability is smaller than 17, so p_1 has the highest dominant capability.

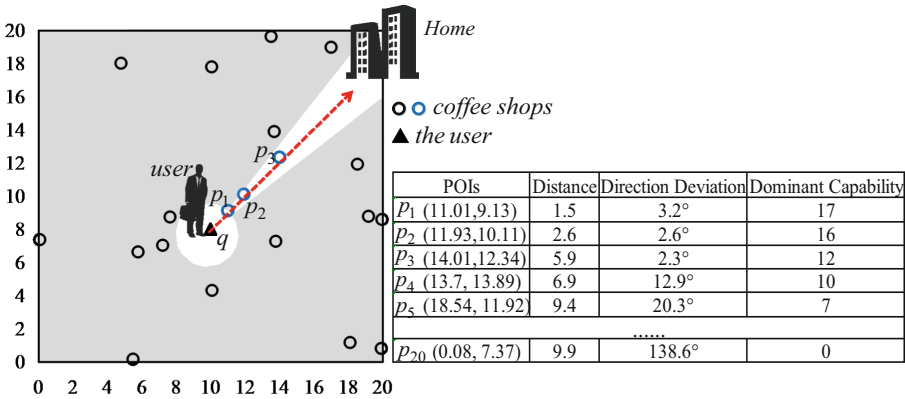


Fig. 1. Motivating example 1 (Color figure online)

The DirDom query has many applications. For example, in long-distance transportation, the driver can use the query to find the gas stations that are on his moving direction and closer to him. In computer games, the player can use the query to find nearby enemies that are on his shooting direction.

The contributions of this paper are listed below:

- We propose the DirDom query, which is a new direction-aware spatial query.
- We propose two R-tree-based algorithms to answer the query.
- We evaluate the performance of the algorithms on both synthetic and real datasets. The experimental results show that our algorithms can answer the query correctly and efficiently.

The rest of our paper is organized as follows. Section 2 summarizes our related work. Section 3 formally defines the DirDom query. Section 4.1 shows the baseline algorithm and Sect. 4.2 gives the algorithm of calculating the dominant capability. Sections 4.3 and 4.4 introduce two R-tree-based algorithms, respectively. Section 5 presents the experimental results.

2 Related Work

The existing direction-aware spatial queries are limited to find POIs in a specific direction range [3, 10–13, 15] and find the nearest POIs distributing around the user [1, 9, 14, 16]. The latter are direction-aware spatial skyline (DSS) queries. Borzsonyi et al. first propose the skyline queries [4] in 2001 and then the skyline queries are extended to the spatial skyline queries [5–8], which usually consider the distance attributes when retrieving spatial objects for users. We call these works the traditional spatial skyline (TSS). Different from the TSS queries, the DSS queries consider not only the distance attribute but also the direction attribute of the spatial object w.r.t. the user.

2.1 Direction-Aware Spatial Skyline

Guo et al. first propose the DSS queries in [1] and [9]. Considering the distance and the direction attributes of the spatial object, DSS query finds all objects that cannot be dominated by any other object from different directions around the user. In DSS query, two objects are in the same direction if their included angle w.r.t. the user is no more than a given angle threshold. *The object closest to the query point among all objects in the same direction can dominate the other objects in that direction.* This is different from the dominance relationship proposed in our DirDom query. In some cases, the results of the DSS queries have obvious low-directional diversity. On the basis of the DSS queries [1, 9], aiming at the limitation of the DSS queries, [16] makes an in-depth study of DSS queries. [16] proposes using the *directional zone* to measure the directional similarity of the spatial objects, which is different from [1] and [9]. Besides, Guo et al. in [14] propose the DNN query, which guarantees a better directional diversity of the query results.

2.2 Other Direction-Aware Spatial Queries

There are some other direction-aware spatial queries. [10] proposes the direction-aware spatial keyword search (DESKS), in which, Li et al. design a new direction-aware indexing structure to answer the DESKS. On the basis of [1, 10, 11, 13] design algorithms based on a grid structure to find the POIs that are constrained by the direction, the distance and the keywords. Besides, [3] proposes a snapshot and a continuous queries, which are all direction-aware spatial queries. [15] proposes the direction-constrained k nearest neighbor (DCNN) query. In the DCNN query, the spatial objects have their own orientations, which are different from the above queries.

2.3 Top- k Dominating Queries

The top- k objects that can dominate the largest number of objects in a dataset are the results of the top- k dominating query. Papadias et al. first put forward

the top- k dominating query in [17]. However, it is considered an extension of the skyline query, and the importance and practicability of the top- k dominating queries aren't realized. Later, some queries based on variants of the dominance relationship [19–22] are proposed. However, these queries cannot be directly applied to evaluate top- k dominating queries. Based on [17, 18] has an extensive study on the evaluation of the top- k dominating queries. Different from the previous top- k dominating queries, our DirDom query considers the direction attributes.

3 Preliminaries

In a two-dimensional Euclidean space, there is a user q and a set of POIs \mathcal{P} . The user q issues his position (x_q, y_q) and his favorite direction ω_q . Notice that a ray starting from (x_q, y_q) shows the user's favorite direction. To measure the direction, we use a polar coordinate system which has q as the reference point. The included angle between the ray and the reference direction is his favorite direction ω_q . Each $p_i \in \mathcal{P}$ has its distance ρ_i w.r.t. (x_q, y_q) and its direction deviation ϕ_i w.r.t. ω_q . The distance ρ_i is the Euclidean distance between p_i and (x_q, y_q) . The direction deviation ϕ_i is defined as follows.

Definition 1 (Direction Deviation). *The angular difference between ω_{p_i} and ω_q is the direction deviation ϕ_i of p_i .*

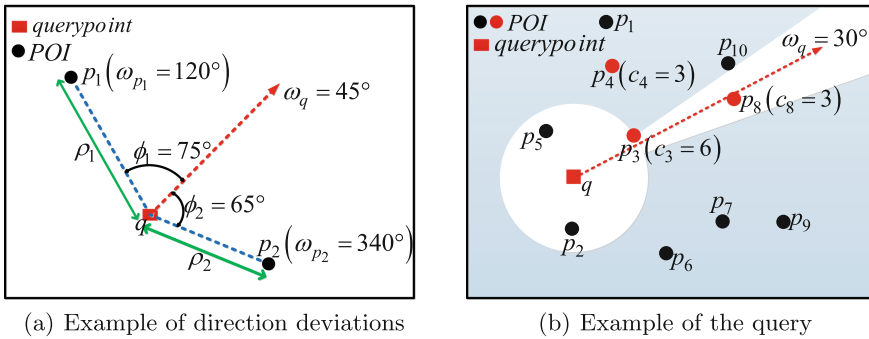


Fig. 2. Examples of the definitions (Color figure online)

As Fig. 2(a) shows, the red ray shows the user's favorite direction. The direction deviation of p_1 is $\phi_1 = 75^\circ$, which is the included angle between the red ray and \mathbf{qp}_1 . In the same way, the direction deviation of p_2 is $\phi_2 = 65^\circ$.

Definition 2 (Dominate). *A POI $p_i(\rho_i, \phi_i)$ dominates another POI $p_j(\rho_j, \phi_j)$, iff $\rho_i \leq \rho_j$ and $\phi_i < \phi_j$ or $\rho_i < \rho_j$ and $\phi_i \leq \phi_j$.*

We use symbol \prec to denote the dominance relationship. For example, in Fig. 2(a), since $\rho_2 < \rho_1$ and $\phi_2 < \phi_1$, p_2 can dominate p_1 ($p_2 \prec p_1$).

Definition 3 (Dominant Capability). *The dominant capability of p_i is the number of POIs which p_i can dominate.*

We use c_i to denote the dominant capability of p_i . We use P_i to denote all POIs dominated by p_i , i.e., $p_i \prec P_i$. For example, as Fig. 2(b) shows, p_3 can dominate $\{p_1, p_4, p_6, p_7, p_9, p_{10}\}$, because all of them are farther than p_3 and their direction deviations are larger than p_3 . We group these POIs into P_3 and we use $p_3 \prec P_3$ to denote the dominance relationships. Thus, the dominant capability of p_3 is 6, i.e., $c_3 = 6$.

Definition 4 (Direction-Aware Top- k Dominating Query). *Given a user's position (x_q, y_q) and his favorite direction ω_q , a direction-aware top- k dominating query (DirDom Query) finds the top- k POIs which have the highest dominant capabilities.*

We use (q, ω_q, k) to denote a DirDom query, where q is the user's position, ω_q is the user's favorite direction, k is the number of results recommended. As Fig. 2(b) shows, the results of the DirDom query $(q, 30^\circ, 3)$ is $\{p_3, p_4, p_8\}$, which has the highest dominant capabilities $c_3 = 6$, $c_4 = 3$ and $c_8 = 3$ Table 1.

Table 1. Symbols and descriptions

Symbols	Descriptions
ρ_i	p_i 's distance
ϕ_i	the direction deviation of p_i
ω_q	user's favorite direction
\prec	dominance relationship
c_i	p_i 's dominant capability

4 Direction-Aware Top- k Dominating Query

In this section, we propose the baseline algorithm to answer the DirDom query. Additionally, two R-tree-based algorithms are also designed to answer the query.

4.1 Baseline Algorithm

In the baseline algorithm, we compare each POI in the POIs set with all the other POIs. In the process of comparison, the dominant capability of each POI is recorded and the top- k POIs with the highest dominant capabilities will be found. At first, the list \mathcal{L} is empty and we think the dominant capability (c_i) of each POI (p_i) is 0. For each POI p_i in \mathcal{P} , we traverse every POI p_j in $\mathcal{P} - \{p_i\}$.

Algorithm 1. Baseline Algorithm

```

Input:  $q, \omega_q, k, \mathcal{P}$ 
Output: The top- $k$  objects with the highest dominant capabilities
1 for  $p_i$  in  $\mathcal{P}$  do
2    $c_i \leftarrow 0$ 
3   for  $p_j$  in  $\mathcal{P} - \{p_i\}$  do
4     if  $p_i \prec p_j$  then
5        $c_i + = 1$ 
6   if  $|\mathcal{L}| \leq k$  then
7      $\text{add}(p_i, c_i)$  to  $\mathcal{L}$ 
8   else
9      $(p_{min}, c_{min}) \leftarrow$  POI with the minimum dominant capability in  $\mathcal{L}$ 
10    if  $c_{min} < c_i$  then
11       $\text{remove}(p_{min}, c_{min})$  from  $\mathcal{L}$ 
12       $\text{add}(p_i, c_i)$  to  $\mathcal{L}$ 

```

Based on the Definition 2, if p_i dominates p_j , then the dominant capability (c_i) of p_i increases by one (Lines 4 and 5). After the inner **for** loop, p_i 's dominant capability c_i is calculated. If the number of the elements in \mathcal{L} is smaller than k , we add (p_i, c_i) to \mathcal{L} . Otherwise, we find an element (p_{min}, c_{min}) in the current list \mathcal{L} (Line 9). Of all the elements in \mathcal{L} , the dominant capability c_{min} of p_{min} is the minimum. If c_{min} is smaller than c_i , p_{min} must not be a result and p_i may be a result. Therefore, (p_{min}, c_{min}) will be removed from \mathcal{L} and (p_i, c_i) will be added to \mathcal{L} . After the outer **for** loop, \mathcal{L} stores the top- k POIs with the highest dominant capabilities.

Algorithm 1 compares each object in the dataset with all the other objects. When the number of POIs is very large, the baseline algorithm is time-consuming. Consequently, we propose efficient R-tree-based algorithms to answer the query.

4.2 Calculate Dominant Capability Fast

Each POI $p_i \in \mathcal{P}$ has a distance ρ_i and a direction deviation ϕ_i . According to p_i 's direction ω_{p_i} and the user's favorite direction ω_q , ϕ_i has three cases.

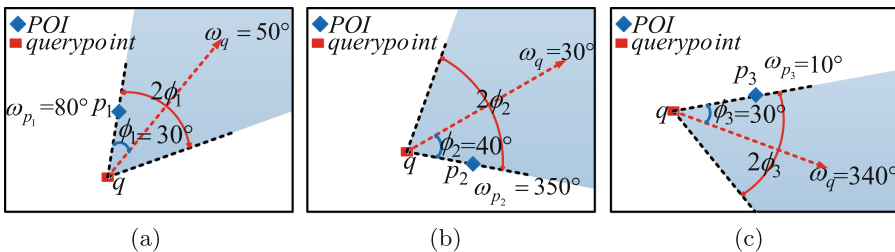


Fig. 3. Direction deviations and deviation angular ranges

- **Case 1:** $\omega_{p_i} - \omega_q \in [-\pi, \pi]$. In Fig. 3(a), $\omega_{p_1} = 80^\circ$, $\omega_q = 50^\circ$ and $\phi_1 = 30^\circ$.

$$\phi_i = |\omega_{p_i} - \omega_q| \quad (1)$$

- **Case 2:** $\omega_{p_i} - \omega_q > \pi$. In Fig. 3(b), $\omega_{p_2} = 350^\circ$, $\omega_q = 30^\circ$, there is $\phi_2 = 40^\circ$.

$$\phi_i = 2\pi - \omega_{p_i} + \omega_q \quad (2)$$

- **Case 3:** $\omega_{p_i} - \omega_q < -\pi$. In Fig. 3(c), $\omega_{p_3} = 10^\circ$, $\omega_q = 340^\circ$, there is $\phi_3 = 30^\circ$.

$$\phi_i = 2\pi - \omega_q + \omega_{p_i} \quad (3)$$

Definition 5 (Deviation Angular Range). The deviation angular range of $p_i \in \mathcal{P}$ is an angular range that the size of it is $2\phi_i$ and the user's favorite direction is its angular bisector.

We use $(\omega_q \downarrow \phi_i, \omega_q \uparrow \phi_i)$ to denote p_i 's deviation angular range. According to ϕ_i and ω_q , $(\omega_q \downarrow \phi_i, \omega_q \uparrow \phi_i)$ has three cases.

- **Case 1:** $\phi_i \leq \omega_q, \omega_q + \phi_i \leq 2\pi$. In Fig. 3(a), $\omega_q = 50^\circ, \phi_1 = 30^\circ \Rightarrow (20^\circ, 80^\circ)$.

$$(\omega_q \downarrow \phi_i, \omega_q \uparrow \phi_i) = (\omega_q - \phi_i, \omega_q + \phi_i) \quad (4)$$

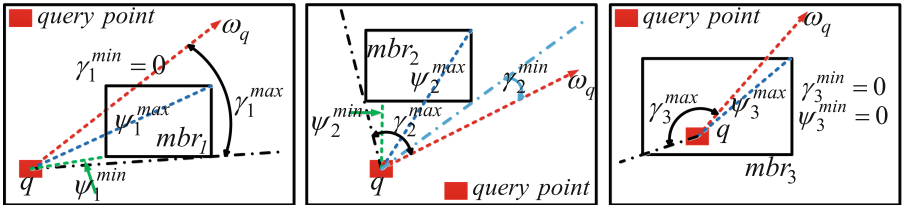
- **Case 2:** $\phi_i > \omega_q$. In Fig. 3(b), $\omega_q = 30^\circ, \phi_2 = 40^\circ \Rightarrow [0, 70^\circ) \cup (350^\circ, 360^\circ)$.

$$(\omega_q \downarrow \phi_i, \omega_q \uparrow \phi_i) = [0, \omega_q + \phi_i) \cup (2\pi + \omega_q - \phi_i, 2\pi) \quad (5)$$

- **Case 3:** $\phi_i < \omega_q, \omega_q + \phi_i > 2\pi$. In Fig. 3(c), $\omega_q = 340^\circ, \phi_3 = 30^\circ \Rightarrow [0, 10^\circ) \cup (310^\circ, 360^\circ)$.

$$(\omega_q \downarrow \phi_i, \omega_q \uparrow \phi_i) = [0, \omega_q + \phi_i - 2\pi) \cup (\omega_q - \phi_i, 2\pi) \quad (6)$$

In a two-dimensional Euclidean space, each node of the R-tree is a minimum boundary rectangle (MBR). Given a user's position q and his favorite direction ω_q , the MBR mbr_i has some attributes w.r.t. q and ω_q . The *minimum distance* and let ψ_i^{\min} denote it; the *maximum distance* and let ψ_i^{\max} denote it; the *minimum direction deviation* and let γ_i^{\min} denote it; the *maximum direction*



(a) Favorite direction intersects the MBR (b) Favorite direction doesn't intersect the MBR (c) Query point is in or on the MBR

Fig. 4. Minimum (maximum) distance and minimum (maximum) direction deviation

deviation and let γ_i^{max} denote it. A MBR can be determined by its lower left vertex coordinate (x_l, y_l) and its upper right vertex coordinate (x_r, y_r) , and $x_l < x_r, y_l < y_r$.

- The maximum distance of mbr_i .

$$\psi_i^{max} = \max(D_i(q)) \tag{7}$$

The set $D_i(q)$ stores the distance from q to each vertex of the MBR mbr_i . And $\max(D_i(q))$ ($\min(D_i(q))$) is the maximum (minimum) distance among the four distances. For example, the three MBRs in Fig. 4.

- The minimum distance of mbr_i .

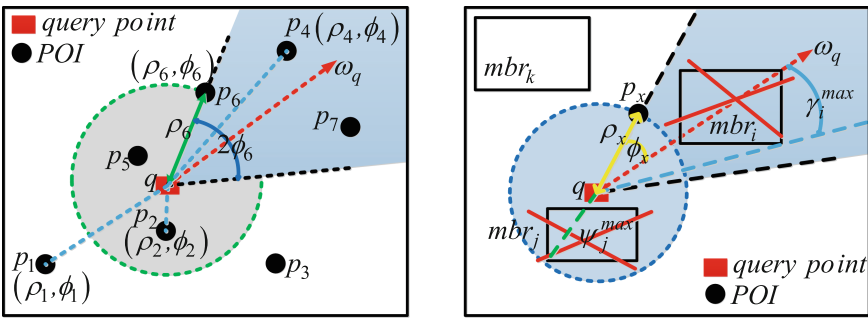
$$\psi_i^{min} = \begin{cases} 0 & q \text{ is in or on } mbr_i \\ x_l - q.x \text{ or } q.x - x_r & y_l \leq q.y \leq y_r \\ y_l - q.y \text{ or } q.y - y_r & x_l \leq q.x \leq x_r \\ \min(D_i(q)) & \text{other cases} \end{cases} \tag{8}$$

As Fig. 4 shows, in mbr_1 , ψ_1^{min} is the distance from q to the lower left vertex of the mbr_1 ; In mbr_2 , $\psi_2^{min} = y_l - q.y$; In mbr_3 , $\psi_3^{min} = 0$.

- The maximum direction deviation of mbr_i .

$$\gamma_i^{max} = \max(A_i(q)) \tag{9}$$

The set $A_i(q)$ stores the direction deviations of mbr_i 's four vertexes w.r.t. q and ω_q . And $\max(A_i(q))$ or $\min(A_i(q))$ is the maximum or the minimum direction deviation in $A_i(q)$. For example, the three MBRs in Fig. 4.



(a) Example of Lemma 1 (b) Example of Lemma 2 and Lemma 3

Fig. 5. Motivating examples

– The minimum direction deviation of mbr_i .

$$\gamma_i^{min} = \begin{cases} 0 & \omega_q \text{ intersects the } mbr_i \\ \min(A_i(q)) & \text{other cases} \end{cases} \quad (10)$$

For instance, the $\gamma_i^{min} = 0$ in Fig. 4(a) and (c). In mbr_2 , the $\gamma_2^{min} = \min(A_2(q))$.

For an object $p_i(\rho_i, \phi_i) \in \mathcal{P}$, we can get a deviation angular range and a circle w.r.t. p_i . The center of the circle is q and the radius of the circle is ρ_i . For example, POI p_6 in Fig. 5(a). On the basis of this, the Lemma 1 is defined as follows.

Lemma 1. *A POI p_j is p_i -dominated, iff p_j is outside the deviation angular range and the circle w.r.t. p_i ($p_j, p_i \in \mathcal{P}, (i \neq j)$).*

Proof. For each POI $p_j(\rho_j, \phi_j)$, if p_j is outside the deviation angular range and the circle w.r.t. $p_i(\rho_i, \phi_i)$, there are $\rho_j > \rho_i$ and $\phi_j \geq \phi_i$ or $\rho_j \geq \rho_i$ and $\phi_j > \phi_i$. According to the Definition 2, p_i dominates p_j , i.e., $p_i \prec p_j$. For each POI $p_x \in \mathcal{P} (i \neq x)$, if $p_x(\rho_x, \phi_x)$ is in the deviation angular range of p_i , there is $\phi_x < \phi_i$, then p_i cannot dominate p_x . For each POI $p_y \in \mathcal{P} (i \neq y)$, if $p_y(\rho_y, \phi_y)$ is in the circle of p_i and outside the deviation angular range of p_i , there are $\rho_y < \rho_i$ and $\phi_y > \phi_i$, p_i cannot dominate p_y .

For example, in Fig. 5(a), $\mathcal{P} = \{p_1, p_2, \dots, p_7\}$ is a POIs set. We draw a circle (i.e., the grey area) by taking q as the center and ρ_6 as the radius. POIs p_2 and p_5 are in the grey area. The blue area is the deviation angular range of p_6 . POIs p_1 and p_3 are outside the blue and the grey areas. For POIs p_1 and p_3 , there are $\rho_6 < \rho_1$, $\phi_6 < \phi_1$, $\rho_6 < \rho_3$ and $\phi_6 < \phi_3$. Consequently, p_6 dominates all POIs outside the deviation angular range and the circle w.r.t. p_6 . Each POI in the deviation angular range of p_6 or in the circle of p_6 cannot be dominated by p_6 . For example, p_4 is in the deviation angular range of p_6 and p_2 is in the circle of p_6 , they cannot be dominated by p_6 .

Lemma 2. *A MBR $mbr_k(\psi_k^{min}, \gamma_k^{min})$ and a POI $p_x(\rho_x, \phi_x)$, if $\rho_x \leq \psi_k^{min}$ and $\phi_x < \gamma_k^{min}$ or $\rho_x < \psi_k^{min}$ and $\phi_x \leq \gamma_k^{min}$, p_x dominates all POIs in mbr_k .*

Proof. For each POI $p_k(\rho_k, \phi_k)$ in mbr_k , there are $\rho_k \geq \psi_k^{min}$ and $\phi_k \geq \gamma_k^{min}$. Because $\rho_x \leq \psi_k^{min}$ and $\phi_x < \gamma_k^{min}$ or $\rho_x < \psi_k^{min}$ and $\phi_x \leq \gamma_k^{min}$, so $\rho_x \leq \rho_k$ and $\phi_x < \phi_k$ or $\rho_x < \rho_k$ and $\phi_x \leq \phi_k$ i.e., $p_x \prec p_k$. Consequently, p_x dominates all POIs in mbr_k .

For instance, in Fig. 5(b), p_x dominates all POIs in mbr_k . Therefore, when calculating p_x 's dominant capability, the number of POIs contained in mbr_k can be directly calculated into the dominant capability of p_x .

Lemma 3. *A POI p_x and a MBR mbr_i , if $\psi_i^{max} < \rho_x$ or $\gamma_i^{max} < \phi_x$, each POI in mbr_i cannot be dominated by p_x .*

Proof. For each POI $p_i(\rho_i, \phi_i)$ in $mbr_i(\psi_i^{max}, \gamma_i^{max})$, there are $\rho_i \leq \psi_i^{max}$ and $\phi_i \leq \gamma_i^{max}$. If $\psi_i^{max} < \rho_x$ or $\gamma_i^{max} < \phi_x$, each POI in mbr_i has $\rho_i < \rho_x$ or $\phi_i < \phi_x$. According the Definition 2, p_x cannot dominate all POIs in mbr_i . Consequently, when calculating p_x 's dominant capability, mbr_i does not need to be checked.

For example, in Fig. 5(b), for mbr_j , there is $\psi_j^{max} < \rho_x$. For mbr_i , there is $\gamma_i^{max} < \phi_x$. Therefore, when calculating p_x 's dominant capability, mbr_i and mbr_j don't need to be checked. Because p_x cannot dominate any POI within mbr_i or mbr_j .

Algorithm 2. GetDC($(\rho_i, \phi_i), \mathcal{S}, q$)

```

1 Add root node to  $\mathcal{S}$ 
2  $c_i \leftarrow 0$ 
3 while  $\mathcal{S}$  is not empty do
4    $node \leftarrow \mathcal{S}.pop()$ 
5   if  $node$  is a non-leaf node then
6     for  $mbr_i$  in  $node.childList$  do
7       Compute  $(\psi_i^{max}, \gamma_i^{max})$  and  $(\psi_i^{min}, \gamma_i^{min})$ 
8       if  $(\rho_i, \phi_i) \prec (\psi_i^{min}, \gamma_i^{min})$  then
9          $c_i +=$ the number of the POIs in  $mbr_i$   $\blacktriangleright$ Lemma 2
10      else if  $(\psi_i^{max} > \rho_i)$  and  $(\gamma_i^{max} > \phi_i)$  then
11         $c_i +=$ 1  $\blacktriangleright$ Lemma 3
12   if  $node$  is a leaf node then
13     for  $p_j$  in  $node.childList$  do
14       if  $p_i \prec p_j$  then
15          $c_i +=$ 1

```

According to the Lemma 1, a R-tree-based algorithm (Algorithm 2) is designed to quickly calculate the dominant capability c_i of a POI $p_i \in \mathcal{P}$. Additionally, Lemmas 2 and 3 can be used to speed up the calculation of the dominant capability. At first, only the root node of the R-tree is stored in the list \mathcal{S} and c_i is 0. When \mathcal{S} is not empty, we enter the **while** loop (Line 3). Line 4, removing the element $node$ from \mathcal{S} and determining the type of $node$. If $node$ is a non-leaf node, the lines 6 to 11 will be executed. For each child mbr_i of $node$, we first calculate $(\psi_i^{min}, \gamma_i^{min})$ and $(\psi_i^{max}, \gamma_i^{max})$ for mbr_i (Line 7). According to the Lemma 2, if p_i dominates all POIs in mbr_i , we execute the line 9. Based on the Lemma 3, if $\psi_i^{max} < \rho_i$ or $\gamma_i^{max} < \phi_i$, then all POIs in mbr_i cannot be dominated by p_i and mbr_i will be not stored in \mathcal{S} . If $node$ is a leaf node, for each POI p_j in $node$, if p_i dominates p_j , the line 15 will be executed. After the **while** loop, p_i 's dominant capability c_i will be calculated.

4.3 RTree Based Algorithm

The R-tree-based algorithm uses a priority queue and it stores R-tree's nodes and their respective maximum dominant capability. The maximum dominant capability of the R-tree's node is taken as the priority. In the R-tree-based algorithm, the top- k objects with the highest dominant capabilities can be retrieved by traversing the R-tree once.

Algorithm 3. RTree Based Algorithm

Input: q, ω_q, k
Output: The top- k objects with the highest dominant capabilities

```

1  $i \leftarrow 0$ 
2  $\mathcal{Q}.\text{push}(\text{root}, |\mathcal{P}|)$ 
3 while  $i < k$  do
4    $mbr_i \leftarrow \mathcal{Q}.\text{pop}()$ 
5   if  $mbr_i$  is a non-leaf node then
6     for  $mbr_j$  in  $mbr_i.\text{childList}$  do
7       Compute  $(\psi_j^{min}, \gamma_j^{min})$ 
8        $d_j^{max} \leftarrow \mathbf{GetDC}((\psi_j^{min}, \gamma_j^{min}), \mathcal{S}, q)$ 
9        $\mathcal{Q}.\text{push}(mbr_j, d_j^{max})$ 
10  if  $mbr_i$  is a leaf node then
11    for  $p_j$  in  $mbr_i.\text{childList}$  do
12      Compute  $(\rho_j, \phi_j)$ 
13       $c_j \leftarrow \mathbf{GetDC}((\rho_j, \phi_j), \mathcal{S}, q)$ 
14       $\mathcal{Q}.\text{push}(p_j, c_j)$ 
15  if  $mbr_i$  is a point then
16    Print  $mbr_i$  and its dominant capability
17   $i += 1$ 

```

For each node mbr_i of the R-tree, we can calculate its *minimum distance* ψ_i^{min} and *minimum direction deviation* γ_i^{min} . According to them, we can call the function $\mathbf{GetDC}((\psi_i^{min}, \gamma_i^{min}), \mathcal{S}, q)$ to calculate the maximum dominant capability d_i^{max} of mbr_i . Initially, the counter i is 0 and the priority queue \mathcal{Q} stores the root node of the R-tree and its maximum dominant capability. At the beginning, the maximum dominant capability of the root node is considered to be the size of the POIs set \mathcal{P} . If $i < k$, entering the **while** loop. Line 4, the element (mbr_i) with the highest dominant capability is popped from \mathcal{Q} . If mbr_i is a non-leaf node, we calculate $(\psi_j^{min}, \gamma_j^{min})$ for each child mbr_j of mbr_i (Line 7). Line 8, we call the function $\mathbf{GetDC}((\psi_j^{min}, \gamma_j^{min}), \mathcal{S}, q)$ to calculate the maximum dominant capability (d_j^{max}) of mbr_j . Line 9, mbr_j and its maximum dominant capability are pushed into \mathcal{Q} . If mbr_i popped from \mathcal{Q} is a leaf node. For each POI p_j in mbr_i , we calculate the dominant capability (c_j) of p_j (Line 13). Line 14, p_j and c_j are pushed into \mathcal{Q} . If the element with the highest dominant capability

is a point, then it is a result and the value of the counter i will increase by 1. When $i = k$, we find all results and end the program.

4.4 Improve the RTree Based Algorithm

An improved R-tree-based algorithm is designed in this section. *An object that cannot be dominated by all other objects is a skyline object.* The key of the algorithm is how to find the top- k skyline objects with the highest dominant capabilities. Because we can quickly calculate the dominant capability of an object according to the Algorithm 2. Consequently, we can first find all skyline objects, then calculate their dominant capabilities, and finally find the top- k skyline objects with the highest dominant capabilities. Next, we introduce an efficient way to quickly find the skyline objects.

Lemma 4. *The POI with the minimum direction deviation among all POIs closest to q must be a skyline object.*

$$\forall p_i \in \mathcal{P}, \text{ if } p_i \in NN(q) \text{ and } \phi_i = \min(NN_\phi), \exists p_i \text{ is a skyline object} \quad (11)$$

The set $NN(q)$ stores q 's nearest neighbors. The $\min(NN_\phi)$ denotes the minimum direction deviation all elements in the set $NN(q)$ can produce.

Proof. If there is only one POI $p_i(\rho_i, \phi_i) \in \mathcal{P}$ closest to q , then the ρ_i is the smallest one among all POIs in \mathcal{P} . According to the Definition 2, all POIs in $\mathcal{P} - \{p_i\}$ cannot dominate p_i . Consequently, p_i is a skyline object. If there is more than one POI closest to q , assuming $p_i(\rho_i, \phi_i) \in \mathcal{P}$ and $p_j(\rho_j, \phi_j) \in \mathcal{P}$, then $\rho_i = \rho_j$ and they are the smallest among all POIs in \mathcal{P} . According to the Definition 2, all POIs in $\mathcal{P} - \{p_i, p_j\}$ cannot dominate p_i and p_j . If the direction deviation of p_i is smaller, i.e., $\phi_i < \phi_j$, then p_i dominates p_j and p_i is a skyline object instead of p_j . Consequently, the POI with the minimum direction deviation among all POIs closest to q cannot be dominated by all other POIs and it must be a skyline object.

Lemma 5. *The $j + 1$ th skyline object must be the POI with the minimum direction deviation among the nearest neighbors within the deviation angular range of the j th skyline object.*

$$\forall p_i \in \mathcal{P}, \text{ if } p_i \in DNN(q) \text{ and } \phi_i = \min(DNN_\phi), \exists p_i \text{ is a skyline object} \quad (12)$$

The set $DNN(q)$ stores q 's nearest neighbors within the deviation angular range of the current skyline object. The $\min(DNN_\phi)$ denotes the minimum direction deviation that elements in the set $DNN(q)$ can produce.

Proof. Let's assume that the current skyline object is $p_j \in \mathcal{P}$. We can get a deviation angular range and a circle w.r.t. p_j . The center of the circle is q and its radius is ρ_j . According to the Lemma 1, all POIs outside this deviation angular range and the circle are p_j -dominated. Therefore, the new skyline objects must be within the deviation angular range of p_j . According to the Definition 2,

the POI with the minimum direction deviation among the nearest neighbors within p_j 's deviation angular range cannot be dominated by all other POIs in \mathcal{P} . Consequently, the POI is a new skyline object.

For example, in Fig. 2(b), POI p_3 is a skyline object and there is only one POI p_8 in the deviation angular range of p_3 . POI p_8 cannot be dominated by all other POIs and it is a new skyline object.

Lemma 6. *MBRs outside the deviation angular range of current skyline object shouldn't be checked.*

Proof. According to the Lemmas 4 and the 5, new skyline objects must be within the deviation angular range of the current skyline object. Therefore, MBRs outside the deviation angular range must not contain new skyline objects and shouldn't be checked.

Algorithm 4. GetSkyline(q, ω_q)

```

1  $\mathcal{M} \leftarrow \text{NNQ}(q)$  ►Lemma 4
2 if  $|\mathcal{M}| == 1$  then
3    $s_0 \leftarrow \mathcal{M}[0]$ 
4 else
5    $s_0 \leftarrow$  find the POI with the minimum direction deviation
6   compute  $\rho_0$  and  $\phi_0$  for  $s_0$ 
7    $c_0 \leftarrow \text{GetDC}((\rho_0, \phi_0), \mathcal{S}, q)$ 
8    $que.push((s_0, c_0))$ 
9    $\mathcal{N} \leftarrow \text{DCNNQ}(s_0, q)$  ►Lemma 5
10 while  $|\mathcal{N}| \neq 0$  do
11   if  $|\mathcal{N}| == 1$  then
12      $s_i \leftarrow \mathcal{N}[0]$ 
13   else
14      $s_i \leftarrow$  find the POI with the minimum direction deviation
15     compute  $\rho_i$  and  $\phi_i$  for  $s_i$ 
16      $c_i \leftarrow \text{GetDC}((\rho_i, \phi_i), \mathcal{S}, q)$ 
17      $que.push((s_i, c_i))$ 
18     clear  $\mathcal{N}$ 
19      $\mathcal{N} \leftarrow \text{DCNNQ}(s_i, q)$  ►Lemma 5

```

According to the Lemma 4, we can easily find the first skyline object and based on the Lemma 5, we can find all skyline objects one by one. On the basis of the two lemmas, the R-tree-based algorithm (Algorithm 4) is designed to quickly find all skyline objects. At the same time, Lemma 6 is used to speed up the query.

From line 1 to line 8, based on the Lemma 4, we use a nearest neighbor query [2] ($\text{NNQ}()$) to find the first skyline object s_0 . The list \mathcal{M} stores the results of the function $\text{NNQ}(q)$ (Line 1). If there is only one POI closest to q , then the POI is a skyline object (Line 3). Otherwise, the POI with the minimum direction deviation is a skyline object (Line 5). We call the function $\text{GetDC}((\rho_0, \phi_0), \mathcal{S}, q)$ to calculate the dominant capability (c_0) for s_0 (Line 7). We store s_0 and its dominant capability c_0 in the priority queue que (Line 8). From the line 9 to the line 19, according to the Lemma 5, we use snapshot DCNN queries [3] ($\text{DCNNQ}()$) to find all skyline objects one by one. Given a query point q and a moving direction ω and an angle threshold θ , the snapshot DCNN query [3] finds the nearest POIs within an angular range and the angular range is calculated according to ω and θ . The list \mathcal{N} stores all results of the function $\text{DCNNQ}(s_i, q)$. They are the nearest neighbors within the deviation angular range of s_i . We calculate the number of the elements in \mathcal{N} and enter the **while** loop (Line 10). From lines 11 to 14, the new skyline object s_i is found. We calculate the dominant capability c_i of s_i (Line 16). We store s_i and its dominant capability c_i in que (Line 17). We clear the list \mathcal{N} and continue to call the function $\text{DCNNQ}()$ until \mathcal{N} is empty. All skyline objects and their dominant capabilities are stored in que .

Lemma 7. *POIs $p_i \prec p_j$, if $p_j \prec p_k$, then $p_i \prec p_k$.*

Proof. According to the Definition 2, if $p_j \prec p_k$, there are $\rho_j \leq \rho_k$ and $\phi_j < \phi_k$ or $\rho_j < \rho_k$ and $\phi_j \leq \phi_k$. Because $p_i \prec p_j$, there are $\rho_i \leq \rho_j$ and $\phi_i < \phi_j$ or $\rho_i < \rho_j$ and $\phi_i \leq \phi_j$. Therefore, there are $\rho_i \leq \rho_k$ and $\phi_i < \phi_k$ or $\rho_i < \rho_k$ and $\phi_i \leq \phi_k$. Consequently, $p_i \prec p_k$.

Lemma 8. *POIs $p_i \prec p_j$, if $p_j \prec P_j$, then $p_i \prec P_j$.*

Proof. If $p_j \prec P_j$, i.e., p_j dominates each POI in the set P_j . According to the Lemma 7, p_i dominates each POI in P_j , i.e., $p_i \prec P_j$.

Lemma 9. *An object with the highest dominant capability must be a skyline object.*

Proof. Assuming that $p_i \in \mathcal{P}$ has the highest dominant capability (c_i) and it isn't a skyline object, then p_i is dominated by at least one object in $\mathcal{P} - \{p_i\}$. Assuming $p_j \prec p_i$, $p_j \in \mathcal{P} - \{p_i\}$. Therefore, $c_j > c_i$, i.e., p_i isn't the POI with the highest dominant capability, which is contrary to the hypothesis. Consequently, the Lemma 9 is valid.

According to the Lemmas 7, 8 and 9, a heuristic conclusion can be drawn. *A POI dominated by the POI with the highest dominant capability is also likely to have a higher dominant capability.* Consequently, based on the Lemma 9 and the heuristic conclusion, an improved R-tree-based algorithm can be proposed.

We first call the function $\text{GetSkyline}(q, \omega_q)$ to get the priority queue que (Line 1). If the number of the skyline objects is not bigger than k , all skyline objects are stored in the list \mathcal{D} (Line 6). And all skyline objects and their respective dominant capability are stored in a priority queue Que (Line 7). Otherwise,

we execute the lines 9 to 13. Skyline object with the highest dominant capability is first popped from the priority queue que . Consequently, skyline objects in \mathcal{D} are stored in descending order according to their respective dominant capability. For each skyline object s_i in \mathcal{D} , according to the idea of finding skyline objects, the algorithm first finds a set S_i for s_i (Line 15). The set S_i stores POIs that are dominated only by s_i in the dominant set of s_i . For each POI p_x in S_i , we call the function **GetDC** $((\rho_x, \phi_x), \mathcal{S}, q)$ to calculate the dominant capability c_x

Algorithm 5. Improved RTree Based Algorithm

Input: q, ω_q, k
Output: The top- k objects with the highest dominant capabilities

```

1   $que \leftarrow \text{GetSkyline}(q, \omega_q)$ 
2   $j \leftarrow 0$ 
3  if  $|que| \leq k$  then
4      while  $|que| \neq 0$  do
5           $(s_i, c_i) \leftarrow que.pop()$ 
6          add  $s_i$  to  $\mathcal{D}$ 
7          push  $(s_i, c_i)$  to  $Que$ 
8  else
9      while  $j < k$  do
10          $(s_i, c_i) \leftarrow que.pop()$ 
11         add  $s_i$  to  $\mathcal{D}$ 
12         push  $(s_i, c_i)$  to  $Que$ 
13          $j + = 1$ 
14 for  $s_i$  in  $\mathcal{D}$  do
15      $S_i \leftarrow$  POIs only dominated by  $s_i$  in the set of POIs dominated by  $s_i$ 
16     for  $p_x$  in  $S_i$  do
17          $c_x \leftarrow \text{GetDC}((\rho_x, \phi_x), \mathcal{S}, q)$ 
18         if  $|Que| < k$  then
19             push  $(p_x, c_x)$  to  $Que$ 
20         else
21              $(s_{min}, c_{min}) \leftarrow Que.pop()$ 
22             if  $c_{min} < c_x$  then
23                 push  $(p_x, c_x)$  to  $Que$ 
24                 if  $s_{min} \in \mathcal{D}$  then
25                     remove  $s_{min}$  from  $\mathcal{D}$ 
26             else
27                 push  $(s_{min}, c_{min})$  to  $Que$ 

```

of p_x (Line 17). If the number of the objects in the priority queue Que is less than k , then (p_x, c_x) will be pushed into Que (Line 19). Otherwise, the POI with the minimum dominant capability (s_{min}, c_{min}) will be popped from Que

(Line 21). If c_x of p_x is higher than c_{min} , (p_x, c_x) will be pushed into *Que* (Line 23). If $s_{min} \in \mathcal{D}$, s_{min} will be removed from \mathcal{D} (Line 25). If $c_x \leq c_{min}$, we push (s_{min}, c_{min}) back into *Que* (Line 27). After the outer **for** loop, *Que* stores the top- k objects with the highest dominant capabilities.

5 Experiments

We report the performance of the proposed algorithms in this section. All algorithms are implemented in Python and carried out on the ubuntu 16.04 system. There are three real datasets $\mathcal{P}_{shanghai}$, $\mathcal{P}_{kunshan}$ and $\mathcal{P}_{changshu}$, which contain 163031, 18549 and 9244 restaurants in three cities (Shanghai, Kunshan and Changshu) of China. Figure 6 visualizes the distributions of the three real datasets. The synthetic datasets are randomly generated (Table 2).

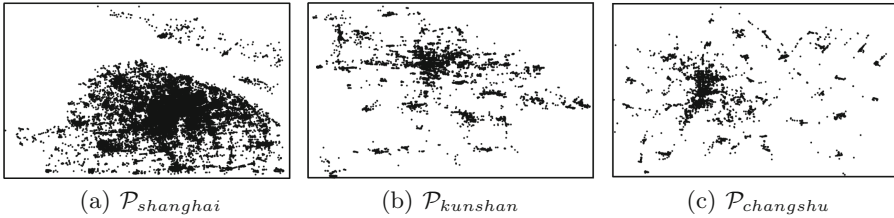


Fig. 6. Real datasets

Table 2. Synthetic datasets

Dataset size	Region size	Point density
1000	$[0, 1000] * [0, 1000]$	1/1000
10000	$[0, 1000] * [0, 10000]$	1/1000
100000	$[0, 10000] * [0, 10000]$	1/1000

In our experiments, the baseline method (Algorithm 1) is represented by “BSL”. Let “DOM” denote the R-tree-based algorithm (Algorithm 3), which is designed according to the maximum dominant capability of the R-tree’s node. Let “SKY” denote the improved R-tree-based algorithm (Algorithm 5), which is designed according to the skyline objects. The comparing factors include the dataset size and the fan-out size of R-tree’s node. If the type of the node is a leaf node, then the fan-out size of the node is the number of the POIs within the node. If the type of the node is a non-leaf node, then the fan-out size of the node

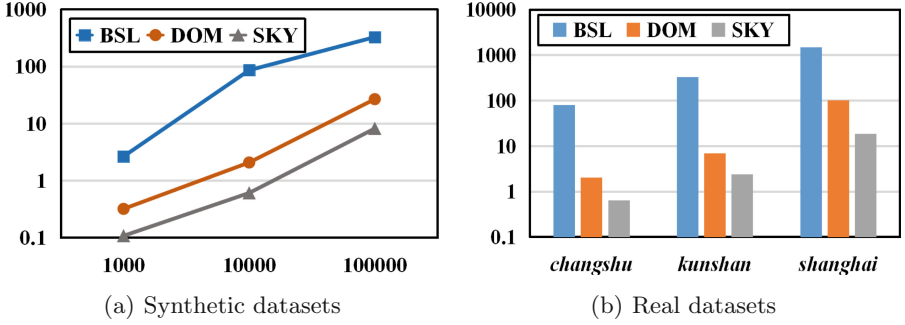


Fig. 7. Experimental results of varying the dataset size ($k = 3$, $f = 35$)

is the number of the children of the node. For simplicity, let the symbol f denote the fan-out size of the R-tree’s node. The unit of the query time is seconds.

Figure 7(a) and (b) show the experimental results of varying the size of the datasets on synthetic and real datasets. The horizontal axis in (a) or (b) represents three synthetic datasets or three real datasets. The vertical axis represents the query time in logarithmic form. From (a) and (b), we can find that the “BSL” is the worst on both synthetic and real datasets, and the “SKY” is the best. In addition, the “SKY” and the “DOM” are significantly better than the baseline algorithm, and the “SKY” is significantly better than the “DOM”.

Because both the “SKY” and the “DOM” use R-tree as the index structure. The fan-out value of R-tree’s node can affect these two algorithms. Figures 8 and 9 show the influence of varying the fan-out value on two algorithms. The fan-out values we selected are 25, 35 and 45, respectively. The horizontal axis represents the datasets, and the vertical axis represents the logarithmic query time.

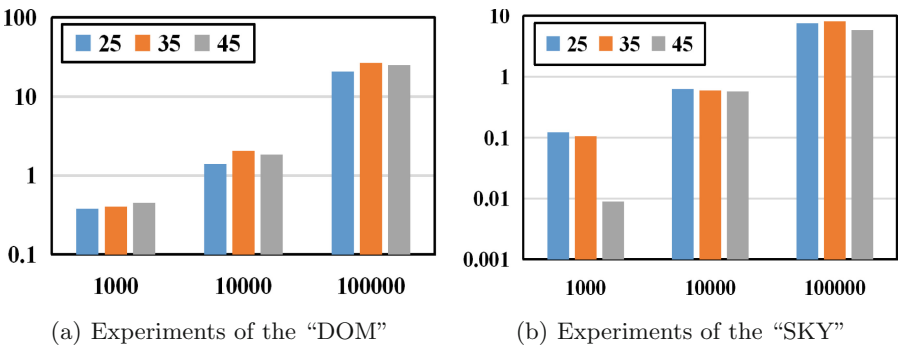


Fig. 8. Experiments of varying the fan-out size on synthetic datasets ($k = 3$)

As shown in the Figs. 8(a) and the 9(a), on three synthetic and three real datasets, when the fan-out value f is 25, the “DOM” has the highest query efficiency. In addition, as shown in the Fig. 8(b), when f is 45, the “SKY” has the highest query efficiency on three synthetic datasets. However, as the Fig. 9(b) shows, when f is 35, the “SKY” has the highest query efficiency on three real datasets.

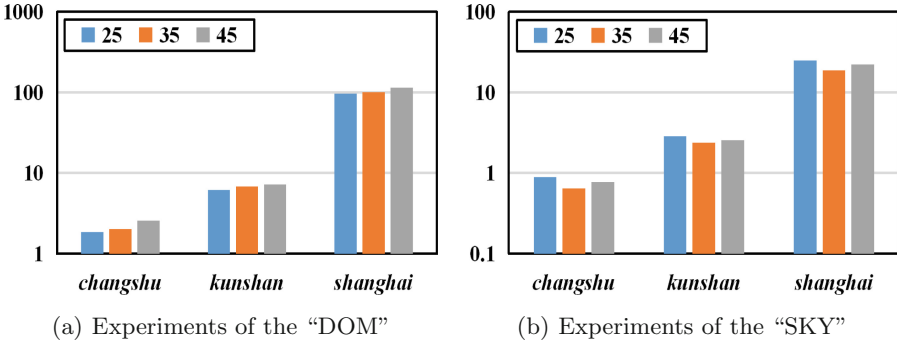


Fig. 9. Experiments of varying the fan-out size on three real datasets ($k = 3$)

Figure 10 shows the effect of varying the fan-out value f and the size of the datasets on the calculation of the dominant capability (Algorithm 2). As shown in the Fig. 10, when the fan-out value is 35 and the synthetic dataset size is 1000, our dominant capability function has the highest query efficiency. However, when the fan-out value is 45 and the synthetic dataset size is 10000 or 100000, our dominant capability function has the highest query efficiency. On three real datasets, the dominant capability function has the highest query efficiency when the fan-out value is 35.

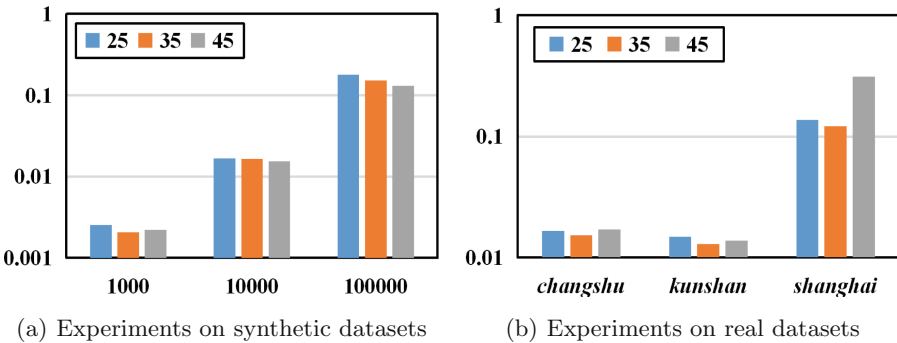


Fig. 10. Experiments of dominant capability calculation

According to the function of calculating the dominant capability (Algorithm 2), the Algorithm 3 can find the top- k POIs with the highest dominant capabilities by traversing R-tree once. The Algorithm 5 needs to find the top- k skyline objects with the highest dominant capabilities first, and then further process these skyline objects to find the top- k POIs with the highest dominant capabilities. So for the Algorithm 5, traversing R-tree once can not solve the problem. However, extensive experimental results demonstrate that the Algorithm 5 is more efficient than the Algorithm 3. Why?

This is because our calculation of the maximum dominant capability of the R-tree’s node is inaccurate. We calculate the maximum dominant capability of the node according to its minimum distance and its minimum direction deviation. Although it ensures that the maximum dominant capability is greater than the dominant capability of each POI within the node, the maximum dominant capability calculated in this way is excessively higher than the precise maximum dominant capability of the node. Each time the node with the highest dominant capability is popped from the priority queue. We calculate the maximum dominant capability for each child of the node and push each child and its maximum dominant capability back in the priority queue. The inaccurate maximum dominant capability will lead to no new child on the top of the heap. As a result, many nodes need to be expanded to make a point at the top of the heap. Additionally, each expansion of the R-tree’s node will be accompanied by extensive computations of the dominant capability.

Table 3. Analysis of the Algorithm 3

Real dataset	DC-Count	Node-Count	Synthetic dataset	DC-Count	Node-Count
<i>Pchangshu</i>	218	12	1000	138	9
<i>Pkunshan</i>	312	18	10000	233	12
<i>Pshanghai</i>	396	20	100000	467	22

As the Table 3 shows, we calculate the approximate number of the nodes expanded by the Algorithm 3 in a DirDom query and let “Node-Count” denote it. We also calculate the approximate times of computing the dominant capability in a DirDom query and let “DC-Count” denote it. In the experiments, k is 3 and the fan-out value is 35.

6 Conclusions

In this paper, we propose a new direction-aware spatial query, i.e., the direction-aware top- k dominating query (DirDom query), which not only considers the distance attributes but also considers the direction attributes of the spatial objects. Given a user’s position and his favorite direction, the DirDom query finds the top- k objects with the highest dominant capabilities. Higher dominant

capability ensures that the query results are closer to the user's position and more consistent with the user's favorite direction. We design efficient R-tree-based algorithms to answer the DirDom query. Extensive experimental results demonstrate the efficiency and the correctness of our algorithms.

Acknowledgments. This work is supported by the National Natural Science Foundation of China (No. 61602031) and the Fundamental Research Funds for the Central Universities (FRF-BD-19-012A). This work is also supported by Research into the High-Definition Remote Sensing-Based Critical Intelligent Monitoring Technology for Spatial Planning and its Model Applications (Dedicated Project of East-West Cooperation) (No. 2018YBZD1629).

References

1. Guo, X., Ishikawa, Y., Gao, Y.: Direction-based spatial skylines. In: ACM International Workshop on Data Engineering for Wireless and Mobile Access (2010)
2. Roussopoulos, N., Kelley, S., Vincent, F.: Nearest neighbor queries. In: ACM Sigmod International Conference on Management of Data, vol. 24, pp. 71–79 (1995)
3. Miao, X., Guo, X., Wang, H., Wang, Z., Ye, X.: Continuous nearest neighbor query with the direction constraint. In: Kawai, Y., Storandt, S., Sumiya, K. (eds.) W2GIS 2019. LNCS, vol. 11474, pp. 85–101. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17246-6_8
4. Borzsony, S., Kossmann, D., Stocker, K.: The Skyline operator. In: International Conference on Data Engineering, pp. 421–430 (2001)
5. Sharifzadeh, M., Shahabi, C.: The spatial skyline queries. In: VLDB, pp. 751–762 (2006)
6. Lee, M.W., Son, W., Ahn, H.K., et al.: Spatial skyline queries: exact and approximation algorithms. *GeoInformatica* **15**(4), 665–697 (2011)
7. Lin, Q., Zhang, Y., Zhang, W., Li, A.: General spatial skyline operator. In: Lee, S., Peng, Z., Zhou, X., Moon, Y.-S., Unland, R., Yoo, J. (eds.) DASFAA 2012. LNCS, vol. 7238, pp. 494–508. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29038-1_36
8. Son, W., Hwang, S., Ahn, H.-K.: MSSQ: manhattan spatial skyline queries. In: Pfoser, D., et al. (eds.) SSTD 2011. LNCS, vol. 6849, pp. 313–329. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22922-0_19
9. Guo, X., Zheng, B., Ishikawa, Y., et al.: Direction-based surrounder queries for mobile recommendations. *VLDB* **20**(5), 743–766 (2011)
10. Li, G., Feng, J., Jing, X.: DESKS: direction-aware spatial keyword search. In: IEEE International Conference on Data Engineering, vol. 1084, pp. 474–485 (2012)
11. Chen, Z.J., Zhou, T., Liu, W.Y.: Direction aware collective spatial keyword query. *J. Chin. Comput. Syst.* **35**(5), 999–1004 (2014)
12. Chen, L., Li, Y., Xu, J., et al.: Direction-aware why-not spatial keyword top- k queries. In: IEEE International Conference on Data Engineering, pp. 107–110 (2017)
13. Chen, L., Li, Y., Xu, J., et al.: Towards why-not spatial keyword top- k queries: a direction-aware approach. *IEEE Trans. Knowl. Data Eng.* **30**(4), 796–809 (2018)
14. Guo, X., Yang, X.: Direction-aware nearest neighbour query. *IEEE Access* **7**, 30285–30301 (2019)

15. Lee, M.J., Choi, D.W., Kim, S.Y., et al.: The direction-constrained k nearest neighbor query. *Geoinformatica* **20**(3), 471–502 (2016)
16. Shen, B., Islam, M.S., Taniar, D.: Direction-based spatial skyline for retrieving surrounding objects. *World Wide Web* (2019)
17. Papadias, D., Tao, Y., Fu, G., et al.: Progressive skyline computation in database systems. *ACM Trans. Database Syst.* **30**(1), 41–82 (2005)
18. Yiu, M.L., Mamoulis, N.: Multi-dimensional top- k dominating queries. *VLDB J.* **18**(3), 695–718 (2009)
19. Chan, C.Y., Jagadish, H.V., Tan, K.L., et al.: Finding k -dominant skylines in high dimensional space. In: *SIGMOD* (2006)
20. Chan, C.-Y., Jagadish, H.V., Tan, K.-L., Tung, A.K.H., Zhang, Z.: On high dimensional skylines. In: Ioannidis, Y., et al. (eds.) *EDBT 2006*. LNCS, vol. 3896, pp. 478–495. Springer, Heidelberg (2006). https://doi.org/10.1007/11687238_30
21. Li, C., Ooi, B.C., Tung, A.K.H., et al.: DADA: a data cube for dominant relationship analysis. In: *SIGMOD* (2006)
22. Lin, X., Yuan, Y., Zhang, Q., et al.: Selecting stars: the k most representative skyline operator. In: *ICDE* (2007)



A Personalized Collaborative Filtering Recommendation System of Network Document Resource Based on Knowledge Graph

Yuezhong Wu^{1,2}, Rongrong Chen³, Changyun Li^{1,2},
and Shuhong Chen^{4,5}(✉)

- ¹ College of Artificial Intelligence, Hunan University of Technology, Zhuzhou, China
- ² Intelligent Information Perception and Processing Technology Hunan Province Key Laboratory, Zhuzhou, China
- ³ College of Business, Hunan University of Technology, Zhuzhou, China
- ⁴ School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou, China
shuhongchen@gzhu.edu.cn
- ⁵ School of Computer and Communication, Hunan Institute of Engineering, Xiangtan, China

Abstract. The Internet has become one of the important channels for users to obtain information and knowledge. It is crucial that how to acquire personalized requirement of users accurately and effectively from huge amount of network document resource. This paper proposes a personalized collaborative filtering recommendation system for network document resource exploration using knowledge graph which can solve the problem of information overload and resource trek effectively. Extensive system test has been carried out in the field of big data application in packaging industry. The experimental results show that the proposed system recommends network document resource more accurately, and further improves recommendation quality using knowledge graph. Therefore, it can meet people's personalized resource need more effectively.

Keywords: Knowledge graph · Recommendation system · Collaborative filtering · Network document resource

1 Introduction

With the popularity of the Internet, network resources have become people's first choice to find information. As a kind of special resources of the Internet, the rapid growth of network document resources make the problem of "information overload" and "resources trek" more and more serious, preventing people from collecting and obtaining information efficiently. For example, there will be more than 19 million query results when the keyword "recommendation system" is given in Baidu library. Massive and excessive information will be presented at the same time, which makes it difficult for people to make correct and efficient choices and obtain the resources they really want. As an essential means of information filtering, recommendation system is one of the most effective methods to solve the current "information overload" and

“resources trek” problems [1]. Collaborative filtering recommendation is the most successful recommendation technology. The main idea of the algorithm is to calculate similarity of users or items based on the user’s scores on items, and then predict the target user’s possible score by referring to the score of similar users or similar items and thereby generate recommendations. However, in practical applications, there is a problem of data sparsity, that is, most users only give a small amount of score.

The emergence of knowledge graph [2] provides an effective way to design recommendation systems in big data environments. It is because that knowledge graph can better enrich and represent the semantics of resources and thereby provide more comprehensive and relevant information. It can enhance the semantic accuracy of the data to further improve recommendation accuracy, and can solve the data sparsity problem of recommendation technology as well.

Based on the traditional collaborative filtering recommendation, a personalized collaborative filtering recommendation system for network document resource discovery based on knowledge graph is proposed. Combining with collaborative filtering-based recommendation and content-based recommendation based on knowledge graph, the proposed system can push accurate information according to users’ needs proactively and solve the “information overload” and “resources trek” problem as well. The main contributions of this paper are as follows:

- (a) A personalized collaborative filtering recommendation system based on knowledge graph is proposed. The proposed system combines collaborative filtering-based recommendation and content-based recommendation based on knowledge. Recommendation results are all individually adjustable that can meet the users’ real need accordingly, which undoubtedly can improve the accuracy of the recommendation.
- (b) Recommendation quality is improved. The proposed system takes advantage of knowledge graph to solve the sparsity of recommendation and improve the recommendation precision rate and recall rate. Therefore, the proposed system provides practical value for personalized recommendation systems of network document resource.
- (c) System test has been accomplished in the field of big data application in packaging industry. The experimental results demonstrate the personalized recommendation results can meet people’s real needs more effectively.

The remainder of the paper covers background and related work discussions (Sect. 2), the preliminaries of personalized recommendation system and detailed illustration (Sect. 3), the design of personalized recommendation system and detailed illustration (Sect. 4), the experiments and test results (Sect. 5), the conclusions and future work (Sect. 6).

2 Related Work

2.1 Recommendation System

With the rapid growth of the Internet information, serious “information overload” and “resource trek” problems have emerged. The recommendation system has received

wide attention as a solution in academia and business. The recommendation system is a subset of the information filtering system that predicts users possible preferences and recommends to users, based on user preferences, habits, personalized needs, and characteristics of information or objects (such as: movies, TV shows, music, books, news, photos, web pages, etc.), and helps users to make quick decisions and improves user satisfaction [3]. In recent years, with the continuous development of recommendation system, according to the different selection methods, there are some recommended algorithms: demographic-based recommendation [4], content-based recommendation [5], collaborative filtering-based recommendation [6], knowledge-based recommendation [7], model-based recommendation [8], association rule mining for recommendation [9], social-based recommendation [10], hybrid recommendation [11], and so on. With the increasing application forms and scenarios of the recommendation system, the research and application of the recommendation system faces some important issues. Such as: cold start problem, user niche problem, personalized recommendation interpretability problem. The existing research focuses on constructing a personalized recommendation service based on a data model that reflects user interest characteristics. Hu [12] proposed a recommendation algorithm based on user interest and topic model to solve the problems of data sparsity, cold start and user interest acquisition. Hu et al. [13] proposed an enhanced group recommendation method based on preference aggregation, incorporating simultaneously the advantages of the aforesaid two aggregation methods, and effectively improved recommendation accuracy. The authors [14–16] all proposed to satisfy the user's preference, rely on the user's own attributes to make recommendations based on utility, and apply them in the recommendation of papers, music, and electronic products. The goal is to maximize the user's interests, improve the accuracy, and ensure the quality of recommendation services.

2.2 Knowledge Graph

The application of knowledge graph is coherently born to enrich and represent the semantics of resources. It was proposed by Google in 2012 to describe the various entities or concepts that exist in the real world and incidence relation between them. Knowledge graph is not a substitute for ontology. Ontology describes data schema of the knowledge graph, namely for knowledge graph building data schema equivalent to establishing its ontology. Knowledge graph basing on ontology enriches and expands, and the expansion is mainly embodied in the entity level. The knowledge graph is more accurate to describe the incidence of various relationships in the real world. The knowledge graph is a great promoter of the semantic annotation of digital resources, and promoting the efficient acquisition of knowledge and information. At present, Google, Sogou cubic, Baidu bosom, Microsoft Probase, etc. already preliminarily applied knowledge graph system in the industry. Most of them are general knowledge graph, which emphasizes the breadth of knowledge, and includes more entities. It is difficult to have complete and global ontology layer to unified management, and mainly used in the search business, and not high accuracy requirements. There are some industry knowledge graphs, has high accuracy requirements, used for auxiliary complex decision support, the rich and the strict data patterns, etc. The authors [17, 18]

reviewed knowledge graph technology in academia. Hu [19] researched on the construction of knowledge graph based on the application. Li et al. [20] proposed an automatic knowledge graph establishment method and established a knowledge graph of packaging industry. Chang et al. [21] summarized the application of knowledge graph in recommendation system. In order to seek semantics support for searching, understanding, analyzing, and mining, Wu et al. [22] proposed a more convenient way which based on domain knowledge graph to annotate network document automatically. The recommendation system based on knowledge graph enhances the semantic information of the data by connecting users and users, users and items, and items and items to further improve the accuracy of recommendation. Therefore, it has important research significance and practical value, and gradually becomes one of the most active branches on research recommendation system.

3 Preliminaries

3.1 The Computation Model of Word Vector

TF-IDF is a very significant concept and method in the field of information retrieval and data mining. The figure of TF-IDF is inversely proportional to the times of the word that exists in the whole gathered document, and is proportional to the frequency that appears in the document. However, all of the document set are converged by all attribute characteristics of instances, including the basic attribute and the domain attribute. In the traditional TF-IDF model, it failed to reflect the contribution of the different attributes to instance word vectors. Hence, this paper advocates to calculate the word vector by the use of the upgraded TF-IDF model based on the contribution [22].

CTF is short for contribution of term frequency, which is defined as follows:

$$CTF(w_i) = \frac{\sum_{j=1}^n C(w_{ij}) * W(Attr_{ij})}{\sum_{i=1}^m \sum_{j=1}^n C(w_{ij}) * W(Attr_{ij})} \quad (1)$$

As well as CIDF is defined as follows, which is short for contribution of inverse document frequency.

$$CIDF(w_i) = \log\left(\frac{\sum_{i=1}^m \sum_{j=1}^n W(Attr_{ij})}{\sum_{j=1}^n W(Attr_{ij}) + 1}\right) \quad (2)$$

In addition, this formula $CTF(w_i)$ demonstrates the word frequency of the contribution for w_i , $C(w_{ij})$ represents the word frequency in the j attribute text for w_i , $W(Attr_{ij})$ represents the weight of the j attribute, and the formula $CIDF(w_i)$ demonstrates the inverse document frequency based on the contribution for w_i .

Calculate the figure of the upgraded TF-IDF:

$$W_i = CTF(w_i) * CIDF(w_i) \tag{3}$$

The network document refers to an article, including information, new, paper and so on. Its format can be structured in types such as TXT and XML. It can also be unstructured types such as WORD, PDF and other. Network document is presented with an upgraded word model TF-IDF model based on the contribution in this paper:

$$d = (w_{d1}, w_{d2}, \dots, w_{dm}) \tag{4}$$

In this paper, the system has a user set, each user has own hobbies and interests. Interests are grouped by subject. Users interests are collected by both manual and automatic acquisition mode in this paper. Adding keywords by users themselves is the manual mode. While automatic mode is that the system obtaining keywords through processing user access records, and achieving adaptive updates in the interactive process, and putting these keywords into the words library. User interest model is presented with an upgraded word model TF-IDF model based on the contribution in this paper:

$$u = (w_{u1}, w_{u2}, \dots, w_{un}) \tag{5}$$

3.2 Knowledge Graph Construction Method

The framework of knowledge graph construction method is shown in Fig. 1. It includes the lifecycle of domain knowledge graph, which mainly has five processes, namely, ontology definition, knowledge extraction, knowledge fusion, knowledge storage and knowledge application respectively. Each process has own methods and tasks. For example, D2RQ is used to transform the atomic entity table and the atomic relation table into RDF in knowledge extraction; defined the knowledge fusion rules to complete the knowledge fusion task while extracting knowledge with D2R and Wrappers, the tasks are such as entity merge, entity linking and attribute merge.

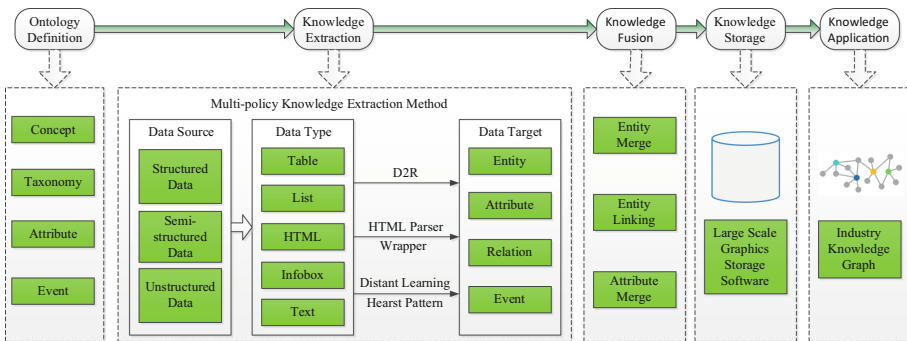


Fig. 1. The framework of knowledge graph construction method

In this paper, the authors obtain the semantic annotation knowledge graph. The semantic annotation helps the generation of sentence text and eliminates the ambiguity and ambiguity of natural language text. The entity in the knowledge graph can be used as a word segmentation dictionary. The semantics of entities, attributes and relationships provide synonymy, inclusion, etc., and remove ambiguity and ambiguity, thus provide standard, concise and comprehensive knowledge information.

4 The Design of Personalized Recommendation System

This paper designs a personalized collaborative filtering recommendation system of network document resource based on knowledge graph. Through the knowledge graph, the new meaning of the string is given, and the knowledge system related to the keyword is systematically made, so that the recommendation is superior in quality.

4.1 System Architecture

Based on knowledge graph, combining the content recommendation algorithm and collaborative filtering algorithms, this paper presents a collaborative filtering recommendation system of network document resource, which has a five data flow part comprising by data collection, data mining, data Fusion, data computing and data application. Figure 2 gives the architecture of our proposed system.

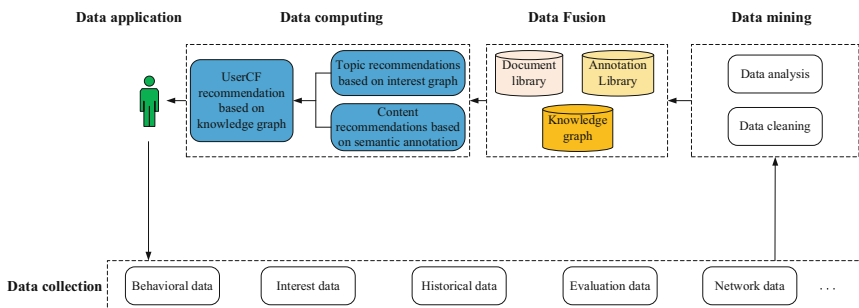


Fig. 2. System architecture

It mainly includes the following parts:

- (1) Data collection: Data sources include user behavior data, user interest data, system historical data, resource evaluation data, and network data. These data are the basis for building knowledge maps and recommending. They need to be processed through the data mining part.
- (2) Data mining: Performing data cleaning and analysis on the collected data. Then the processed data is aggregated into the data fusion part.

- (3) Data Fusion: Data from different data sources are processed integration of heterogeneous data under the same framework specification and stored in different types of databases for use in the data calculation part.
- (4) Data computing: Personalized recommendation results are obtained through user interest graph topic association interest recommendation, semantic annotation based content recommendation and knowledge map based UserCF recommendation, and transmitted to the data application part.
- (5) Data application: Display the recommended results to users according to the topic of network document resources. At the same time, relevant data is fed back to the data collection part.

4.2 The Description of Recommendation Algorithm

Topic Recommendations Based on Interest Graph. Through the user's interest graph, find other users associated with the user's interests, and then combine the other users who have acted in the document what the target user has acted on, and form a similar interest user set U_1 . At the same time, through the user's interest graph, the user's interest is extended to the topic layer, then perform the content-based recommendation, and remove the document what the target user has acted on, and obtain the corresponding document set L_1 .

Content Recommendations Based on Semantic Annotation. In the process of constructing the domain knowledge graph, the documents and instances are semantically annotated to obtain the triplet <document, instance, similarity> annotation library. Then, based on the user's attention graph instance, perform the content-based recommendation, and remove the document what the target user has acted on, and obtain the corresponding document set L_2 .

UserCF Recommendation Based on Knowledge Graph

Computing User Interest Similarity. In the system, the user interest similarity is defined sim , which is measured with the similarity between two user interest vector q and vector d , seeing Eq. (6):

$$sim(q, d) = \frac{\sum_{i=1}^n W_{i,q} W_{i,d}}{\sqrt{\sum_{i=1}^n W_{i,q}^2} \sqrt{\sum_{i=1}^n W_{i,d}^2}} \quad (6)$$

$w_{i,q}$ represents the weight of the interest keywords i in user q , $w_{i,d}$ represents the weight of the interest keywords i in user d , n is the number of the keywords in the user interest set. The matrix of the user interest similarity is obtained by processing with cosine similarity calculation between two user interest vector, seeing Table 1. The similar interest user set U_2 is obtained by computing the user interest similarity.

Table 1. The matrix of two users interest similarity

	u_1	u_2	u_3	u_4	u_5
u_1	1	0.2766	0	0.8620	0.1054
u_2	0.2766	1	0.3931	0.1144	0.2082
u_3	0	0.3931	1	0.6675	0.4932
u_4	0.8620	0.1144	0.6675	1	0.3704
u_5	0.1054	0.2082	0.4932	0.3704	1

Predicting User Document Behavior Evaluation. In the system, there is behavior evaluation between the user and the document. Six behavioral characteristics were selected as the users’ interest in the document to participate in the prediction score, selecting the highest behavioral score. Implicit scoring principle [23] which is used for reducing the degree of user participation in this paper. It marks 1 point when the user downloads the document; it marks 0.8 point when the user transponds the document; it marks 0.6 point when the user comments the document; it marks 0.4 point when the user collects the document; it marks 0.2 point when the user clicks the document; it marks 0.1 point when the user only browses the document; it marks ‘/’ when user does not browse the document. All users and documents form a behavior evaluation matrix at the same time, seeing Table 2.

Table 2. User document behavior evaluation

	d_1	d_2	d_3	d_4	d_5
u_1	0.1	0.2	/	0.1	0.4
u_2	0.3	0.1	0.6	0.1	/
u_3	0.1	0.8	0.2	0.6	0.2
u_4	0.6	0.6	1	0.8	1
u_5	/	1	0.4	0.2	0.6

Based on K users who are similar to the target user’s interest, find documents that K users like but the target user has not touched, and predict the target user’s interest in a document using the Eq. (7), and sort the documents according to the degree of interest and get the document set L_3 finally.

$$P(u, i) = \sum_{v \in S(u, K) \cap N(i)} w_{uv} r_{vi} \tag{7}$$

w_{uv} represents the interest similarity of two users u and v , r_{vi} represents the interest weight of the user v and the document i , $S(u, K)$ represents K users most similar to user u interests, $N(i)$ represents having acted on document i .

Input: domain knowledge graph KG , users set U , document set $docs$, < document name, instance, similarity > triple list

Output: recommendation document set

0. for $i = 1$ to n do
 1. computing user interest similarity $sim(q, d)$, and obtain a similar interest user set U_2
 2. for each user in users associated with the user's interests in KG do
 3. topic recommendations based on interest graph to obtain document set L_1 and obtain a similar interest user set U_1
 4. end
 5. for each individual ins in <document, instance, similarity> triplet list do
 6. content recommendations based on semantic annotation to obtain document set L_2
 7. end
 8. for each document in $docs$ the user u has not acted on do
 9. for each user in users of the intersection of U_1 and U_2 having acted on document j do
 10. predicting user document behavior evaluation $P(u, j)$ to obtain document set L_3
 11. end
 12. end
 13. do
 14. the intersection of L_1, L_2 and L_3 , then sort by TopN
 15. return recommendation document set
 16. end

5 Experiment and Evaluation

In order to verify the feasibility of the proposed system and its services, we conducted experiments in packaging industry. The data in the experiments are collected from government information, business information, industry information, academic papers, global packaging patents and other data resources, which add up to more than 3 million articles. We choose 28150 document resources for the experiment. Off-line experiments aimed at 10 users and pretreated their web usage access logs.

5.1 Experiment Environment Configuration

The experiment environment configuration is as shown in Table 3. We build a knowledge base of packaging knowledge graph covering information, policies, conferences, standards, papers, patents, companies, products, universities, institutions and experts. The instances in the knowledge graph are stored in MongoDB via Key Value. The data of semantic annotation library are stored in ES in triples. Network document resource are also stored in ES.

Table 3. Experiment environment configuration

Name	Versions
Operating system	CentOS6.5
Java runtime environment	jdk 1.8.0_141
Application server	apache-tomcat-9.0.16
Mahout	Mahout 0.9
Program development platform	IntelliJ IDEA 13.1.2
Data bases	MySQL5.6, mongodb-linux-x86_64-3.4.10 and elasticsearch-5.4.2

5.2 Constructing Packaging Knowledge Graph

We construct a packaging knowledge graph [20], which is as shown in Fig. 3. For example, the knowledge graph includes the following basic concepts, namely, “packaging knowledge point”, “Company”, “Product”, “Organization”, “Patent”, “Paper” and “Event”. Major relations include “has product”, “upstream”, “downstream”, “has patent”, and “executive”.

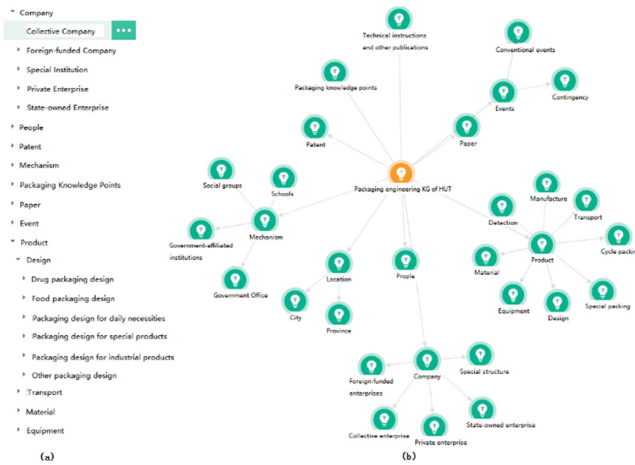


Fig. 3. Packaging knowledge graph

5.3 Algorithm Evaluation

In this paper, we adopt an evaluation method that calculating the precision rate, recall rate and F-measure value.

The Precision Rate calculation formula is as follows:

$$P = \frac{\text{The number of documents searched that users are interested in}}{\text{The total number of the documents searched}} \quad (8)$$

The Recall Rate calculation formula is as follows:

$$R = \frac{\text{The number of documents searched that users are interested in}}{\text{The total number of the documents}} \quad (9)$$

The F-measure Value calculation formula is as follows:

$$F_1 = \frac{2 \times R \times P}{R + P} \quad (10)$$

Through the system implementation, we put part of the data of the matrix of two users interest similarity and user document behavior evaluation in Tables 1 and 2, and give recommendation results by using the traditional collaborative filtering recommendation and proposed personalized collaborative filtering recommendation Based on knowledge graph. The experimental results are as shown in Table 4.

Table 4. Experimental results

Algorithm	Precision rate	Recall rate	F ₁ value
Traditional content-based recommendation	0.322	0.215	0.258
Traditional collaborative filtering recommendation	0.399	0.266	0.319
Proposed personalized collaborative filtering recommendation Based on knowledge graph	0.605	0.403	0.484

From the results of Table 4, we can see that the improved personalized collaborative filtering recommendation algorithm has higher precision rate, recall rate and F-measure value than the traditional collaborative filtering recommendation algorithm, indicating that the use of domain knowledge graph helps to enhance the semantic information of data and improve the quality of recommendations.

6 Conclusion

With the explosive growth of information on the Internet, the mining of multi-source heterogeneous data is a key issue in the recommendation system. The emergence of knowledge graph brings a new opportunity for the integration processing of multi-source heterogeneous data in the recommendation system. Therefore, the recommendation system based on knowledge graph has become a new research field. In this paper,

based on packaging industry knowledge graph, the authors, by joining the content-based recommendation and collaborative filtering-based recommendation algorithms, provide a technical implementation scheme for the personalized collaborative filtering recommendation system of network document resource. The experimental results show that the proposed system in this paper improves the recommendation quality.

The next step is to apply deep learning to learn and text eigenvector, researches on personalized recommendation system based on emotion analysis, experiments in packaging evaluation corpus, and constructs a complete packaging big data recommendation system.

Acknowledgment. This work is supported in part by the National Natural Science Foundation of China under grant number 61502163, in part by the Hunan Provincial Natural Science Foundation of China under grant numbers 2016JJ5035 and 2016JJ3051, in part by the Hunan Provincial Key Research and Development Project of China under grant numbers 2019GK2133, in part by the Scientific Research Project of Hunan Provincial Department of Education under grant number 16C0865 and name “Research on Key Technology of Intelligent Question Answering System in Packaging Field Based on Knowledge Graph”, in part by the Project of China Packaging Federation under Funding Support Numbers 17ZBLWT001KT010, in part by the National Packaging Advertising Research Base and Hunan Packaging Advertising Creative Base under grant number 17JDXMA03, in part by the Intelligent Information Perception and Processing Technology Hunan Province Key Laboratory under grant number 2017KF07.

References

1. Meng, X.W., Hu, X., Wang, L.C., Zhang, Y.J.: Mobile recommender systems and their applications. *J. Softw.* **24**(1), 91–108 (2013)
2. Amit, S.: Introducing the knowledge graph. Official Blog of Google, America (2012)
3. Chang, L., Cao, Y.T., Sun, W.P., Zhang, W.T., Chen, J.T.: Review of tourism recommendation system research. *Comput. Sci.* **44**(10), 1–6 (2017)
4. Pazzani, M.J.: A framework for collaborative, content-based and demographic filtering. *Artif. Intell. Rev.* **13**(5–6), 393–408 (1999)
5. Gunawardana, A., Shani, G.: A survey of accuracy evaluation metrics of recommendation tasks. *J. Mach. Learn. Res.* **10**(10), 2935–2962 (2009)
6. Ju, B., Qian, Y.T., Ye, M.C.: Preference transfer model in collaborative filtering for implicit data. *Front. Inf. Technol. Electron. Eng.* **17**(6), 489–500 (2016)
7. Burke, R.: Knowledge-based recommender systems. *Encycl. Libr. Inf. Syst.* **69**(32), 180–200 (2000)
8. Adomavicius, G.: Incorporating contextual information in recommender systems using a multidimensional approach. *ACM Trans. Inf. Syst.* **23**(1), 103–145 (2005)
9. Yuan, J., Ding, S.: Research and improvement on association rule algorithm based on FP-growth. In: Wang, F.L., Lei, J., Gong, Z., Luo, X. (eds.) *WISM 2012*. LNCS, vol. 7529, pp. 306–313. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33469-6_41
10. Meng, X.W., Liu, S.D., Zhang, Y.J., Hu, X.: Research on social recommender systems. *J. Softw.* **26**(6), 1356–1372 (2015)
11. Yu, S.S., Su, J.D., Li, P.F.: Improved TextRank-based method for automatic summarization. *Comput. Sci.* **43**(6), 240–247 (2016)

12. Hu, F.Y.: Research and implementation of hybrid recommendation algorithm based on user interest and topic model. Beijing University of Posts and Telecommunications, Beijing (2018)
13. Hu, C., Meng, X.W., Zhang, Y.J., Du, Y.L.: Enhanced group recommendation method based on preference aggregation. *J. Softw.* **29**(10), 3164–3183 (2018)
14. Yin, Y., Feng, D., Shi, Z.: A personalized paper recommendation method based on utility. *Chin. J. Comput.* **40**(12), 2797–2811 (2017)
15. Park, H.-S., Yoo, J.-O., Cho, S.-B.: A context-aware music recommendation system using fuzzy Bayesian networks with utility theory. In: Wang, L., Jiao, L., Shi, G., Li, X., Liu, J. (eds.) FSKD 2006. LNCS (LNAI), vol. 4223, pp. 970–979. Springer, Heidelberg (2006). https://doi.org/10.1007/11881599_121
16. Manouselis, N., Costopoulou, C.: marService: multiattribute utility recommendation for e-market. *Int. J. Comput. Appl. Technol.* **33**(2–3), 176–189 (2008)
17. Liu, Q., Li, Y., Duan, H., Liu, Y., Qin, Z.G.: Knowledge graph construction techniques. *J. Comput. Res. Dev.* **53**(3), 582–600 (2016)
18. Xu, Z.L., Sheng, Y.P., He, L.R., Wang, Y.F.: Review on knowledge graph techniques. *J. Univ. Electron. Sci. Technol. China* **45**(4), 589–606 (2016)
19. Hu, F.H.: Chinese knowledge graph construction method based on multiple data sources. East China University of Science and Technology, Shanghai (2014)
20. Li, C.Y., Wu, Y.Z., Hu, F.H.: Establishment of packaging knowledge graph based on multiple data sources. *Revista de la Facultad de Ingeniería* **32**(14), 231–236 (2017)
21. Chang, L., Zhang, W.T., Gu, T.L., Sun, W.P., Bin, C.Z.: Review of recommendation systems based on knowledge graph. *CAAI Trans. Intell. Syst.* **14**(2), 207–216 (2019)
22. Wu, Y.Z., Wang, Z.H., Chen, S.H., Wang, G.J., Li, C.Y.: Automatically semantic annotation of network document based on domain knowledge graph. In: 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications, Guangzhou, China, pp. 715–721 (2017)
23. Ryohei, S., Tetsuji, K., Hiroshi, Y.: User behaviour modelling by abstracting low-level window transition logs. *Int. J. Comput. Sci. Eng.* **11**(3), 249–258 (2015)



Short Text Representation Model Construction Method Based on Novel Semantic Aggregation Technology

Dong Yi¹(✉), Zhai Jia², Li Xin³, and Chen Feng¹

¹ Science and Technology on Optical Radiation Laboratory, Beijing 100000, China
18810331577@sina.cn

² Science and Technology on Electromagnetic Scattering Laboratory,
Beijing 100000, China

³ Beijing Institute of Electronic System Engineering, Beijing 100000, China

Abstract. The semantic representation model of short texts has insufficient semantic representation ability, and the semantic representation method of short text based on the combination of word embedding and semantic weight is low in computational complexity and its performance is even better than that based on complex structure such as RNN and LSTM. This paper proposes a semantic representation model of short text based on ELMO (Embeddings from Language Models). The innovation of this model is: firstly, it is adopted the more advanced word embedding model ELMO; secondly, it is designed the semantic keyword extraction method of short text based on the topic model (Latent Dirichlet Allocation, LDA); thirdly, the stochastic gradient descent (SGD) is adopted, which is used to learn the semantic weights of semantic keywords in short texts. The experimental results show that compared with the existing short text semantic representation model, the representation model of short text, which is proposed in this paper, shows a high semantic representation ability of short text in specific domain and in the open domain.

Keywords: Short text representation model · ELMO · Topic model · Stochastic gradient descent

1 Introduction

Word vector can effectively capture the contextual semantic information and grammatical information of words, and it realizes the vectorized representation of words. It is a bridge for computer to understand human language. Therefore, various types of word embedding models emerge one after another, such as word embedding model based on statistical methods [1], word embedding model based on neural network language model word2vec [2] and it is recently proposed word

Supported by Science and Technology on Optical Radiation Laboratory.

© Springer Nature Singapore Pte Ltd. 2019

H. Ning (Ed.): CyberDI 2019/CyberLife 2019, CCIS 1137, pp. 107–118, 2019.

https://doi.org/10.1007/978-981-15-1922-2_7

embedding model based on deep learning ELMO [3]. Vector representations of words are constantly emerging, which improves the semantic representations of word vectors. However, the current research on efficient vector representations for short texts (sentences, paragraphs, etc.) is still facing great challenges [4].

Currently, short text representation methods are based on complex networks (RNN, CNN) and word vector [11]. Le et al. [5] proposed an unsupervised text representation method (paragraph2vectors) that uses a method similar to Word2Vec [2], and can learn from variable length text fragments (such as sentences, paragraphs and documents) to a fixed length vector representation. Kiros et al. [6] proposed a generalized distributed sentence codec for unsupervised learning and trained the encoder-decoder model by using continuous text, which attempts to reconstruct sentences around the encoded paragraph and the sentences of share semantics and syntax information are mapped into a vector representation. Tai et al. [7] proposed a Tree-Lstm text semantic representation model based on tree structure, which introduced the standard LSTM structure into the tree structure network topology and achieved a superior sequence structure. The sentence vector representation capability of LSTM.

However, compared with the text representation method based on complex network, the methods based on word vector often have low computational complexity and satisfactory results. Generally, it can be achieved by averaging or maximizing the word vectors in short texts [8, 9]. Wieting et al. [10] used a word vector and a semantic pair dataset to construct a text representation model by training the word average model. This method has excellent performance in natural language processing tasks, especially in text similarity, its performance is better than unweighted word vector averaging and even better than text representation models based RNN/CNN. Arora et al. [11] used a mainstream word vector representation model in unlabeled corpus (such as Wikipedia) to represent text by weighted averaging of word vectors, while using principal component analysis (PCA)/singular value decomposition (SVD) to fine-tuning, this text representation method improves the performance of text similarity measurement by about 10% to 30%. Boom et al. [12] constructed a short text representation model by weighted combination of inverse document frequency IDF and Wode2Vec and proved its validity in short text matching tasks. On this basis, a short text representation model based on Wode2Vec (*Word2Vec-SGD*) was proposed, that is, each word in the short text is given a corresponding weight by a random gradient descent algorithm, and then the word vectors corresponding to the respective words in the short text are weighted and summed to obtain a vector representation of the short text.

Inspired by [12], this paper proposes a novel semantic aggregation technique based on the latest word vector generation model ELMO to construct a short text representation model. On the one hand, the semantic aggregation technique uses the LDA to extract the semantic keywords in the short text, thereby reducing the interference on words that are not related to the semantic expression of the short text, and reducing the computational redundancy in the subsequent training process of the semantic weight parameters; on the other hand, the Stochastic

Gradient Descent (SGD) is used to optimize the semantic keyword weights to give corresponding weights according to the importance of semantic keywords in short text semantic expression. The experimental results show that the proposed short text semantic representation model has excellent ability of semantic representation and domain adaptability.

2 Related Work

2.1 Word Embedding

ELMO [3] that is proposed recently can capture the semantic and syntactic information of words, and can also consider the situation in which words can express different meanings in the different context. Then, compared with the mainstream word vector model Word2Vec [2], it solves the problem of polysemy, and can obtain more accurate vector representation of words. The model is characterized by the fact that the characterization of each word is a function of the entire input. The specific method is to train the bidirectional long-term memory network model (bi-Lstm) with the language model as the target, and then use LSTM to generate the semantic vector of the words. The ELMO representation is “deep”, that is, the word vector generated by ELMO is a function of the internal characterization of all layers of bi-Lstm to get the rich representation of words. The high-level LSTM can capture related features such as word semantics and context, while low-level LSTM can find grammatical features. Therefore, this paper will use the advanced word vector model ELMO to build a more semantic characterization ability of the representation model of short text.

2.2 LDA

LDA model is a bayesian unsupervised probability model with three-layer structure of word, topic and document, which can model the underlying topic information in the document [13]. The model makes the assumption that each word is extracted from a potential topic, each article is the probability distribution of the topic, and each topic is the probability distribution of the word.

Figure 1 shows the graph model of LDA, where V represents the number of dictionaries in the training corpus and M represents the number of documents in the training corpus, N_m represents the total number of words in m_{th} the document in the training corpus, and K represents the number of topics. θ_m represents the probability distribution of all topics in the m_{th} document, $Z_{m,n}$ represents the n_{th} topic in the m_{th} document, $W_{m,n}$ represents the n_{th} word of the m_{th} document, φ_K represents the probability distribution of all words in the n_{th} topic; θ_m is the Dirichulet prior distribution of super-parameter α , recorded as $\theta_m \sim \text{Dirichulet}(\alpha)$, φ_K is the Dirichulet prior distribution of super-parameter β recorded as $\varphi_K \sim \text{Dirichulet}(\beta)$.

The purpose of the LDA is to find potential topics in the document. It can be seen from Fig. 1 that the theme probability distribution θ_m ($m = 1, 2, \dots$,

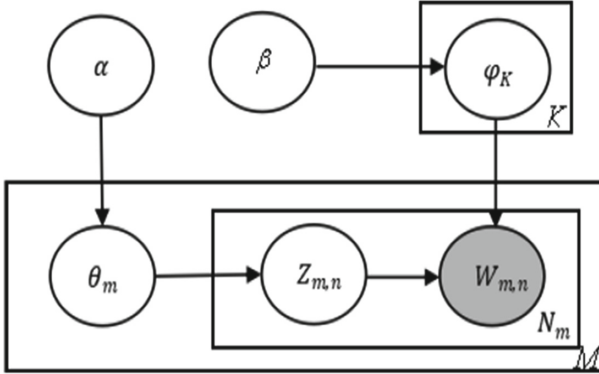


Fig. 1. The graph model of LDA

M) of the document is obtained according to the Dirichlet prior distribution Dirichlet (α). Then, the probability distribution of each potential topic φ_K ($k=1, 2, \dots, K$) in the document is obtained according to the Dirichlet prior distribution. In other words, the generation process of each word $W_{m,n}$ ($n=1, 2, \dots$) in any document D_m ($m=1, 2, \dots, M$). Extract a topic $Z_{m,n}$ from the multinomial distribution $Multi(\theta_m)$ corresponding to the document, and then extract a word $W_{m,n}$ from the multinomial $Multi(\varphi_K)$ corresponding to the topic $Z_{m,n}$. If the process is repeated N_m times, the document D_m is produced. This paper will use LDA's powerful text topic modeling ability to propose a short text semantic keyword extraction method based on LDA.

3 Short Text Representation Model Based on Novel Semantic Aggregation Technology

In order to improve the semantic representation ability of short text representation model, this paper adopts the advanced word vector model ELMO, and combines the semantic weighting scheme based on LDA and SGD to propose a novel short text representation model (STRM-SAT). The flow chart of the algorithm is shown in Fig. 2, including data preprocessing and semantic aggregation techniques.

3.1 Data Preprocessing

Data preprocessing is the first step of the STRM-SAT algorithm, which is mainly to perform lemmatization, word deduplication, and removing stop words on short texts. Then, for any short text $Text(w_1, w_2, \dots, w_N)$, N represents the total number of words in the short text, and it is obtained the word sequence $Sequence_{word}(s_1, s_2, \dots, s_M)$ about the short text after the data pre-processing. Where M is the number of words contained in the word sequence and $M \leq N$. This step mainly uses StanfordParser to do the above.

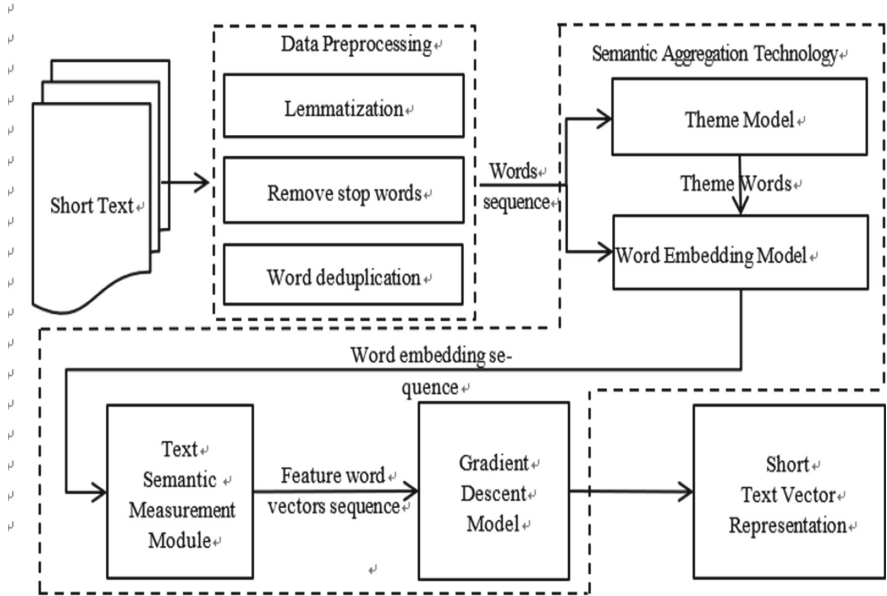


Fig. 2. Algorithm flow of STRM-SAT

3.2 Semantic Aggregation Technology

This paper proposes a novel semantic aggregation technique, which is based on the advanced Word embedding model ELMO, and fused LDA and SGD, to construct a vector representation of short text. It should be pointed out that there are some words in the short text that are useless to their semantic expression or no clear semantic meaning. These words appear in many short texts, so there is more coincidence between non-related short texts. Deleting these words from short texts or reducing their impact helps to reduce their interference with the overall semantic expression of short texts. Based on this, the LDA is introduced in the new semantic aggregation technology to design a short text semantic keyword extraction method based on LDA. On the other hand, the SGD is introduced to design a keyword semantic weight learning mechanism based on SGD.

Short Text Semantic Keyword Selection Mechanism Based on LDA.

The LDA can learn potential topic information from largescale corpus. Then, the topic words is obtained through LDA for any short text, those topic information can be regarded as a highsummary expression of short text semantic information. Therefore, the semantic distance must be close between a word, which plays a key role in the semantic expression of a short text, and the sequence of the topic words.

Based on above, this paper constructs a semantic keyword extraction method based on LDA to obtain semantic keywords in short text. The specific calculation

steps are as follows: firstly, the topic word sequence $Sequence_{topic}(t_1, t_2, \dots, t_K)$ of the corresponding short text is obtained through the trained LDA model, where K represents the number of topic words, and then the word vector sequence F and H about A and B are respectively obtained according to the trained ELMO; then, it is calculated the semantic distance between $s_m(0 < m \leq M)$ and $Sequence_{topic}$, ie.

$$Dis = \frac{1}{K} \sum_{k=1}^K \frac{v_{sm} \cdot v_k}{|v_{sm}| \times |v_k|} \quad (1)$$

Therefore, the semantic distance between each word in the short text and $Sequence_{topic}$ is sequentially calculated by formula (1) to determine the semantic keyword sequence $Sequence_{features}(f_1, f_2, \dots, f_H)$ of the short text, where H represents the total number of semantic keywords. After many experiments, it is verified that H takes 20, and the words in $Sequence_{features}$ are arranged in descending order according to the semantic distance.

Keyword Semantic Weight Learning Mechanism Based on SGD.

Through the above steps, the semantic keywords of short text can be obtained. However, the semantic keywords in $Sequence_{features}$ are different in the semantic expression of short text. Therefore, this paper uses the machine learning algorithm to learn the corresponding weighting factors β_g of semantic keywords, $g \subseteq [1, H]$, in the semantic expression of short text from the large-scale corpus to obtain the short text semantic vector. The specific idea is as follows: As shown in Fig. 3, the vector representation sequence $Vec(v_{f_1}, v_{f_2}, \dots, v_{f_H})$ of $Sequence_{features}(f_1, f_2, \dots, f_H)$ is obtained by the trained ELMO model. Next, v_{f_g} is multiplied by its corresponding weighting factor β_g , and summing and averaging to obtain the feature vector of the short text. The calculation formula is as shown in (2):

$$V = \frac{1}{H} \sum_{g=1}^H \beta_g \cdot v_{f_g} \quad (2)$$

In order to learn the weighting factor β_g in Eq. (2), a loss function is defined in this paper. For any short text pairs $p(V_1, V_1)$, if p is semantically related, maximize the semantic similarity between short texts in p ; if p is semantically uncorrelated, minimize the semantic similarity between short texts in p :

$$f(p) = \begin{cases} SC(V_1, V_2) & , \text{ if } p \text{ is related} \\ -SC(V_1, V_2) & , \text{ if } p \text{ is unrelated} \end{cases} \quad (3)$$

$SC(\cdot)$ is a function to measure the semantic distance between two short texts. This paper uses the cosine of the short text feature vector to measure the semantic distance:

$$SC(V_1, V_2) = \frac{V_1 \cdot V_2}{|V_1| \times |V_2|} \quad (4)$$

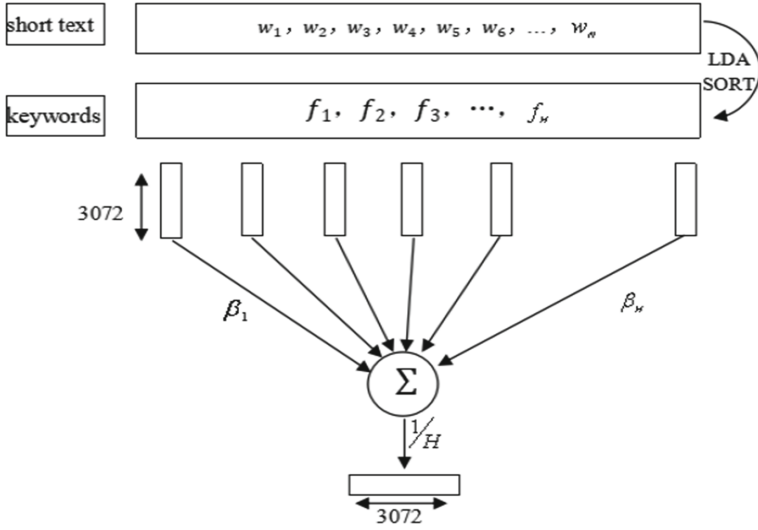


Fig. 3. The calculation process of short text semantic aggregation

Next, the paper constructs the following objective function of the weighting factor:

$$S(\beta_1, \beta_2, \dots, \beta_h) = \frac{1}{|D|} \sum_{p \subseteq D} f(p) + \lambda \sum_{j=1}^h \beta_j^2 \tag{5}$$

where the corpus D is composed of short text pairs and the number of semantically related short text pairs is the same as the number of non-semantic related short text pairs, and $|D|$ represents the total number of short text pairs in D . In order to maximize the objective function, this paper uses the stochastic gradient descent algorithm (SGD). Figure 4 shows the changes in the semantic weighting factors, which obtained by SGD. Obviously, as the index of semantic keywords increases, the value of the weighting factor decreases gradually. This indicates that the closer the semantic distance between the sequence of theme words of short text and keyword, the weighting factor of this keyword is the larger, so it is more important in the semantics expression of the short text.

4 Experiment and Result Analysis

Next, the short text matching task is used to verify the validity of the short text representation model STRM-SAT proposed in this paper. The performance of STRM-SAT in specific fields and open fields will be verified on the self-built corpus and the public corpus respectively.

The control methods we used are described as follows:

XXX_ Mean: the model of short text representation is constructed by adding and averaging the word vectors in the short text.

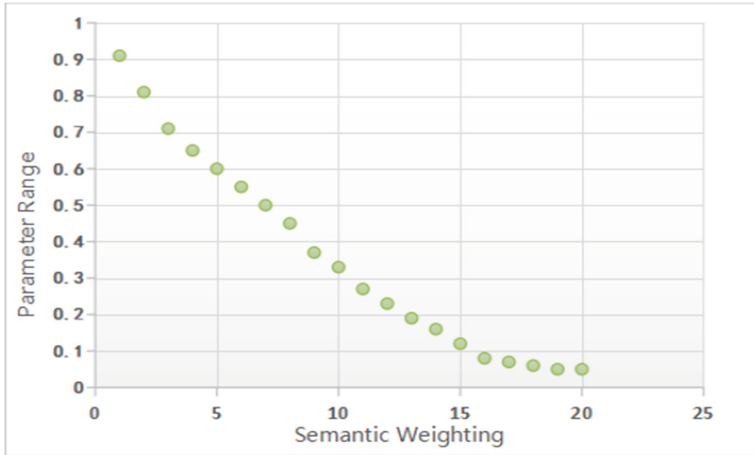


Fig. 4. Trend of semantic weighting factor

XXX_Idf: Constructing a short text representation model by using the inverse document frequency (idf) of each word in the short text as the weight and the word vector is multiplied by the corresponding weight to be added and averaged.

XXX_Top30%_Idf: the words in the short text are sorted according to their idf values from large to small, and the word vectors corresponding to the first 30% of the words are multiplied by the corresponding idf to be added and averaged, and the short text representation model is constructed.

Among them, “XXX” represents the word vector model, we use Word2Vec, ELMO_3072 and ELMO_1024 respectively. At the same time, we also use Word2Vec_SGD for control experiment.

4.1 Short Text Matching Experiment Based on Domain Corpus

The corpus used in this experiment was crawled from the official website of PubMed and the official website of Journal of Neuroscience, mainly to verify the semantic representation ability of the short text representation models in the biomedical literature corpus.

Original corpus: The corpus used in this paper consists of two parts, one is the abstract data set $Corpus_{pubMed}$ from the PubMed official website, and the other is the full-text data set $Corpus_{neurosc}$ from the Journal of Neuroscience.

LDA training corpus consists of abstracts from the fields of depression, epilepsy, cytology, clinical medicine, and computer science in $Corpus_{pubMed}$.

Building a short text pairs corpus: the summaries of the papers associated with the depression or depression drug entity is extracted from $Corpus_{pubMed}$ to form a set A , and then the set B is consisted of a summary of different topics in A is then extracted from the $Corpus_{pubMed}$. Next, calculate the correlation of short text pairs based on the method described in [10]. The rules of the construction

of Corpus: firstly, calculate the correlation of any two short text pairs in A . If the value is greater than 0.7, mark it as a semantically related short text pair and join the $Corpus_{pairs}$. Then, take a short text from each of A and B and calculate the correlation. If the value is less than 0.3, mark it as a non-semantic related pair and add it to the $Corpus_{pairs}$. Finally, semantically related pairs and non-semantic related pairs take 50,000 each to form the final $Corpus_{pairs}$. $Corpus_{pairs}$ is divided into training set TS_1 and test set TS_2 according to 4:1, where TS_1 is used to train SGD and TS_2 is used for final short text matching experiment.

The training corpus of ELMO and Word2Vec is composed of $Corpus_{pubMed}$ and $Corpus_{neurosc}$. In addition, the dimension of ELMO adopts the three-layer feature and top-level feature respectively, and the corresponding vector dimension is 3072 and 1024, respectively, which are recorded as ELMO_3072 and ELMO_1024, respectively. The dimension of the Word2Vec word vector is 300. Then, the results of this experiment are shown in Table 1.

Table 1. Comparison of experimental results.

No	Algorithm	Precision
1	Word2Vec_Mean	73.87%
2	Word2Vec_Idf	71.13%
3	Word2Vec_Top30%_Idf	78.39%
4	Word2Vec_SGD	80.59%
5	ELMO_1024_Mean	74.12%
6	ELMO_1024_Idf	70.87%
7	ELMO_1024_Top30%_Idf	80.31%
8	STRM-SAT_1024	81.17%
9	ELMO_3072_Mean	73.57%
10	ELMO_3072_Idf	74.67%
11	ELMO_3072_Top30%_Idf	80.74%
12	STRM-SAT_3072	83.32%

According to Table 1, the model of short text representation using ELMO is better performance than the model of short text representation using Word2Vec in the task, and the higher the dimension of the ELMO, the better the performance of the short text representation model, which shows that on the one hand, the word vector generated by ELMO has more semantic representation ability than the word vector generated by Word2Vec; on the other hand, the higher the dimension of ELMO, the richer the semantic information can be captured and the more powerful the semantic representation ability.

In this experiment, XXX_Top30%_Idf improved 5%–7% performance compared to XXX_Mean, while Word2Vec_SGD and STRM-SAT with finer semantic

weighting schemes showed higher performance, on the one hand, the weighted combination of word vector and inverse document frequency is effective, on the other hand, the weighting scheme used in Word2Vec_SGD and STRM-SAT uses the machine learning method to obtain more accurate weights, therefore, so, the better performance has been achieved.

Compared with Word2Vec_SGD, STRM-SAT performed better in this experiment. On the one hand, STRM-SAT eliminates these words that are useless or no clear semantic meaning for short text semantic expressions through the LAD. These words appear in many short texts, so there is more coincidence between unrelated short texts. These words are deleted from short text or reduced their impact to help to increase the values of similarity between similar short text pairs and reduce the values of similarity between non-similarity short texts. On the other hand, STRM-SAT adopts a more advanced word vector model ELMO, which not only can effectively capture the semantics of words and the grammar of words, but also can generate corresponding word vector representations according to the meaning of words in different contexts. Therefore, the word vectors, which is generated ELMO, are of higher quality, which is critical to the semantic representation of the STRM-SAT.

4.2 Short Text Matching Experiment Based on Open Domain Corpus

ELMO: The model is from the official website of ELMO (<https://allennlp.org/elmo>). ELMO's training corpus is from Wikipedia (1.9B) and WMT 2008–2012 (3.6B). The dimensions of the ELMO used in this paper are 3072 and 1024, respectively, which are recorded as ELMO_3072 and ELMO_1024, respectively.

Word2Vec: The model comes from its official website (<http://code.google.com/archive/p/word2vec/>), its training data comes from the Google News dataset (100 million words), and the dimension of vector is 300.

The training data of LDA uses the Wikipedia corpus used in [14]. The SGD training corpus uses the SemEval Semantic Text Similarity Task (2012–2015) data set used in [11]. The test data used in this experiment were from the SemEval Twitter task [15] and the SemEval semantic relevance task [16]. The experimental results are shown in Table 2.

As can be seen from Table 1, Word2Vec_SGD, STRM-SAT_1024, and STRM-SAT_3072 achieved good results, which is consistent with the results of short text matching experiments based on specific domain corpus. Further analysis shows that the weighted word vector method exhibits better semantic representation ability than the unweighted word vector method, and the vector representation of short text is obtained by way of the machine learning based semantic weighting scheme that is the best semantic representation ability. In addition, the STRM-SAT proposed in this paper has achieved the best results in the experiment due to the more effective word vector model ELMO and the semantic keyword extraction method based on machine learning.

Through the above experiments, the performance of STRM-SAT proposed in this paper is higher than other comparison methods, whether it is in specific

Table 2. Comparison of experimental results.

No	Algorithm	Precision
1	Word2Vec_Mean	80.10%
2	Word2Vec_Idf	80.42%
3	Word2Vec_Top30%_Idf	81.11%
4	Word2Vec_SGD	84.42%
5	ELMO_1024_Mean	78.23%
6	ELMO_1024_Idf	81.67%
7	ELMO_1024_Top30%_Idf	81.71%
8	STRM-SAT_1024	86.37%
9	ELMO_3072_Mean	79.88%
10	ELMO_3072_Idf	81.17%
11	ELMO_3072_Top30%_Idf	84.55%
12	STRM-SAT_3072	87.11%

domain or in the open domain test corpus. This shows the superiority of STRM-SAT, and also shows that STRM-SAT has strong domain adaptability.

5 Conclusion

This paper explores the semantic aggregation technology based on the advanced word vector generation model ELMO to construct the short text semantic representation model STRM-SAT, and designs the short text semantic keyword extraction method based on LDA and the keyword semantic weight learning mechanism based on SGD, which tries to combine the semantic information of the word vector in an optimal way to realize the Precise expression of short text semantic information. The order information of word plays an important role in semantic expression of short text. Therefore, in the future work, we will try to integrate the order information of word into the vector representation model of short text to realize the all-round modeling of short text from semantic to word order.

References

1. Bengio, Y., Ducharme, R., Vincent, P., Janvin, C.: A neural probabilistic language model. *J. Mach. Learn. Res.* **3**, 1137–1155 (2003). ISSN 15324435. <https://doi.org/10.1162/153244303322533223>
2. Mikolov, T., Sutskever, I., Chen, K., Corrado, G.S., Dean, J.: Distributed representations of words and phrases and their compositionality. In: *Advances in Neural Information Processing Systems*, pp. 3111–3119 (2013)
3. Peters, M.E., et al.: Deep contextualized word representations. In: *Proceedings of NAACL* (2018)

4. Conneau, A., Kiela, D., Schwenk, H., Barrault, L., Bordes, A.: Supervised learning of universal sentence representations from natural language inference data. In: EMNLP, pp. 670–680. Association for Computational Linguistics (2017)
5. Le, Q.V., Mikolov, T.: Distributed Representations of Sentences and Documents. [arXiv.org](https://arxiv.org/abs/1402.1728), May 2014
6. Kiros, R., Zhu, Y., Salakhutdinov, R.R., Zemel, R., Urtasun, R., Torralba, A., Fidler, S.: Skip-thought vectors. In: Advances in Neural Information Processing Systems (2015)
7. Tai, K.S., Socher, R., Manning, C.D.: Improved semantic representations from tree-structured long short-term memory networks. arXiv preprint [arXiv:1503.00075](https://arxiv.org/abs/1503.00075) (2015)
8. Weston, J., Chopra, S., Adams, K.: #TagSpace: semantic embeddings from hashtags. In: Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP) (2014)
9. dos Santos, C.N., Gatti, M.: Deep convolutional neural networks for sentiment analysis of short texts. In: The 25th International Conference on Computational Linguistics, COLING 2014, Dublin, pp. 69–78, July 2014
10. Wieting, J., Bansal, M., Gimpel, K., Livescu, K.: Towards universal paraphrastic sentence embeddings. In: International Conference on Learning Representations (2016)
11. Arora, S., Liang, Y., Ma, T.: A simple but tough-to-beat baseline for sentence embeddings (2017)
12. Boom, C.D., Canneyt, S.V., Bohez, S., et al.: Learning semantic similarity for very short texts, pp. 1229–1234 (2015)
13. Ghassabeh, Y.A., Rudzicz, F., Moghaddam, H.A.: Fast incremental LDA feature extraction. *Pattern Recogn.* **48**(6), 1999–2012 (2015)
14. De Boom, C., Canneyt, S.V., Demeester, T., et al.: Representation learning for very short texts using weighted word embedding aggregation. *Pattern Recogn. Lett.* **80**, 150–156 (2016)
15. Xu, W., Callison-Burch, C., Dolan, W.B.: SemEval-2015 task 1: paraphrase and semantic similarity in Twitter (pit). In: Proceedings of SemEval (2015)
16. Marelli, M., Bentivogli, L., Baroni, M., Bernardi, R., Menini, S., Zamparelli, R.: SemEval-2014 task 1: evaluation of compositional distributional semantic models on full sentences through semantic relatedness and textual entailment. In: SemEval-2014 (2014)



FLSTM: Feature Pattern-Based LSTM for Imbalanced Big Data Analysis

Liang Xu¹, Xingjie Zeng², Weishan Zhang²(✉), Jiangru Yuan³, Pengcheng Ren², Ruicong Zhang², Wuwu Guo², and Jiehan Zhou⁴

¹ University of Science and Technology Beijing, Beijing 100083, China

² China University of Petroleum, Qingdao 266580, Shandong, China
zhangws@upc.edu.cn

³ Research Institute of Petroleum Exploration and Development, Beijing 100083, China

⁴ University of Oulu, 8000, 90014 Oulu, Finland

Abstract. It is important for monitoring and predicting equipment failures. The existing fault prediction method has poor efficiency and accuracy on processing imbalanced data. This paper proposes a feature pattern-based LSTM method (called FLSTM, Feature based Long Short Term Memory) to analyze failures through processing imbalanced data. The method constructs a time-series feature matrix as the input to the LSTM model. In addition, we propose a failure prediction system based on Hadoop environment. The experimental results show that the FLSTM can improve failure prediction with imbalanced big data and the failure prediction system performs well.

Keywords: LSTM · Big data · Imbalanced data · Failure prediction

1 Introduction

Predicting failure is important for industry equipment. With the rapid development of Industrial Internet of Things, a large number of real-time data are collected, which provides useful data for failure prediction [1, 2]. There are lots of approaches to predict equipment failure, mainly including two types. The first one is traditional machine learning based approach. Chatrabgoun et al. [3] uses a statistical method to predict the probability of equipment failure with Bayesian, which requires a large amount of fault data and the same occurrence environment. However, the environment may change over time. With the development of deep learning, failure prediction with neural network has been developed. Nadai et al. [4] combines neural network with radial basis function to predict equipment failure, and achieves good results. But this method does not consider the time factor. As a typical time series data, the time factor should be applied. Therefore, Zhang et al. [5] proposed LSTM (Long Short Term Memory) [6] based method, and also graph neural network based approach [7], which improve the accuracy of fault prediction. However, due to the intrinsic LSTM structure, massive data

will make it difficult to train the LSTM model. At the same time, it requires data balance between positive and negative samples, or else, it is difficult to achieve good prediction performance. For massive unbalanced data, there still lack effective methods.

Taking air conditioner compressor as an example, there are 44 embedded sensors recording the operating parameters every half minute. These raw data have the following characteristics: (1) the data on the normal state are more than that on the failure state, which cause data imbalance; (2) the data collection is endless if the air conditioner is working. How to deal with massive continuous data and seriously unbalanced data has become a problem hindering the development of failure prediction.

To address these two challenges, this paper proposes a method based on feature patterns to extract failures in order to effectively process imbalanced big data (i.e., FLSTM). FLSTM aims to process imbalanced big data through reducing horizontal and vertical dimensions, it uses Tsfresh [8] to construct the time series matrix, and make failure prediction with the LSTM. For processing the failure prediction with big data well, a Hadoop¹ and Dask² based fault prediction system is also designed.

The contributions of this paper include:

- We propose the FLSTM method integrating feature pattern analysis with the LSTM to predict equipment failures.
- The FLSTM enables to process imbalanced data and improve failure prediction accuracy.
- We design an equipment failure prediction system based on Hadoop and Dask framework. The system can efficiently process big data and accurately make equipment failure prediction at real time.

The remainder of this paper is structured as follows. Section 2 shows the related works about equipment failure prediction. Section 3 presents the FLSTM method for failure prediction with imbalanced big data. Section 4 describes the device failure prediction system based on Hadoop environment. Section 5 draws a conclusion and presents the future work.

2 Related Work

There are lots of traditional machine learning based methods for failure prediction. Hyun-Keun et al. [9] proposed an open-switch fault detection method based on the spectrum analysis of the measured voltage and the current in the converter. Chatrabgoun et al. [3] proposed the Bayesian network pair-copula construction to solve the problem of asymmetric features and have good performance. Daneshkhah et al. [10] proposed the concept Partial Expected Value for Perfect Information to optimize the sensitivity analysis method and finally

¹ <http://hadoop.apache.org/>.

² <https://dask.org/>.

perform well for life-cycle management problem. But the above methods cannot handle high-dimensional data and has bad adaptability to other equipment data. Yuan et al. [11] combined two data-driven models and considered various data factors to predict transformer failures. This method only calculates data features such as average, variance, etc. with small-scale data.

The rapid development of deep learning promotes the development of failure prediction. Nadai et al. [4] proposed a Neural Network based on Radial Basis Function to support decision-making regarding operational performance of equipment. After training, the Neural Network was able to detect abnormal operational condition for hydro generator. Mei et al. [12] compared three RNN (Recurrent Neural Network) models for failure prediction with aero-engine data, and the experimental results show that the LSTM (Long Short-Term Memory) and GRU (Gated Recurrent Unit) models perform better than the conventional RNN. However, the LSTM is limited in processing imbalanced big data. Malhotra [13] proposed an LSTM-based life prediction model, which could not predict the type of future failures, and hard to address imbalanced data.

In order to serve the industrial site well, the failure prediction system is also a key requirement. Wang et al. [14] designed a laboratory equipment management and failure prediction system based on Web Service. Liu et al. [15] applied the Hadoop platform to the power equipment condition monitoring system, and proposed a Hadoop data storage query model based on virtualization technology. These existing systems are not efficient enough to process predict fault at real-time.

3 FLSTM Based Approach for Fault Prediction

The FLSTM based approach consists of five phases: data preprocessing, data dimension reduction, data skew processing, model design and model evaluation.

Data preprocessing mainly resolves missing and outliers in data, and normalizes the data.

Data dimension reduction reduce data dimension from 44 to 13 dimensions.

Data skew processing solves the problem that the failure data is seriously less than normal data.

FLSTM model design first makes data discretized, and then extracts the potential data patterns separately.

Model evaluation compares FLSTM with multiple models for accuracy and time consumption.

The following describes these steps in details.

3.1 Data Preprocessing

Outliers and Missing Values Processing. We firstly use expert experience to eliminate outliers and then fill them in the following way.

Assume that the data dimension is $m * n$, where n is the number of features of the data, and each line is a data sample. This paper fills the outliers with the

value of most similar samples. And sample similarity is calculated by Eq. 1, where y is the sample with outliers, x is the normal samples, and x_n and y_n are the remaining feature values after the outliers are removed from the samples. When the most similar samples are found, the outliers are replaced by the characteristic values of similar samples.

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2} \quad (1)$$

Normalization. There are two common normalization methods. One is to convert a number to a binary value between (0, 1), that is, 0–1 normalization. The other is the Z-score normalization. We adopt Z-score method in the paper since we could not determine the maximum and minimum values of the experimental data, and they are approximate to the Gaussian distribution. In Eq. 2, μ represents the mean and σ represents the variance.

$$x = \frac{x - \mu}{\sigma} \quad (2)$$

3.2 Dimension Reduction

There are 44 dimensions for the raw air conditioner data set. The FLSTM uses feature selection and data reduction to reduce dimensions.

The first step is to screen features based on their correlation coefficients and variances. The second step chooses the VarianceThreshold³ + PCA method for data dimension reduction. We finally reduce the 44 dimensions to 13.

3.3 Data Skew Processing

There are currently five main methods for data skew processing: sub-sampled, oversampling, hybrid method of sub-sampled and oversampling, integrated learning and batch generation method. For the air conditioner compressor data, the normal data are much more than the failure data. Data preprocessing only by oversampling will amplify the impact of failure data noise on the model. Therefore, we choose the hybrid method for data skew processing.

SMOTEENN [16] and SMOTETomek [17] are combined methods of oversampling and sub-sampled. The performance of experiments show that combined method does not greatly improve the overall F1-score, but has a low RMSE. The SMOTEENN method reduces the normal data and increases the failure data, which can reduce the calculation overhead of the subsequent algorithm. Therefore, the paper finally selects the SMOTEENN algorithm as the data skew processing method.

³ <https://scikit-learn.org>.

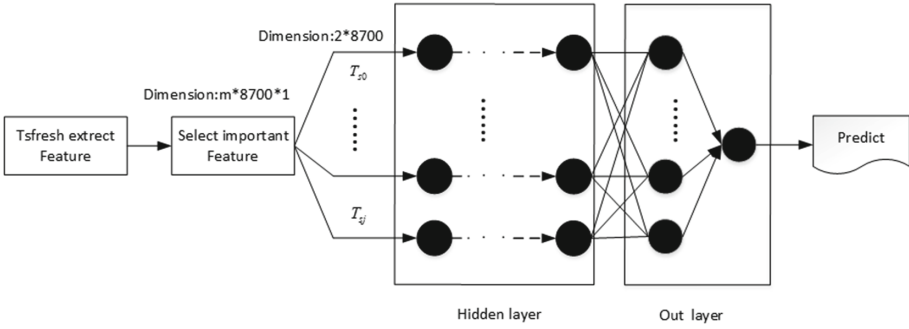


Fig. 1. Structure of FLSTM

3.4 FLSTM Model Design

Figure 1 presents the FLSTM network. First, the FLSTM uses the Tsresh for extracting features and selects 8700 features to represent a day's data which m is the number of days. The FLSTM combine multiple selected features with 8700 dimensions to construct time series, and the number used in Fig. 1 is 2, that is the S_i and S_{i+1} in Fig. 2. Finally, LSTM reshape the time series and training the network to realize failure prediction.

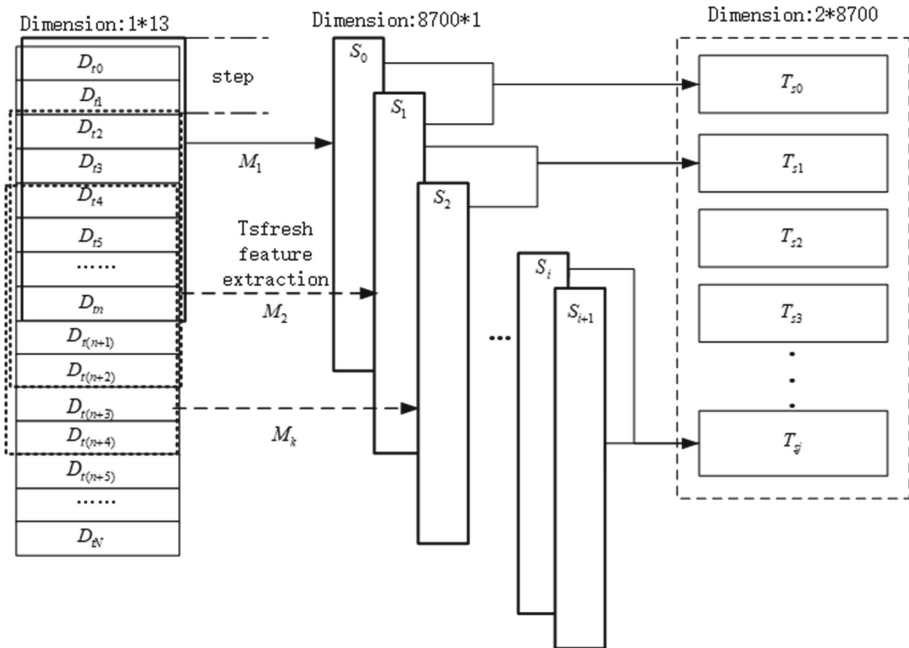


Fig. 2. Data processing flow of FLSTM

After data reduction by ArianThreshold+PCA, the data collected at one time would be 13 dimension. Then the processed data can be imported into FLSTM. Figure 2 presents the data processing flow of FLSTM, in which D_{tn} represents the data with 13 dimensions collected at time tn . We set the time interval between $t(n-1)$ and tn to 30s. Therefore, there are 2880 points in a day. In order to construct the time series, this paper uses the data of 2880 times to construct a time series matrix, that is, the data of 24h. For example, the time series matrix M_0 which consists of data from 0 to n^{th} ($n = 2880$)times is $[D_{t0}, D_{t1}, \dots, D_{tn}]$. And the time-series matrix is updated with a sliding window of size $step$. For clear description, the step in Fig. 2 is 2 times, which is 1 min for air conditioning data as data are collected every half minute. For example, M_1 and M_k are shown as follows.

$$M_0 = [D_{t0}, D_{t1}, \dots, D_{tn}] \quad (3)$$

$$M_1 = [D_{t0+step}, D_{t1+step}, \dots, D_{tn+step}] \quad (4)$$

$$M_k = [D_{t0+k*step}, D_{t1+k*step}, \dots, D_{tn+k*step}] \quad (5)$$

For each M_k , the feature is extracted by Tsfresh to generate a corresponding representation vector S_i which dimension is $8700 * 1$. In order to make the Tsfresh extracted vector have timing characteristics, this paper uses multiple S_i to construct the feature matrix T_{sj} of the timing vector. For example, T_{s0} and T_{s1} are shown as follows.

$$T_{s0} = [S_0, S_1, \dots, S_v] \quad (6)$$

$$T_{s1} = [S_1, S_2, \dots, S_{v+1}] \quad (7)$$

Where v is the number of time series vectors for constructing the feature matrix, and v is 2 in Fig. 2 for air conditioning data.

Finally, T_{sj} constitutes the data set as the input of LSTM. The hidden layer of the model contains multiple LSTM layers, and the number of neurons in each layer is the same. There is a drop layer between every two LSTM layers. The output layer of the model is a fully connected layer, and the final output of the model is derived from a sigmoid function.

3.5 Model Evaluation

We conducted the experiment with the following hardware configurations: Intel(R) Core(TM) i7-6700K CPU @ 4.00 GHz, GeForce GTX 1070, 16G memory.

We compared the FLSTM method with XGBoost [18], Tsfresh+XGBoost, and LSTM, We used 70% data as the training set and 30% as the test set.

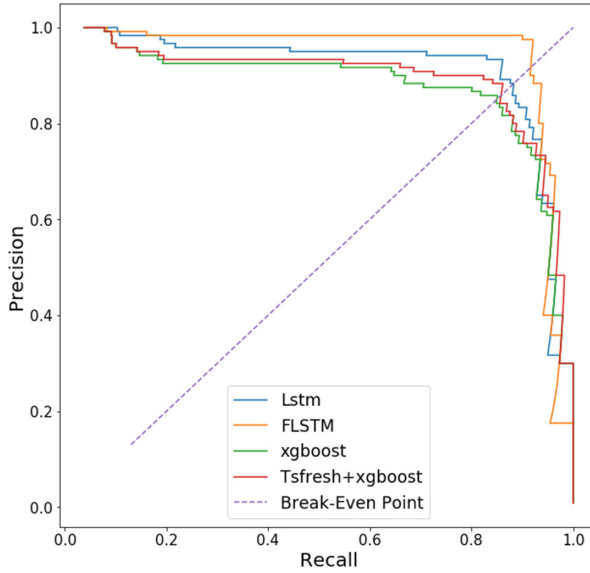


Fig. 3. P-R values with various algorithms

Figure 3 shows the P-R (Precision vs Recall) values with various algorithms. The area enclosed by the curve, the x-axis and y-axis indicates the algorithm accuracy. The larger the area is, the higher the accuracy. We cannot determine the area since the P-R curves in Fig. 3 have multiple intersections. Therefore, we introduce the Break-Even Point to differentiate the areas. The Break-Even Point refers to the point where the P value is equal to the R value. The larger the Break-Even Point is, the more accurate the algorithm is. The Break-Even Point values of FLSTM, LSTM, Tsfresh+XGBoost and XGBoost in Fig. 3 are 0.916, 0.883, 0.858, and 0.850. It means that FLSTM performs the best and XGBoost has the worst performance.

Table 1. Performance comparisons

	FLSTM	LSTM	Tsfresh+XGB	XGB
Time/s	3.254	0.0219	3.233	0.000216

Table 1 presents the performance of different algorithms with the average 10,000 operations. The experimental results show that when the Tsfresh is not used, the algorithm time is controlled within 0.1s. When Tsfresh is used, the overall running time of the algorithm increases about 3s. The operation speed of Tsfresh+XGBoost is slightly faster than that of FLSTM. The overall accuracy of LSTM is higher than XGBoost, but the time consumption is also higher than

XGBoost. In summary, XGBoost has the least time consumption and FLSTM has the best algorithm accuracy.

4 An FLSTM-Based Failure Prediction System

4.1 System Design

We design a FLSTM-based failure prediction system, which consists of a data layer, a service layer, a communication layer and a presentation layer, as shown in Fig. 4.

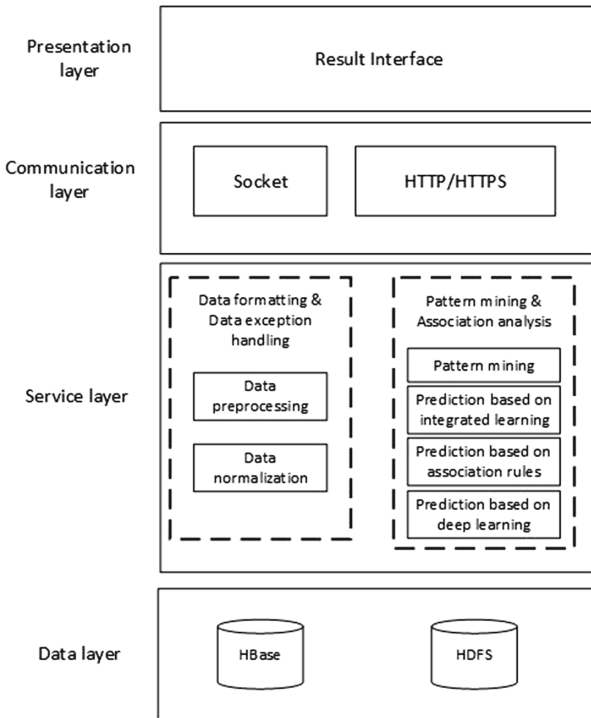


Fig. 4. System architecture

The data service module adopts a WEB-Server to avoid program failure problems caused by the interaction of multiple hosts and multiple environments, and realizes the push-pull combination of data in the form of two-way services.

Data asynchronous processing, message loss re-transmission, and resum-ing from break-point are realized while ensuring high-speed data transmission, thereby ensuring reliability and stability of bidirectional data transmission. The module not only pulls data from the cloud platform, but also feeds back the

results of the data prediction back to the cloud platform. In addition, the data service module and the data processing layer are isolated, and socket communication is used between these two layers.

The data analysis module is implemented in the service layer, where data processing and feature extraction are based on the Dask distributed computing framework, and the prediction is based on the Keras⁴ framework. The main functions of data processing are: data missing padding, detection and replacement of outliers, data normalization and data dimension reduction. The main function of the feature extraction and selection module is data feature extraction and selection. The main functions of data prediction are training, testing and operation of the prediction algorithm. In addition, the module supports features such as model replacement and data persistence. The data storage module is responsible for data storage services such as saving the model, saving the predicted results, and saving the extracted features. Since the amount of data will increase with time, this paper uses HBase⁵ and HDFS [19] as the data storage.

4.2 Evaluation of the System

The input of this FLSTM is a $(4*2880)*13$ -dimension matrix. This paper tests the system under two conditions: the first is to send multiple task requests to the distributed computing platform at the same time with same computing content; the second is to send multiple task requests to the distributed computing platform at the same time with different computing content. The experimental conditions and test results are shown in Tables 2 and 3.

Table 2. The test results under the first condition

Concurrency	1	2	3	4	5	6	10
Nodes	13	13	13	13	13	13	13
Time/s	3.39	3.46	3.54	3.55	3.53	3.49	3.65

It can be seen from Table 2 that the number of submitted tasks in the same period is 1, 2, 3, 4, 5, 6, and 10, and the experimental results are all running time averages of 100 times.

Table 3. The test results under the second condition

Concurrency	1	2	3	4	5	10	11
Nodes	13	13	13	14	15	17	17
Time/s	3.3	6.2	8.7	10.6	12.8	27.3	30.0

⁴ <https://keras.io/>.

⁵ <https://hbase.apache.org/>.

It can be seen from Table 3 that when the number of submitted tasks increases, the time consuming starts to rise gradually. When the platform can process multiple tasks concurrently, the average task takes about three seconds. In order to ensure that the task can obtain the calculation result within the effective time (the data collection interval is 30 s), the distributed computing platform submits at most 10 different tasks at the same time.

5 Conclusion

We propose the FLSTM approach, a feature-based LSTM for equipment failure prediction. The FLSTM integrates feature extraction and prediction algorithms to improve equipment failure prediction. The experimental results show that the accuracy of the FLSTM is improved compared to LSTM, with good performance for industrial usage. We deployed the FLSTM-based failure prediction system to an IoT company which has been work reliably for over half a year and shows the effectiveness of the solution.

In the future, we will continue the current research from two aspects: (1) minimizing the calculation for non-primary features; (2) reducing the data dimension while keeping the accuracy.

Acknowledgement. “This research is supported by the National Key R&D Program (2018YFE0116700), the Shandong Provincial Natural Science Foundation (ZR2019MF049, Parallel Data Driven Fault Prediction under Online-Offline Combined Cloud Computing Environment), the supporting project from China Petroleum Group (2018D-5010-16) for Big Data Industry Development Pilot Demonstration Project from Ministry of Industry and Information Technology, the National Major Science and Technology Project (2017ZX05013-002), the China Petroleum Group Science and Technology Research Institute Co., Ltd. Innovation Project (Grant No. 2017ycq02) and the Fundamental Research Funds for the Central Universities (2015020031).”

References

1. Ning, H., Liu, X., Ye, X., Zhang, J.H.W., Daneshmand, M.: Edge computing based ID and nID combined identification and resolution scheme in IoT. *IEEE Internet Things J.* **6**, 1 (2019)
2. Sikorska, J.Z., Hodkiewicz, M., Ma, L.: Prognostic modelling options for remaining useful life estimation by industry. *Mech. Syst. Sign. Process.* **25**, 1803–1836 (2011)
3. Chatrabgoun, O., Hosseinian-Far, A., Chang, V., Stocks, N.G., Daneshkhah, A.: Approximating non-Gaussian bayesian networks using minimum information vine model with applications in financial modelling. *J. Comput. Sci.* **24**, 266–276 (2018)
4. Nadai, N., Melani, A.H.A., Souza, G.F.M., Nabeta, S.I.: Equipment failure prediction based on neural network analysis incorporating maintainers inspection findings. In: *Reliability & Maintainability Symposium* (2017)
5. Zhang, W., et al.: Lstm-based analysis of industrial IoT equipment. *IEEE Access* **6**, 23551–23560 (2018)
6. Graves, A.: Long short-term memory. *Neural Comput.* **9**(8), 1735–1780 (1997)

7. Zhang, W., et al.: Modeling IoT equipment with graph neural networks. *IEEE Access* **7**, 32754–32764 (2019)
8. Christ, M., Braun, N., Neuffer, J., Kempa-Liehr, A.W.: Time series feature extraction on basis of scalable hypothesis tests (tsfresh - a python package). *Neurocomputing* **307**, 72–77 (2018)
9. Ku, H.-K., Im, W.-S., Kim, J.-M., Suh, Y.-S.: Fault detection and tolerant control of 3-phase NPC active rectifier, pp. 4519–4524, September 2012
10. Daneshkhah, A., Hosseinian-Far, A., Chatrabgoun, O.: Sustainable maintenance strategy under uncertainty in the lifetime distribution of deteriorating assets. In: Hosseinian-Far, A., Ramachandran, M., Sarwar, D. (eds.) *Strategic Engineering for Cloud Computing and Big Data Analytics*, pp. 29–50. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-52491-7_2
11. Yuan, D., et al.: Fault prediction of power electronics modules and systems under complex working conditions. *Comput. Ind.* **97**, 1–9 (2018)
12. Mei, Y., Wu, Y., Li, L.: Fault diagnosis and remaining useful life estimation of aero engine using LSTM neural network. In: *IEEE International Conference on Aircraft Utility Systems* (2016)
13. Malhotra, P., et al.: Multi-sensor prognostics using an unsupervised health index based on LSTM encoder-decoder. *CoRR*, abs/1608.06154 (2016)
14. Jie, W., Yu, Z.: Laboratory equipment management and failure prediction system based on web service. In: *IEEE International Conference on Software Engineering & Service Science* (2012)
15. Wang, Y., Sheng, W.: Research and implementation on spatial data storage and operation based on hadoop platform. In: *Second IITA International Conference on Geoscience and Remote Sensing* (2010)
16. Hemmat, R.A., Hafid, A.: SLA violation prediction in cloud computing: a machine learning perspective (2016)
17. Goel, G., Maguire, L., Li, Y., McLoone, S.: Evaluation of sampling methods for learning from imbalanced data. In: Huang, D.-S., Bevilacqua, V., Figueroa, J.C., Premaratne, P. (eds.) *ICIC 2013. LNCS*, vol. 7995, pp. 392–401. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39479-9_47
18. Chen, T., Tong, H., Benesty, M.: Xgboost: extreme gradient boosting (2016)
19. Veerabhadra Rao Chandakanna: REHDFS: a random read/write enhanced HDFS. *J. Netw. Comput. Appl.* **103**, 85–100 (2018)



A Construction Method of Author Influence Map Based on Data Field Theory and Entropy Weight Method

Jie Yu^(✉), Dongdong Wang, Lingyu Xu, and Rongrong Chen

School of Computer Engineering and Science, Shanghai University,
Shanghai 200444, China

{jieiye, wangdongdong, xly, rongrongchen}@shu.edu.cn

Abstract. In the face of a large number of academic paper and authors in various fields, building an intuitive and effective map about authors' influence and relationship can help us quickly screen and search for influential authors from a large number of authors, and then can be applied to author ranking, author recommendation and other systems. A method of building an author influence map is proposed in this paper. By introducing entropy weight method, each factor's contribution to evaluating an author's influence can be quantified. Based on data field theory, an author's influence in a specific field can be accurately evaluated. The relations between authors include cooperation relationship and reference relationship. In addition, this paper constructed the author influence map in the field of information retrieval, which proved the effectiveness of the method.

Keywords: Author influence map · Data field · Cooperation relationship · Reference relationship

1 Introduction

With the rapid development of information science and technology, information and data are exploding. It is an urgent problem to solve how to extract information effectively and discover knowledge in the face of massive information data. Knowledge Map uses the symbolic form to describe concepts and their relationships in the physical world. Through the analysis and process of structured knowledge, they are displayed graphically. With the development of scientific research in the field, a large number of scientific research results and academic papers have emerged. Faced with a large number of academic authors and complicated author relations, it is particularly important to construct the author influence map. Based on author map, we can explore the potential relationship between authors effectively and build a personalized recommendation system for authors. It also helps to analyze the research ability of individual authors, academic rankings, etc.

The work of building the author map focuses mainly on the evaluation of the author's influence and the author's relationship. H-index is a popular evaluation method in recent years and has been applied in the impact assessment of author and academic journals [1, 2]. A large h-index usually means that the author has great influence. Mccarty suggests that the highest h-index can be achieved by working with

many co-authors, at least some with high h-indexes themselves [3]. It has become a popular scientific measurement method because of its simplicity and intuitiveness. Kudelka proposed a new author evaluation measure named a h-index based on h-index to evaluate the citation quantity received by individual scientists [4]. In addition, authors' influence can also be analyzed based on the number of publications, the number of co-authors and the times cited. However, the author influence is not only reflected in the amount of static data, but also in the behavior that the author's point of view is noticed and communicated [5]. Meanwhile, the influence spreads through the relational path of cooperation and citation between authors, on which the authors should have similar academic interests. Author's cooperation network and citation network such as PageRank algorithm based on network structure can also be used to evaluate the author's influence. PageRank-based methods for evaluating authors' influence, namely Pub Rank, Star Rank and WMI Rank were introduced in [6]. An optimized topic-related PageRank algorithm was used to measure the ranks of publications and authors [7]. The study of the authors' relationship is mainly based on co-citation relationship and cooperation relationship. The citation content of authors was applied to measure the similarity between co-citation authors and construct the co-citation map of authors [8]. Based on all papers published in SIGMOD from 1975 to 2002, the author's cooperation relationship map was constructed [9]. Xu selected papers from 2005–2014 in CNKI series database, and used social network analysis method to study the author cooperation relationship of the digital publishing [10].

Author map not only can reflect the authors' influence but also reflect the relationships between them intuitively. Although some research achievements have been made, only a single factor, such as the number of publications or citations, has been considered in the evaluation of the authors' influence. Based on data field theory and entropy weight method, we put forward a method to construct author influence map, which evaluates the number of publications, the order of author's signature, the level of the publisher, the reference relationship among authors and the amount of citation comprehensively. Firstly, the entropy weight method is used to evaluate the author's contribution comprehensively by analyzing the different weight of the factors such as the quantity of publication, author's signature order, the level of the publisher and so on. Second, data field theory is introduced to measure the author's influence. Finally, the author influence map (AIM) which contains reference relationship, cooperation relationship and influence can be constructed.

The rest of this paper is organized as follows. The secondly section introduced the definition of AIM. The third section elaborates on the key techniques of measuring author's influence and the method of evaluating the author's relationship. The fourth section gives the experimental analysis and conclusion. The fifth section gives a summary of this paper.

2 Formal Definition of AIM

This paper presents an Author Influence Map (AIM) in academic fields. The AIM reflects the author's influence, cooperation relationship and reference relationship among different authors. The nodes in the AIM reflect the author's influence, and the

connection between nodes indicates the relationship such as reference relationship and cooperation relationship.

Definition 1: Author Influence Map (AIM).

$AIM = \langle A, R \rangle$, where

- $A = \{a_i\}$ is the set of nodes, each element represents the author of a particular academic field.
 - $a_i = \langle a_n_i, a_p_i \rangle$, a_n_i indicates the name of author a_i , and a_p_i indicates the influence of author a_i .
- R is a set of relations between authors, $R = QR \cup CR$, where
 - $QR = \{\langle a_j \rightarrow a_i \rangle\}$ denotes the reference relationship between authors, and the element $\langle a_j \rightarrow a_i \rangle$ denotes that author a_j refers author a_i 's paper.
 - $CR = \{\langle a_i, a_j \rangle\}$ denotes the cooperation relationship between authors, and the element $\langle a_i, a_j \rangle$ denotes author a_i and author a_j have completed at least one paper together.

It can be seen that the key issues in building AIM are: mining and measuring relations among authors, measuring authors' influence, which will be introduced in Sects. 3.1 and 3.2.

3 Construction of Author Influence Map Based on Data Field Theory and Entropy Weight Method

3.1 Mining Relations Between Authors

Reference Relations among Authors. There are reference relationships between different authors, which are directed relationships.

$$r_{a_j \rightarrow a_i} = \frac{C_{a_j \rightarrow a_i}}{MAX} \quad (1)$$

Formula (1) denotes the calculation method of reference weights between them. Where $a_j \rightarrow a_i$ denotes author a_j quotes author a_i 's papers. $r_{a_j \rightarrow a_i}$ denotes the weights of author a_j refers to author a_i 's papers. If $r_{a_j \rightarrow a_i}$ is larger than $r_{a_j \rightarrow a_k}$, it denotes that the author a_j refers to author a_i more closely than author a_k . $C_{a_j \rightarrow a_i}$ denotes the times of author a_j refers to author a_i 's papers, and MAX is the largest times in all reference relationships.

Cooperation Relations Among Authors. In a scientific research paper, there will be multiple co-authors, so these authors constitute cooperation relationships. The cooperation weights between authors indicate the degree of cooperation between authors, which is not only related to the times of cooperation between them, but also to the degree of cooperation in a single paper. The degree of cooperation can be measured through the author's contribution in a single paper. The order of authors' signature, whether they are the first authors or not, and whether they are a corresponding author

all can reflect the degree of authors' contribution. Therefore, the effective measurement of authors' contribution in a paper is the key to calculating the degree of cooperation between authors.

Contribution Degree of Authors in Different Signature Order. At present, there are many studies on the authors' contribution in different signature order. This paper adopts linear model [11, 12]. As shown in formula (2).

$$C(s, n) = \frac{(n - s + 1)}{\sum_{s=1}^n (n - s + 1)} = \frac{n - s + 1}{\frac{1}{2}n(n + 1)} \tag{2}$$

where n denotes the number of collaborators and s denotes the author's signature order. Without considering the corresponding authors, the author's contribution decreases linearly with the increases of the author's signature order, and the degree of decline is related to the number of authors. The degree of decline can be described in formula (3).

$$\Delta C = \frac{2}{n(n + 1)} \tag{3}$$

The value of n gets larger; the degree of decline get smaller. However, the value of n should not be too large, because ΔC varies little if n is too large. So the model can not accurately describe the impact of the number of collaborators on the contribution degree of authors.

The corresponding author is usually the first author of the paper, but some corresponding authors are not the first author. So the formula can be modified as follows after adding the factor of the corresponding author [12].

$$C(s, n, p, t, m) = \frac{n + 1 - s^{1-m}}{\frac{1}{2}n(n + 1) + p(t - 1)} \tag{4}$$

where s denotes the author's signature order, n is the number of authors in a paper. If there are corresponding authors, p is 1. Otherwise, p is 0. t denotes the corresponding author's signature position, m denotes whether the current author is the corresponding author, if true then $m = 1$, otherwise $m = 0$.

Degree of Cooperation Between Authors. The co-authors in each paper can form many cooperation relationships, but their cooperation degrees are different. The cooperation weight is the sum of multiple cooperation degree behaviors between authors. The cooperation degree of single cooperation is measured by the author contribution model mentioned above. We referred to the calculation method of cooperation degree in [12].

$$W_{i,j}^k = \frac{2(n + 1) - (S_i^{1-m_i} + S_j^{1-m_j})}{n(n + 1) + 2p(t - 1)} \tag{5}$$

where $W_{i,j}^k$ indicates the degree of cooperation between author i and author j in paper k . Based on the cooperation degree of a single co-authored paper, the total cooperation

degree between authors can be calculated, and the calculation formula is shown as follows.

$$W_{i,j} = \sum_k W_{i,j}^k \tag{6}$$

where $W_{i,j}$ denotes the total cooperation weights between author i and author j .

3.2 Assessment of Authors' Influence Based on Data Field

The author's influence is related to two aspects: the author's "quality" weights and the reference weights between authors. The specific flowchart of the author's influence process of the mechanism is shown in Fig. 1. Author's "quality" is the reflection of the author's own characteristics in academic research, which is related to the amount of publication, the publisher level and the order of signature. In a certain field, the more papers the author published, the higher the order of signatures in each paper and the higher the publisher level of the paper all will produce the greater "quality" for each author. Therefore, the author's "quality" weights are the comprehensive evaluation results of the several above indicators. We will describe in detail later about the calculation method of "quality" weights. The reference weights are related to the times of reference between them. Inspired by the idea of the physical field, we try to introduce the interaction between particles and the description method of their fields into abstract numerical space [13] and use data field theory to measure the author's influence. The above two aspects are considered comprehensively in the method.

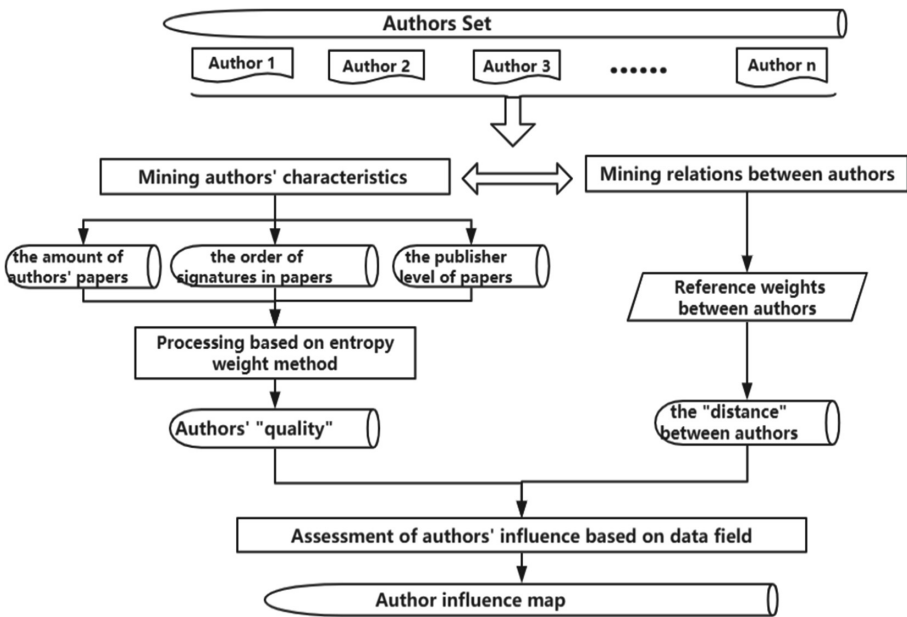


Fig. 1. Flowchart of overall process of author influence map

The Data Field of Authors. According to the data field theory, there are several entities in a range, and each entity will produce a field of potential energy. These fields also affect the surrounding entities. The size of the potential energy field of each entity is not only related to its own quality but also affected by the superposition of potential energy fields around it. The affection of the potential energy field around the entity is related to the distance between them. The smaller the distance, the greater the affection. Be applied to the academic field, and each author represents an entity which generates a data field. And they also are in the field produced by other authors and affected by the data field of other authors. The size of the data field of each author is not only related to its own “quality” factors but also related to the superposition the data field of the authors around him. The authors around him are the authors who quoted his papers. The larger the reference weights, the smaller the distance between them, and the greater the affection of the reference authors. Therefore, the value of the authors’ data field is a sum of his own field and others’ superposition field. The author’s influence can be expressed by the value of the data field. We use the Gauss formula to calculate the value of each author’s data field.

$$P(a_i) = W_{a_i} \sum_{j=1}^n W_{a_j} \times e^{-\left(\frac{\text{dis}(a_j \rightarrow a_i)}{\sigma}\right)^2} \quad (7)$$

$$\text{dis}(a_j \rightarrow a_i) = 1 - r_{a_j \rightarrow a_i} \quad (8)$$

where $P(a_i)$ denotes the data field of author a_i , σ is the balance parameter, $\text{dis}(a_j \rightarrow a_i)$ denotes the distance between author a_j and author a_i , and $r_{a_j \rightarrow a_i}$ denotes the reference weights between author a_j and author a_i . W_{a_i} represents “quality” weights of author a_i , and the next section describes in detail the calculation method of “quality” weights.

Evaluation of Author’s Quality Based on Entropy Weight Method. The author’s “quality” is mainly related to the number of papers published, the order of signatures in papers and the publisher level of papers. In this paper, we mainly analyze the three factors. To measure their contribution to the comprehensive evaluation of authors’ “quality”, we used the method of entropy weight.

The concept of information entropy is a measure to describe the degree of information disorder in a system. If the information entropy of an indicator is greater, the uncertainty of information will be greater and the amount of information provided will be smaller, so the contribution of the indicator will be smaller in the multi-indicator comprehensive evaluation. On the contrary, the smaller the indicator’s information entropy is, the larger the amount of information it provides and the larger the contribution it provides in the comprehensive evaluation. In this paper, the author’s publication quantity, the publisher level and the order of signature are taken as the indicators to evaluate the author’s “quality” comprehensively. Author’s publication quantity and publisher level can be obtained directly. And the order of authors’ signatures needs to be treated as the contribution degree of authors because the signature order can reflect the author’s contribution degree correctly in a paper. The higher the order of the author’s signature is, the greater the contribution degree is. The contribution degree decreases linearly with the increase of the order of signatures [13].

Suppose $AC = \{a_1, a_2, a_3 \dots a_n\}$ represents a set of authors. The author a_i 's publication quantity is X_{i1} , publisher level is X_{i2} and contribution degree is X_{i3} , and Y_{i1}, Y_{i2}, Y_{i3} are the results after normalization. Then the information entropy of three indicators is calculated as shown in formula (9).

$$H_j = -\ln(n)^{-1} \sum_{i=1}^n Y_{ij} \ln Y_{ij}, \quad j = 1, 2, 3, \quad i = 1, 2, 3 \dots n \quad (9)$$

where j denotes the above three indicators, and n denotes the number of authors set AC .

After calculating the information entropy of each indicator, the entropy weight of each indicator is clear. It can be calculated by formula (10).

$$w_j = \frac{1 - H_j}{k - \sum H_j}, \quad j = 1, 2, 3, \quad k = 3 \quad (10)$$

Obviously, when the information entropy H_j of indicator j reaches its maximum 1, and the entropy weight w_j is 0. It denotes that indicator j can hardly provide useful information when determining the author's "quality", so it occupies fewer weights in a comprehensive evaluation. After the entropy weights of the three indicators are obtained, the value of authors' "quality" can be obtained by formula (11).

$$W_{A_i} = \sum_{j=1}^k w_j Y_{ij}, \quad i = 1, 2, \dots n, \quad k = 3 \quad (11)$$

where W_{A_i} denotes the authors' "quality".

4 Experimental Analysis

This paper takes information retrieval as the target research field and takes the academic papers published in ACM SIGIR¹ conference and their authors as our experimental objects. We selected papers and authors from 2006 to 2015, and obtained a total of 2241 papers and 3207 different authors, including 7548 pairs of cooperation relationships and 29774 pairs of reference relationships (excluding self-citations). For the authors who have repeat names, we distinguish them mainly through the model of "author + institution".

4.1 Assessment of Authors' "Quality"

Measuring the author's "quality" is the key to calculate the author's influence. Due to the source data in the experiment are all from SIGIR, so the indicator of publisher level is not considered in this paper. We extracted all authors who appeared in the paper of ACM SIGIR conference from 2006 to 2015 as the author set $AC = \{a_1, a_2, a_3 \dots a_n\}$. And the number of each author's papers can be obtained from the ACM database. We extracted the paper and the author's signature order from SIGIR conference in 2006 to

¹ <https://dl.acm.org>.

2015. Then according to the method of authors' contribution mentioned in Sect. 3.1, we can conclude the total contribution degree of every author.

Different indicators occupy different importance in a comprehensive evaluation. This paper reflects the evaluation weights of each indicator through information entropy and entropy weights. The results are shown in Table 1.

Table 1. Information entropy of publication quantity and contribution degree.

	Publication	Contribution degree
The information entropy	0.91	0.93
The entropy weights	0.57	0.43

It can be seen that the information entropy of the amount of publication is a little smaller and the entropy weights is a little larger. Then the author's "quality" value is calculated based on the entropy weight method. We select author threshold as the core authors according to Price Formula.

$$M_p = 0.749\sqrt{N_{p\ max}} \tag{12}$$

The total number of authors $N_{p\ max}$ is 3207, and the number of selected core authors is $M_p = 42$. Due to space limitations, Fig. 2 shows the "quality" value of the top 20 authors.

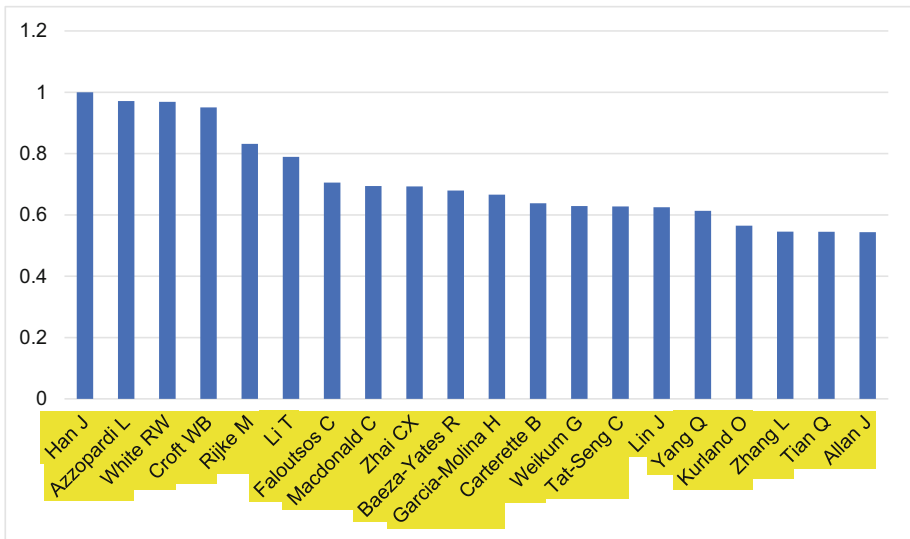


Fig. 2. Authors' "quality" weights

The author’s “quality” only reflects the author’s own characteristics, but not enough to reflect the author’s influence. In order to reflect the authors’ influence more accurately, we should also consider the impact of the author, who has a reference relationship with him.

4.2 Evaluation Results of the Author’s Domain Influence

After the reference relationship and weights between authors are extracted and the author’s “quality” is obtained, then we calculate the author’s data field value by formula (7). The data field value of authors can reflect the author’s influence.

Then we compare the authors’ influence with their “quality” weights. The top 20 authors’ influence values and top 20 authors’ “quality” weights are shown in Fig. 3.

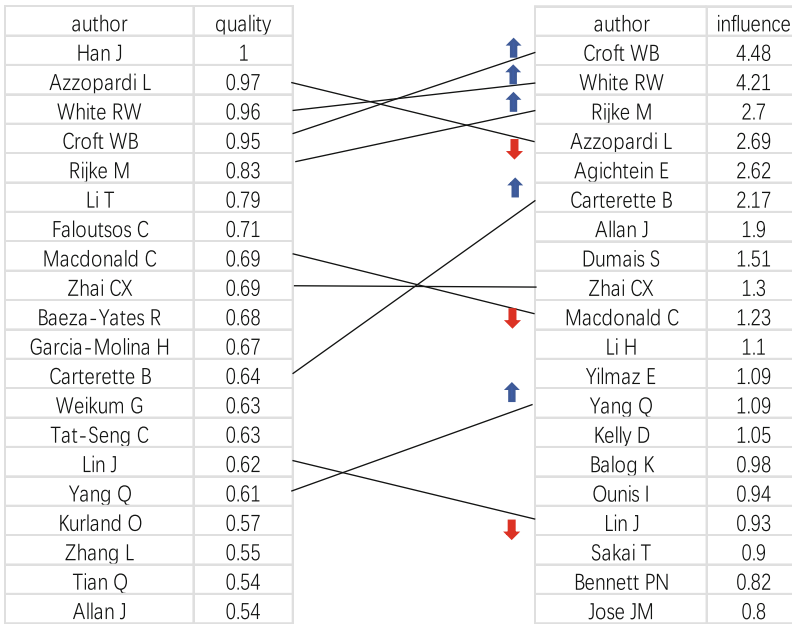


Fig. 3. Comparison of authors’ “quality” and influence

It can be seen that some authors are in the “quality” ranking top 20, while they are not necessarily in influence ranking top 20. Han J, for example, ranked first in authors’ “quality”, but his influence ranked 157th. It was found that Han J was cited by only 10 people and cited 10 times in the ACM SIGIR conference from 2006 to 2015. And Garcia-molina H dropped from 11th in the “quality” ranking to 312th in the influence ranking. We find that he is cited by only 4 people, with a total of 4 times. In addition, he only co-authored papers with 5 people during this period. That indicated they were weakly correlated with the surrounding authors during this period. So their academic

influence should be lower. However, Agichtein E and Dumais S rose from the 50th and 28th positions in the “quality” ranking to the 5th and 7th positions in the influence ranking respectively. By analyzing the times of citation, it can be found that Agichtein E is cited by 323 authors for 579 times, and Dumais S was cited by 265 authors for 426 times. In terms of the number of collaborators, they have co-authored papers with 35 and 31 people respectively during this period. It is obvious that they have closer connection with the surrounding authors. So they should have more influence.

From the analysis above, we can draw the following conclusions:

1. Authors’ “quality” and authors’ influence reflect different dimensions. The “quality” reflects the author’s own characteristics, such as the number of author’s papers and the order of signature. While the influence not only reflects the author’s “quantity”, but also reflects the reference degree from other authors who quoted him.
2. The higher the author’s “quality” is, the more articles are published by the author, and the higher the order of the author’s signature is. However, he doesn’t have to be cited more by other authors, so his influence doesn’t have to be greater.
3. Influence based on date field emphasizes the authors’ influence on other authors and reflects the real influence situation better.

5 Conclusions

This paper mainly studies the method of constructing author influence map and the mining of author reference relationship and cooperation relationship. For the measurement of author influence, we use the author data field method, which not only considers the author’s own characteristics related to influence, but also considers the superposition impact of the authors who quoted him. The effective evaluation of the authors’ “quality” is the premise to measure the author’s influence. We use entropy weight method to measure the “quality” of authors, which can effectively evaluate the different importance of each indicator in the comprehensive evaluation. In the aspect of cooperation relationship and weights between authors, we introduce the method of calculating authors’ contribution degree in different signature order to measure authors’ cooperation weights. Through experimental analysis, we explore the relevance between authors’ influence and authors’ “quality”, and realize the data field method reflects the authors’ influence more accurately. This will provide a reliable way to construct the author influence map.


This paper aims at the research of author influence and relationship map. In the future work, we will expand the research areas and paper databases. In addition, we will apply the author influence map to the personalized information service recommendation and build the personalized service recommendation system for academic authors.

References

1. Hirsch, J.E.: An index to quantify an individual's scientific research output. *Proc. Natl. Acad. Sci.* **102**(46), 16569–16572 (2005). <https://doi.org/10.1073/pnas.0507655102>
2. Braun, T., Nzel, W., Schubert, S.: A hirsch-type index for journals - the scientist - magazine of the life sciences. *Scientist* **19**(22), 8 (2005)
3. Mccarty, C., Jawitz, J.W., Hopkins, A., et al.: Predicting author H-index using characteristics of the co-author network. *Scientometrics* **96**(2), 467–483 (2013). <https://doi.org/10.1007/s11192-012-0933-04>
4. Kudelka, M., Plato, J., Kromer, P.: Author evaluation based on H-index and citation response. In: *International Conference on Intelligent Networking and Collaborative Systems (INCOS)*, pp. 375–379. IEEE Press, Ostravva, Czech Republic (2016). <https://doi.org/10.1109/incos.2016.100>
5. Chang, N., Huang, F., Zhang, Y., et al.: Author influence spreading prediction based on co-citation interest similarity. In: *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/UCC)*, pp. 459–463. IEEE Press, Guangzhou, China (2017). <https://doi.org/10.1109/ispa/iucc.2017.00075>
6. Daud, A., Aljohani, N.R., Abbasi, R.A., et al.: Finding rising stars in co-author networks via weighted mutual influence. In: *World Wide Web International World Wide Web conference Steering Committee*, pp. 33–41. Perth, Australia (2017). <https://doi.org/10.1145/3041021.3054137>
7. Liu, X., Zhang, J., Guo, C.: Full - text citation analysis: enhancing bibliometric and scientific publication ranking. In: *ACM International Conference on Information and Knowledge Management*, pp. 1975–1979. Maui, Hawaii (2012). <https://doi.org/10.1145/2396761.2398555>
8. Jeong, Y.K., Song, M., Ding, Y.: Content-based author co-citation analysis. *J. Inf.* **8**(1), 197–211 (2014). <https://doi.org/10.1016/j.joi.2013.12.001>
9. Nascimento, M.A., Sander, J., Pound, J.: Analysis of SIGMOD's co-authorship graph. *ACM SIGMOD Rec.* **32**(3), 8–10 (2003). <https://doi.org/10.1145/945721.945722>
10. Xu, X., Jia, W., Tang, M., et al.: Author cooperation relationship in digital publishing based on social network analysis. In: *12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, pp. 1631–1635. IEEE Press, Zhangjiajie, China (2015). <https://doi.org/10.1109/fskd.2015.7382189>
11. Hooydonk, G.V.: Fractional counting of multiauthored publications: consequences for the impact of the authors. *J. Am. Soc. Inf. Sci.* **48**(10), 944–945 (1997). [https://doi.org/10.1002/\(sici\)1097-4571\(199710\)48:103.0.co;2-1](https://doi.org/10.1002/(sici)1097-4571(199710)48:103.0.co;2-1)
12. Lijuan, Z., Jianrong, Y.: Research of weight measurement of co-author networks based on author contribution. *Libr. J.* **30**(5), 16–50 (2011)
13. Wenyan, G., Deyi, L., Jianmin, W.: An hierarchical clustering method based on data fields. *Acta Electronica Sin.* **34**(2), 258–262 (2006). [https://doi.org/10.1016/s1005-8885\(07\)60041-7](https://doi.org/10.1016/s1005-8885(07)60041-7)



Online Public Opinion Deduction Based on an Innovative Cellular Automata

Xin Liu^{1,2}(✉) , Shuai Cao^{1,2}, Yang Cao^{2,3}, Jie He^{2,4}, Weishan Zhang¹,
Xueli Wang¹, and Liang Zheng¹

¹ College of Computer Science and Technology, China University of Petroleum,
Qingdao 266580, China

lx@upc.edu.cn

² Application on Improving Government Governance Capabilities National
Engineering Laboratory, Guiyang 550022, China

³ CETC Big Data Research Institute Co., Ltd., Guiyang 550022, China

⁴ Information Science Academy of China Electronics Technology Group Corporation,
Beijing, China

Abstract. As the Internet entered the 2.0 era, online users have become the main part of public opinion, and significant events happened around the world quickly disseminate through the Internet. Some negative comments usually are mixed into posts and articles. If let public opinion develop at will, some serious social events may trigger very fierce online volatility and they will have adverse effects on social stability. Therefore, to simulate the propagation mode of topic events on the Internet, and to predict the trending of public opinion on the entire Internet, this paper constructs a new type of model based on the idea of cellular automata and applies it to the online public opinion situation deduction. We arrange the nodes in new ways. An individual user is represented by a cell node in our model, and we build the cellular space based on directed graph to represent social network topology that users follow about each other in an innovative way. We delineate the users' portrait based on the users' attributes, design evolutionary rules based on the behaviors of users on the Internet and the law of information dissemination. Experiments with real data of online users showed that the proposed model in this paper had excellent performance, it not only reflected the law of information dissemination on the Internet, but also its deduction result was similar to the trending of real historical events.

Keywords: Public opinion · Cellular automata · Graph calculation

1 Introduction

Public opinion is a collection of statements, attitudes, and beliefs expressed by a considerable number of people in society on a particular topic. It usually involves major social issues such as public safety, social peace, and social life. As an online platform for the public to accept information and express opinions, the Internet

gathers people's attitudes, opinions and emotions about social phenomenon and problems which show people's needs and wishes. With the rapid development of online new media and social network platforms, the convenience of posting comments on the Internet is constantly improving, and the situation of online public opinion play an increasingly important role on social stability. Predicting the trending of public opinion and finding key accounts on the Internet are important for governments, and governments could guide information dissemination on the basis of knowing what the consequences of relevant decisions may be. Our work also could make a certain purification of the network environment to reduce the negative impact of some information.

To simulate the rules and patterns of users' behavior and information dissemination on the Internet, this paper constructs online public opinion deduction model based on an innovative cellular automata. The model characterizes real user data, innovatively constructing a cellular space using a directed graph data structure and deducting the process of public opinion evolution by designing evolutionary rules. In the process of deduction, the public opinion situation at every moment is monitored and predicted.

2 Related Work

With the explosive growth of the influence of online public opinion, the online public opinion forecast has not only become the focus of journalism communication and political science in the social sciences, but also attracts the extensive attention of computer science, system science and psychology. As a cross-disciplinary complex issue, various public opinion analysis has been studied by many researchers based on their own theoretical basis and research methods [38].

At present, the main research directions in the field of public opinion analysis include hot topic data acquisition, hot topic detection and online public opinion situation forecast [33]. Hot topics refer to topics that most online users are concerned about in a certain period. Online hot topic detection generally follows three steps: data collection, data cleaning, natural language processing and topic identification [9, 14, 29]; The research content of the public opinion forecast is quite broad, including the prediction of hot event [10, 18, 25, 40, 41], the warning of serious events [7, 27, 31, 37, 42], and the prediction of public opinion trending [15, 21, 39]. In order to achieve different public opinion prediction purposes, scholars have adopted a variety of methods to practice, including public opinion forecast based on big data, public opinion forecast based on neural network and public opinion situation deduction based on the propagation model.

2.1 Public Opinion Forecast Based on Big Data

Public opinion forecast based on big data mainly relies on the analysis of a large amount of data, using statistical and probabilistic knowledge to explore the changing law of the public opinion situation. Shang et al. [24] used the Hadoop platform and their data mining algorithms' set called "Mahout" to make special

extractions of lyrical texts, to analyze what public opinion will happen next, and to provide better decision support for governments and enterprises. Fan et al. [6] proposed a hot public opinion detection model based on quantitative comment and emotion, in this model, web opinion mining was applied in presence of report vector, by constructing the web opinion dictionary, the inclination and intensity of web comment were quantitated by the form of vector. Lian et al. [16] built a multi-dimensional factor index system based on a large amount of public opinion data, multivariate logistic regression analysis was used to explore the relationship between the types of online public opinion events and the characteristics of public opinion, and then predict the public opinion characteristics of events in the public opinion latency of the same type of events; Maclellan et al. [19] predicted the attitude of New Zealanders towards alcohol policy through survey sampling; Krueger [13] used Gallup World Poll data to predict public attitudes toward terrorist attacks; Ceron et al. [1] obtained the emotional orientation data of netizens on Twitter in the 2012 French election, and used statistical analysis methods to predict the results of the election. Xia et al. [30] monitored the anomalous events by monitoring the abnormal data of the network in the big data environment.

The public opinion forecast based on big data extracts features from existing events by statistics and constructs feature models. These methods predict the possible trending of new events by comparing the features of new events with existing feature models. However, the models based on statistics simplifies the actual complexity of public opinion, they cannot fully describe, restore and explain the details of events [33]. Due to the law based on statistics from historical data, the prediction on the similar event is accurate, while the prediction on different kind of event may be Ineffective, which is the limitation of those methods.

2.2 Public Opinion Forecast Based on Neural Networks

Public opinion forecast based on neural networks uses the prediction ability of the neural network to predict hot event. Chen et al. [3] constructed a hybrid prediction model combining convolution neural network with corpora to predict the vegetable price fluctuation in China's market. Chachra et al. [2] used deep convolution neural networks (DCNN) to model sentences and perform sentiment analysis, then predict the possible changes in the public's emotions in public opinion. Sun et al. [26] designed an online public opinion model based on adaptive learning rate of recurrent neural network, it selects a variety of features based on the characteristics of comments to construct a cyclic neural network sequence generation model, the results of the public opinion forecast were evaluated based on the Baidu index; Huang et al. [10] used the strong global search ability of genetic algorithm and the local search ability of particle swarm optimization algorithm to optimize the weight of BP neural network, the online public opinion prediction model optimized by hybrid algorithm is constructed to accelerate the convergence speed of the neural network. Isa et al. [11] utilized the strengths of the self-organizing map (SOM) to overcome the inadvertent dimensionality

reduction resulting from using only the Bayes formula to classify, combining the hybrid system with ranking techniques further improves the performance of the proposed document classification approach; Chen et al. [12] used multi-output neural network to design a public opinion index fitting optimization model to predict unknown Microblog users' gender and the number of fans.

Microblog is the main experimental data source for scholars to study public opinion. However, comments in Microblog are randomized, fragmented, and language unstructured, the feature extracted from text is not accurate, which in turn affects the output of neural networks [34], due to the random nature of such features of the Internet, it is difficult to establish a model by neural networks with wide applicability. Furthermore, public opinion forecast based on neural networks uses historical data as a training set, so the prediction on new types of events is poor.

2.3 Public Opinion Situation Deduction Based on the Propagation Model

Public opinion situation deduction based on the propagation model uses the law of information dissemination, studying the propagation mode of information on the Internet, the information dissemination simulation and user behavior are used to deduct and predict the online public opinion situation. Liu et al. [17] constructed Internet opinion propagation model by improving the classical disease spreading Susceptible-Infective-Recovered (SIR) model, based on this model, the parameter inversion algorithm was used to predict the online public opinion's trending of actual cases. Ha et al. [8] refined the mode of transmission of infectious diseases and established a public opinion model for top-down research; You et al. [35] used the infectious disease model combined with the influence of Microblog users' forwarding behavior on the information dissemination mechanism, they constructed an evolution equation group with Microblog propagation characteristics to predict the spread of Microblog information. Yang et al. [23] according to the behavior characteristics of the user's social information, introduced the interest degree and intimacy into the process of public opinion propagation and proposed the IC-SEIR online public opinion propagation model, and predicted the user relationship on the Internet.

In 1966, John Von Neumann [22] proposed the Theory of Self-Reproducing Automata, inspired by the self-replication of cells, he built a simple machine with self-replicating features and general computer capabilities using mathematical abstract models. In 1968, Codd [4] used a two-dimensional cellular automaton to implement self-replicating features, simplifying Von Neumann's original extremely complex model. In the method of the propagation model, some scholars built a public opinion propagation model based on cellular automata. Wang et al. [28] abstracted the individual of a certain grid space into a cell with sentimental tendencies, set the degree of opinion preference and other attributes described as discrete values, and predicted the phenomenon of group opinion reversion on the Internet; Mao et al. [20] proposed a cellular automata model based on fuzzy inference theory for online public opinion aggregation, which

defined three kinds of public opinion attributes: attention degree, attitude community and environmental adaptation intensity, through the simulation experiment, the aggregation effect of online public opinion under two different fuzzy demarcations is obtained; Yu et al. [36] proposed a WeChat public opinion propagation mechanism model based on adaptive neuro-fuzzy inference system and cellular automata, and used simulation experiments to predict the changes of users' attitudes toward public opinion events during WeChat propagation. Deng et al. [5] based on the cellular automata model to quantitatively study the influencing factors of network information dissemination and explored the impact of these factors on public opinion communication and intervention mechanisms; Li et al. [32] established a cellular automata model based on decision theory, using the relative income model as the evolutionary rule, designing a traversal algorithm for the evolution of cell states at the same time, which can achieve the propensity of public opinion.

Public opinion situation deduction based on the propagation model starts from the characteristics of user nodes and information dissemination rules, constructing a lyric situation deduction model close to the real Internet operation law. However, the relevant research stays in the theoretical stage, and only simulation experiments are used to the operation model. There is also no clear calculation method for the determination of the node feature value. The model used for online public opinion prediction is relatively simple, and lack a more accurate and comprehensive prediction system [33].

To solve the above problems, this paper proposes online public opinion deduction model based on an innovative cellular automata. We calculate the values of several attributes of cell nodes based on users' historical comments, and construct the cellular space using the directed graph data structure and the specific evolutionary rules for the first time. The proposed model can forecast multiple indicators such as hot event, emotional tendency, and proportion of comment types.

In Sect. 3, the related knowledge of the standard cellular automata is introduced, then various attributes of the cell node, calculations for attributes, cellular space, neighbor set and specific evolutionary rules are defined; In Sect. 4, the reliability and authenticity of the proposed model are verified by experiments on real Microblog user data; In Sect. 5, we summarize our work in this paper and give some future work.

3 Online Public Opinion Deduction Based on the Thought of Cellular Automata

The standard cellular automata is a four-tuple composed of cell node, cellular space, neighbor set, and evolutionary rule. The mathematical expression is as follows:

$$A = \{C, L_a, N_n, f\} \quad (1)$$

where A denotes a standard cellular automata system; C denotes a set of cell nodes; L_a denotes a cellular space, a is the dimension of the cellular space; N_n

denotes a set of cell nodes' neighbors, and n is the number of cell nodes in a neighbor set; f represents the evolutionary rule of the cellular automata system.

Each cell node C contains a state set S , S contains a plurality of states. At each moment, the cell node is in a certain state in S , and the deduction process of the cellular automata is the transformation process of all cell nodes from one state to another. The nodes in the cellular space L_a are arranged in a variety of ways, such as one-dimensional, two-dimensional, and three-dimensional arrangements, and a represents the dimensions of the arrangement. Since it is impossible to construct a cellular space that is infinitely extended in multiple dimensions in a computer, it is necessary to define different boundary conditions of the cellular space, mainly three types: periodic type, reflective type and custom type. All cell nodes adjacent to a cell are considered as neighbors of the cell, neighbor nodes are included in the neighbor set N_n of the cell node, and n represents the number of neighbor nodes, taking two-dimensional cellular space as an example, the common neighbor set has 3 cases such as 4-node neighbor set, 8-node neighbor set, and 24-node neighbor set. Any other cell nodes in the range are regarded as neighbor nodes of this cell node, during the deduction of the cellular automata, the state of a node is affected by its neighbors.

The evolutionary rule f in the cellular automata is the core of the cellular automata deduction. The formula is defined as:

$$s_i^{t+1} = f(s_i^t, N^t) = f(s_i^t, s_1^t, s_2^t, \dots, s_n^t) \quad (2)$$

where $s_i^t, s_1^t, s_2^t, \dots, s_n^t$ represents the state of the cell node i and its n neighbor nodes in the neighbor set at time t . The state of each cell node at the next moment is determined by the state of the previous moment itself and all its neighbor nodes. The cell nodes in the cellular automata will change their state with discrete time according to the defined evolutionary rules, thereby realizing the deduction of the cellular automata.

The online public opinion deduction model based on an innovative cellular automata proposed in this paper uses cell node to simulate the user node on the Internet, constructing the neighbor set and cellular space of cell node based on the followers of each user node in the social network. Then we designed evolutionary rules based on the propagation of information on the Internet, the change of user's emotional value, the degree of user acceptance of information, etc. Therefore, in order to be close to the operation law of the real Internet, it is necessary to adjust the four basic attributes of the standard cellular automata.

3.1 Cell Node

In our model, the cell node is used to characterize the users on the Internet. To enable the cell nodes to reflect the situation of the entire Internet, we add a feature set $P = \{I, Iv, Sp, Mu, Il\}$ for each cell node. The set elements are users' node influence I , autonomic opinion index Iv , comment firmness index Sp , emotional tendency degree Mu , and interest list Il . The values of the set element in P are determined based on users' own historical comments, they will affect the user's reaction to different public information.

Node Influence: Node influence I reflects the importance of the user on the Internet, it is judged based on the user’s activity W_1 and the user’s comment degree of propagation W_2 , wherein W_1 is calculated based on the user’s total number of comments X_1 and the total number of original comments X_2 . X_1 indicates the number of comments published and forwarded by the user, X_2 represents the number of comments made by the user himself. The user’s comment degree of propagation W_2 is based on the number of comments being forwarded X_3 , number of comments being commented X_4 , the number of original comments being forwarded X_5 , number of original comments being commented X_6 and the number of comments being liked X_7 . Each part is given a different weight when calculating the node influence, as shown in Table 1:

Table 1. The weight of different parts of the node influence calculation

Variable	Weight	Variable	Weight
W_1	0.2	X_1	0.3
		X_2	0.7
W_2	0.8	X_3	0.2
		X_4	0.2
		X_5	0.25
		X_6	0.25
		X_7	0.1
Standardization: $X' = \ln(X+1)$			

Based on the weight ratio of each part in Table 1, the formula for calculating the node influence is shown in Eq. (3):

$$I = (0.2 \times W_1 + 0.8 \times W_2) \times 160 \tag{3}$$

The user’s activity W_1 calculation formula is as shown in Eq. (4), and user’s comment degree of propagation W_2 calculation formula is as shown in Eq. (5):

$$W_1 = 0.3 \times \ln(X_1 + 1) + 0.7 \times \ln(X_2 + 1) \tag{4}$$

$$W_2 = 0.2 \times \ln(X_3 + 1) + 0.2 \times \ln(X_4 + 1) + 0.25 \times \ln(X_5 + 1) + 0.25 \times \ln(X_6 + 1) + 0.1 \times \ln(X_7 + 1) \tag{5}$$

Autonomic Opinion Index: Some users are the main body of the public opinion. When significant event happens, these users will actively express their opinions to participate in public opinion events. User’s autonomic opinion index Iv is used to measure the probability that a user will actively express his or her own opinion when participation in an event. Autonomic opinion index is calculated as follows:

$$Iv = \frac{X_2}{X_1} \times 100 \tag{6}$$

Comment Firmness Index: Comment firmness index Sp reflects the extent to which users' own opinions are easily influenced by their neighbors. To calculate Sp , we designed the following process:

Process 1. Comment firmness index calculation

- (1) Get top 10 keywords of user's each comment, and obtain the keyword data set Dw , where each record contains the corresponding comments, the length of Dw is equal to the total number of comments of the user;
 - (2) Construct comments-keyword matrix $W = (a_{ij})$, it contains n m -dimensional vectors, where n is equal to the length of the keyword data set Dw , m is equal to the number of all non-repeating keywords appearing in Dw , each dimension corresponds to one keyword, and the value of a_{ij} takes 0 or 1, 0 means that the keyword corresponding to the dimension i in the j -th sentence does not appear, and 1 indicates that the corresponding keyword appears;
 - (3) Use the PCA dimensionality reduction algorithm to reduce the comments-keyword matrix W to the $n \times 2$ matrix $W_{PCA} = (b_{ij})$, the matrix contains n 2-dimensional vectors (b_{i1}, b_{i2}) , b_{i1} and b_{i2} are the m -dimensional vectors in W Results after dimensionality reduction;
 - (4) Set the scanning radius eps and the minimum inclusion point $minPts$, use the DBSCAN clustering algorithm to cluster two-dimensional vectors in the W_{PCA} to obtain the cluster number C_n ;
 - (5) Calculate user's comment firmness index based on formula: $Sp = \frac{1}{C_n} \times 100\%$
-

Interest List: Every user on the Internet has their own areas of interest, and users are more likely to accept comments in areas of their own interest. The interest list Il is a q -dimensional vector, each dimension of the vector corresponds to a domain, and each dimension has a value between 0 and 1, the larger the value, the more interested the user is. The interest list can be established by counting the number of occurrences of keywords in different fields in user's total comments. The more occurrences of keywords in a certain field, the more interesting the user is to the field. The value of the i -th dimension in the interest list is as follows:

$$Il_i = \frac{Kw_i}{Kw_{max}} \quad (7)$$

Kw_i indicates the number of occurrences of keywords in the i -th interest area in user's total comments, Kw_{max} indicates the maximum number of occurrences of keywords in each field in the q domain in the user's comments.

Emotional Tendency Degree: Emotion is divided into three categories: positive, neutral, and negative. User's emotional tendency degree μ indicates that the user is prone to emotional tendencies when touching a topic event, and what sentiment tends to be expressed when the comment is posted. To calculate user's emotional tendency degree, the following process is designed:

Process 2. Emotional tendency degree calculation

- (1) Collect positive words, negative words, negative words, and degree adverbs;
 - (2) Obtain all the comments published and forwarded by the user, and initialize the emotional value of each comments $M = 0$;
 - (3) For each of the user's comments, use the word segmentation to segment the words, remove the stop words, meaningless words and punctuation marks;
 - (4) Traversing the sequence of words obtained after each sentence is processed in step 3. If a keyword appears in the positive word lexicon, it is judged whether the previous word is a fixed word or a degree adverb. If it is a negative word, the value of M is decreased by 1. If it is a degree adverb, add the value of M to 2. If it is not a negative word or a degree adverb, then the value of M is increased by 1. If a keyword appears in the negative word lexicon, the previous word is judged. Whether the word is a degree adverb, if it is a negative word, the value of M is increased by 1. If it is a degree adverb, the value of M is decremented by 2. If it is not a negative word or a degree adverb, the value of M is decremented by 1;
 - (5) Calculate the emotional value of each comments of the user based on step 4, user's emotional tendency degree $Mu = \frac{1}{n} \sum_{i=1}^n M_i$, where n is the total number of comments for the user and M_i is the emotional value of the user's i -th comment.
-

3.2 Neighbor Set and Cellular Space

Users on the Internet have a list of users who are followed by themselves, and each user will also be followed by other users from their fan lists. In the neighbor set N_n of the standard cellular automata, n cannot obtain a fixed value to represent the number of neighbors of each user on the Internet. Moreover, the cellular space L_a of the standard cellular automata is also difficult to show the intricate follow relationship on the Internet.

In our model, the directed graph data structure is used to represent the following relationship between users on the Internet. Cellular space $L = (V, E)$, where $V = \{C_0, C_1, \dots, C_n\}$ is a collection of cell nodes in the cellular space, n is the total number of cell nodes in the cellular space, $E = \{(C_i, C_j) | (0 < j, j \leq n \text{ and } i \neq j)\}$ is a set of directed edges between different cell nodes in the cellular space, the direction C_i points to C_j , indicating that the user C_i is followed by the user C_j . E can be established by the following relationship between users on the real Internet, and the nodes connected to all the ingress sides of the node constitute the set of neighbor nodes of the node. The size of this type of cellular space is determined by the number of cell nodes and directed edges, so there is no need to design a boundary mode of cellular space.

3.3 Evolutionary Rule

To simulate the law of users' behavior on the real Internet, the evolutionary rules are formulated in four aspects: participation state, emotional change, comments publication and forwarding, loss of interest.

Participation Topic State: Entering the participation state indicates that the user is in contact with a topic event and generates interest, which in turn will be noted, forwarded, and published. There are three actions after the user participates the participation state: onlookers, forwarding comments, publishing comments. Onlookers indicates that the user will pay attention to and read the relevant comments on the topic event, but does not carry out any information dissemination; Forwarding comments indicates that the user will forward the relevant comments of his neighbor node, and the forwarded comments will be browsed by the user's fans; Publishing comments indicate that the user will publish relevant statements on his own, and the published comments can be transmitted through the neighbor nodes of the user. Based on the above rules, we defined evolutionary rule 1 for cell nodes entering the state of participation topics.

Evolutionary rule 1. Participation topic state

- (1) Let the topic vector of the topic event be T , T is a q -dimensional vector, each dimension corresponds to an area of interest, and the value is 0 or 1, 0 means that the topic event does not involve the interest area corresponding to the dimension, and 1 indicates the topic relates to the area of interest of the dimension, wherein each dimension of T is the same as the area of interest corresponding to each dimension in user's interest list Il ;
 - (2) If a user in user C 's neighbor set forwards and publishes a comment about the topic event, then subtract topic vector T and user's interest list Il , if the value of a certain dimension in the subtracted result vector is smaller than the interest difference threshold $I.t$, the user C will enter the participation topic state at the next moment;
 - (3) If more than 70% users of user C 's neighbor set forward and publish the related comments of the topic event, user C will enter the participation state at the next moment;
 - (4) If a user of user C 's neighbor set has more than two higher levels of node influence than C , the number of this kind of users that forward and publish related statements reaches 20% of the total number of neighbor nodes, then user C will enter the participation state at the next moment;
-

Emotional Change: When users participate in online public opinion events, they will have certain opinions on the events based on their own emotional tendency. Because of the exchange of information, user's emotional tendency will also be affected by the opinions of other comments. Based on the above rules, the evolutionary rules of emotional changes of users' participation in online public opinion events are designed in evolutionary rule 2.

Evolutionary rule 2. Emotional change

- 1) If a user C will post a comment at the next moment, the comment will carry an emotional value, which is the same as the emotional tendency degree Mu_{t+1} of the user C at the next moment $t + 1$, the emotional value carried by the user-forwarded comments will not change during the forwarding process;
- 2) The emotional tendency degree Mu_{t+1} of user C at the next moment does not change under a certain probability, and the probability is equal to the comment firmness index Sp of user C . If the probability condition is not satisfied, the calculation formula of the emotional tendency degree Mu_{t+1} of user C at the next moment is as follows:

$$Mu_{t+1}^C = Mu_t^C + \alpha \frac{1}{m} \sum_{i=1}^m (Mu_t^i - Mu_t^C) \tag{8}$$

Mu_t^C represents the emotional tendency degree of user C at current moment t , m is the number of users in user C 's neighbor set that have been forwarded or published comments and whose node influence is greater than C , Mu_t^i indicates emotional value of i -th user in C 's neighbor set have been forwarded or published comments, α is the influence weight of the neighbor, it is used to adjust the influence degree of the neighbor node on the user.

Loss of Interest: Users will not always participate in the online public opinion event. After reaching certain conditions, users will lose interest in topic event, and then withdraw from the participation state, and no longer publish and forward relevant comments. Therefore, we designed evolutionary rule 3 for users about when will they loss interest to an event.

Evolutionary rule 3. Loss of interest

- (1) Set a unified interest demise time limit $Id.t$. After the user enters the participation state, the iteration will exceed the $Id.t$ time and the participant will be permanently logged out of the participation state;
 - (2) If the number of users in user C 's neighbor set who forwards and publishes the relevant comments is less than 20% of all the neighbors, user C temporarily withdraws from the participation state at the next moment;
 - (3) If the situation in step 2 is continuously iterated β times in the neighbor node of user C , the user C will permanently exit the participation state at the next moment.
-

User exits events are divided into two situations: temporary and exit permanent exit. After temporarily exiting the topic participation state, the user can still re-enter the participation state according to the conditions in the evolutionary rule 1. For permanent exit, users will permanently withdraw from the participation and not enter the participation state during the deduction.

Comments Publication and Forwarding: When users participate in topic events, they will have a certain probability to actively express their opinions or

forward the comments of neighbor users, and users tend to forward comments that are similar to their own opinions. To simulate the user's actions and comments, the following evolutionary rules are designed in evolutionary rule 4.

Evolutionary rule 4. Comments publication and forwarding

- (1) The user can perform both the comments publication and comments forwarding at the same time;
 - (2) If user C is in the participation state, it has a certain probability that the relevant comments will be published at the next moment, and the probability value is equal to user's autonomic opinion index Iv ;
 - (3) If user C is in the participation state, and the user whose node influence is greater than user C in its neighbor set forwards and publishes relevant comments at the current moment, the absolute value of the difference between emotional value of user C 's neighbors comments and emotional tendency degree Mu of the user C is less than a certain emotional difference threshold $Mu.t$, then user C has a certain probability that the relevant comments will be forwarded at the next moment, and the probability value is $(1 - Iv)$;
 - (4) If user C is in the participation state, and in step 2 and step 3, the user fails to reach the requirement of speaking and commenting, the user will continue to maintain the participation state at the next moment when the condition of the demise of interest is not reached.
-

4 Experiments

To verify the practicability of the online public opinion deduction model based on an innovative cellular automata, the cell nodes are constructed by real user information obtained from the Microblog network, and the cellular space is constructed according to the follow relationship between users. Experiments were carried out based on the cell node attributes, states, cellular space and evolutionary rules proposed in this paper.

4.1 Data Collecting

We used web spider to get users' information centered on the account called "People.cn" randomly from the Microblog as experiment data. User information includes user name, user location, gender, fan volume, number of users followed, following list, total number of comments, account creation time, and personal description. At the same time, obtaining all the Microblog comments of each user, the Microblog comments includes the comments text, post time, the number of comments being commented, the number of comments forwarded, the number of comments liked, the title of the comments topic, the author of the comments published, and the original tag.

We collected a total of 1442 user nodes and 2,568,023 comments, and 14,676 follow relationships between users. To protect the privacy of users, the personal username information involved in this article are desensitized.

4.2 User Portrait

Based on the personal information of all users and all comments, combined with the calculation algorithm described in Sect. 3.1, each user’s node influence, autonomic opinion index, comment firmness index, emotional tendency degree, and interest list are calculated.

In step 1 for calculating the comment firmness index, we set the scanning radius $eps = 0.5$ in the step 4, and the minimum inclusion point $minPts = 10$.

When calculating the user’s interest list, the keywords of eight interest areas which are college, military, finance, international, audio, sports, society and games are collected based on the Sogou vocabulary. Therefore, when the q -dimensional vector is used to represent the interest list, where $q = 8$.

In step 2 for calculating the user’s emotional tendency degree, the positive words, negative words, and degree adverbs used are combined with Tsinghua University Li Junzhong Wen Yiyi Dictionary, Taiwan University NTUSD Simplified Chinese Emotion Dictionary, and CNKI Hownet Emotion Dictionary.

Based on the value of the above parameters, in the 1442 user nodes used in the experiment, the node with the most influence is “-Qianshan***”, and its node influence is 2472.26. The node influence is discretely divided into 4 levels based on the maximum value of node influence in the cellular space, the correspondence between the node influence level and node influence is shown in Table 2:

Table 2. Discrete node influence level

Node influence level	Node influence I
Level 1	$I \leq 619$
Level 2	$619 < I \leq 1238$
Level 3	$1238 < I \leq 1857$
Level 4	$1857 < I$

The node influence level is marked to each node which can be used for the evolutionary rule 1. The calculated values of the user images of the “People.cn” users obtained by calculation are shown in Fig. 1:



Fig. 1. User portrait of “People.cn”

4.3 Network Topology

Based on user's follow list, the topology based on the directed graph is constructed as the cellular space. Each node in the cellular space represents a Microblog user, and the edge in the cellular space represents the following relationship between the Microblog users. A user node will receive information from the user he followed. The cellular space constructed in this experiment is shown in Fig. 2.



Fig. 2. Cellular space

The size of nodes in Fig. 2 represents different node influence levels of the underlying cell node, and the larger the node, the greater the influence of node.

4.4 Experimental Process and Results Analysis

The experimental process first sets the topic information of the online event that will be propagated in the cellular space. The comment information includes the topic vector T , the initial comment tendency, and selects the initial cell node for the dissemination of comments with different node influence level randomly. In the process of evolution, let the interest difference threshold $I.t = 0.1$ in step 2 of the evolutionary rule 1; in the evolutionary rule 2 step 2, the neighbor influence weight $\alpha = 1$; in the first step of the evolutionary rule 3, the interest demise time limit of the cell node $Id.t = 30$, and $\beta = 3$ in the evolutionary rule 3 step 3; in the step 3 of the evolutionary rule 4, the emotion difference threshold $Mu.t =$

3. Several comparative experiments were carried out to observe and record the changes in the situation such as event heat, emotional tendency and comments during the deduction.

Different Initial Comment Topics: To observe the spread rate of different topics on the Internet, we set different initial public opinion topics. Firstly, the initial cell nodes are selected to spread the comments, and 30 four-level node influence nodes including “People’s Daily” and “CCTV News” were selected as the initial propagation cell nodes. Two topic vectors T_1 and T_2 were constructed, where T_1 indicates that the initial topic event involves the “military” field, and T_2 indicates that the initial topic event involves the “game” field. The propagation of two kinds of initial comment information in the cellular space is shown in Fig. 3.

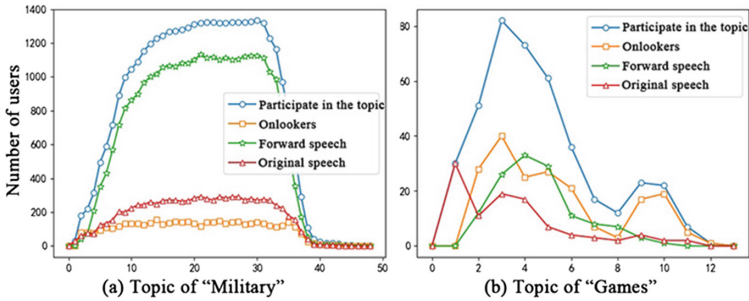


Fig. 3. The spread of different initial comment information in the cellular space

The number of users who participate in the “military” event shown in Fig. 3(a), in the first 20 iterations of the model, a large number of cell nodes in the cellular space quickly entered participation state. In the 30-step iteration, the number of participants in the event was the most. In the 40th iteration, the event heat decreased, and the nodes in the cellular space successively exited the participation state. The number of users who participate in the “game” event shown in Fig. 3(b). Since the user information collected in this experiment was centered on the account called “People.cn”, users were less interested in the game field. Figure 3(b) showed the maximum number of participants in the iteration of step 3 with only 83 people, the event heat disappeared after the iteration of step 12, the number of onlookers in the whole event was relatively large, and there were few related comments. By comparison, it can be found that the content of comments in different areas of interest was significantly different in the user group involved in the experiment. For topic events of interest to the user, most users mainly participate in the topic due to hobbies, and the remaining users were affected by their neighbors who were involved in the topic, while topics that are not of interest to the user group were difficult to be propagated, and the event heat was falling fast.

Different Initial Propagation Nodes: To verify the influence of cell nodes with different influences on information dissemination efficiency, this group of experiments set up different initial propagation nodes for 4 groups of experiments. Based on 4 levels of node influence, each group of experiments selects some nodes as the initial propagation node to propagate information. The initial comment involve the field of “finance”. The trend of user participation in each group of experiments was shown in Fig. 4.

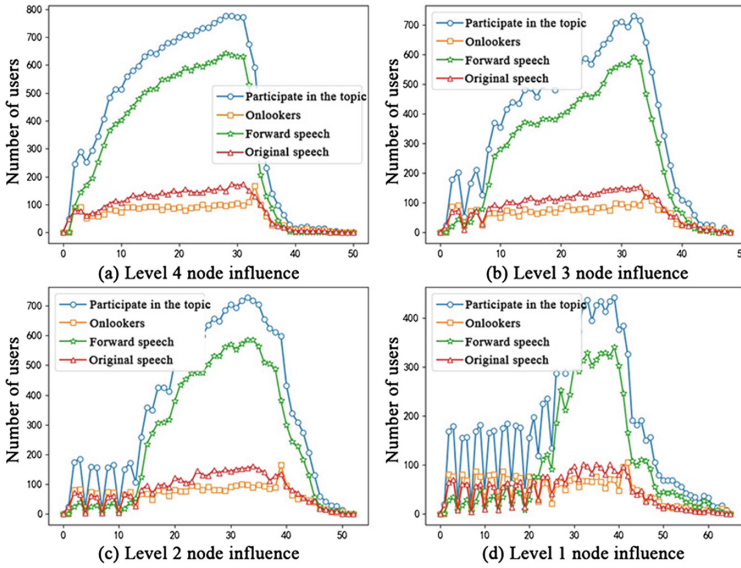


Fig. 4. The influence of different node influence on information dissemination

In Fig. 4(a), 25 nodes with level 4 node influence, including “People’s Daily” and “CCTV News” were selected as the initial comment propagation nodes. During the first 20 iterations, the number of people entering the participation state increased rapidly, and the number of people participation in the topic reached the maximum of 773 during the iteration of step 30; In Fig. 4(b), 25 nodes with level 3 node influence were selected as the initial comment propagation nodes, the number of people entering the participation state after the iteration of step 10 began to increase rapidly, and the number of people participation in the topic reached the maximum of 735 during the iteration of step 35; In Fig. 4(c), 25 nodes with level 2 node influence were selected as the initial comment propagation node, during the first 20 steps of the iteration, the propagation rate of the topic event is slow. In the 20th step iteration, since a small number of cell nodes with level 4 node influence enter the participation state, the propagation rate of the topic event has a certain increase; In Fig. 4(d), 25 nodes with level 1 node influence were selected as the initial comment propagation nodes, during the first 25 steps of the iteration, the propagation rate of the topic event was

relatively slow, before the topic event heat disappeared, only 446 users in the cellular space had entered the topic of participation, and in the early stage of the topic event.

Through the comparison experiments of this group, it can be found that the users with greater node influence were conducive to the dissemination of information. If users with low node influence were selected as the initial propagation node, the slower the propagation rate in the early stage of propagation. However, in the process of communication, if a node with a large node influence participates in the topic event, it will help the information dissemination.

Analysis of Public Opinion Trending Prediction Results: To further verify the reliability of the derivation model, this group of experiments will be deduced. The results were compared with the trend of the number of participants in the historical real events. The selected event was “The US White House officially signed a trade memorandum to China on March 22, 2018”. The incident was initially reported by multiple Microblog accounts such as “Financial Circle” and “Sina.com” and caused a sensation in the Microblog.

In this set of experiments, setting the initial topic vector T involves the fields of “international” and “finance”. According to the Microblog comments, there were 53 initial propagation nodes including “Financial Circle” and “Sina.com” reported the news on March 22, 2018. During the deduction, the number of people who published and forwarded to each iteration was recorded as the result of the deduction. For comments we got, the number of users who published and forwarded relevant comments from 0:00 to 12:00 and 12:00 to 24:00 during the period from March 22, 2018 to April 10, 2018 was counted as the actual trend of participants. The result obtained by comparing this trend with the deduced result was shown in Fig. 5.

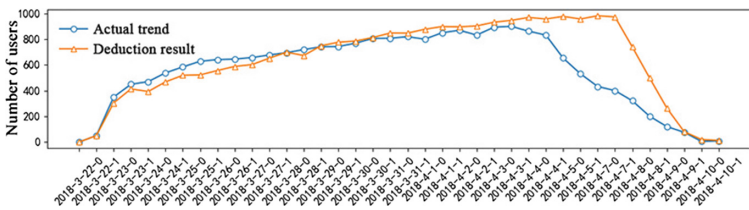


Fig. 5. Comparison of actual results and deduction result

In Fig. 5, the abscissa was a time series, the suffix was “0” for the period from 0 to 12 o’clock, and the suffix was “1” for the period from 12 o’clock to 24 o’clock. By comparison, it can be found that in the early stage of the event, the proposed model in this paper can accurately reproduce the propagation rate of historical events in the user group involved in the experiment. In the stage of event extinction phase, the time of extinction caused by the deduction model

was slightly delayed, but it was basically consistent with the actual situation at the time when the event completely disappears.

5 Conclusion and Future Work

In this paper, we constructed an online public opinion deduction model based on cellular automata. Our model used cell nodes to represent individual users on the Internet, we designed five attributes that can affect users' behavior in significant events, and we used users' historical comments to calculate these attribute values to delineate users' portrait. And a topology structure was constructed based on the users' following relationship in the social network, and the topology structure was used to represent the cellular space in the model for the first time. More importantly, a set of evolutionary rules that can simulate users' behavior and information dissemination law of the real Internet was designed. The experiment results showed that the deduction model proposed in this paper can observe the characteristics of multiple public opinion events in the cellular space, and the evolution process is similar to the user activity on the Internet.

The online public opinion deduction model based on an innovative cellular automata proposed in this paper was highly flexible. Cellular space based on the directed graph structure can be applied to any social network structure, and there are many parameters and thresholds can be set freely to adapt to specified Internet user group in the cell node feature calculation process and evolutionary rules proposed in this paper.

Due to the randomness of human behavior, the deduction model proposed in this paper is difficult to predict random events and turning points of some events. In the future we will optimize the performance of our model on time complexity and space complexity.

Acknowledgement. This work is supported by the Key Research Program of Shandong Province (No. 2017GGX10140), National Natural Science Foundation of China (No. 61309024), the Fundamental Research Funds for the Central Universities (2015020031).

References

1. Andrea, C., Luigi, C.: Every tweet counts? How sentiment analysis of social media can improve our knowledge of citizens' political preferences with an application to Italy and France. *New Med. Soc.* **16**(2), 340–358 (2012)
2. Chachra, A., Mehndiratta, P., Gupta, M.: Sentiment analysis of text using deep convolution neural networks. In: Tenth International Conference on Contemporary Computing (2017)
3. Chen, J., et al.: Research on agricultural monitoring system based on convolutional neural network. *Future Gener. Comput. Syst.* **88**, 271–278 (2018)
4. Codd, E.F., Ashenurst, R.L.: Cellular automata (1968)
5. Deng, Q., Yi, L., Ma, Y., Hui, Z.: Information propagation and intervention on online social networks using cellular automata. *Manag. Rev.* **28**(8), 106–114 (2016)

6. Fan, C., Wu, Y., Zhang, J., Zhao, T.: Research of public opinion hotspot detection model based on web big data. In: IEEE International Conference on Network Infrastructure & Digital Content (2017)
7. Forkan, A.R.M., Khalil, I., Atiquzzaman, M.: ViDiBiD: a learning model for early discovery and real-time prediction of severe clinical events using vital signs as big data. *Comput. Netw.* **113**, 244–257 (2017)
8. Ha, D., Wu, Q.: Prediction for public opinion transmission based on epidemic model. *J. Command Control* **3**(1), 57–60 (2017)
9. Hatton, T.: Public opinion on immigration in Europe: preference versus salience. Social Science Electronic Publishing (2017)
10. Huang, Y., Chen, F., You, D.: Research on the prediction of network public opinion based on hybrid algorithm. *Inf. Sci.* **V36**(2), 24–29 (2018)
11. Isa, D., Kallimani, V.P., Lee, L.H.: Using the self organizing map for clustering of text documents. *Expert Syst. Appl.* **36**(5), 9584–9591 (2009)
12. Chen, J., Wand, G., Xu, Y., Wang, H.: Study of the fitting and optimization for public opinion analysis indicator based on the multi-output neural network. *Chin. High Technol. Lett.* **29**(1), 19–26 (2019)
13. Krueger, A.B., Jitka, M.: Attitudes and action: public opinion and the occurrence of international terrorism. *Science* **325**(5947), 1534–1536 (2009)
14. Lergetporer, P., Werner, K., Wößmann, L.: Public opinion on education policy in Germany. Social Science Electronic Publishing (2017)
15. Li, C., Kai, L., Wang, S., Management, S.O.: Propagation law and control decision of false public opinion in the government intervention based on multi-agent. *J. Mod. Inf.* **38**(323), 55–61 (2018)
16. Lian, Z., Lan, Y., Xia, Y.: Research on multi-dimensional dynamical classification and prediction model of network public opinion with big data. *Int. J. Drug Policy* **37**(5), 127–137+144 (2018)
17. Liu, Q., Jin, L.I., Xiao, R., Automation, S.O.: Trend prediction of public opinion propagation based on parameter inversion—an empirical study on Sina micro-blog. *J. Comput. Appl.* **5**, 36 (2017)
18. Ma, K., Yu, Z., Ke, J., Bo, Y.: Stream-based live public opinion monitoring approach with adaptive probabilistic topic model. *Soft Comput.* **3**, 1–20 (2018)
19. MacLennan, B., Kypri, K., Langley, J., Room, R.: Public sentiment towards alcohol and local government alcohol policies in New Zealand. *Int. J. Drug Policy* **23**(1), 45–53 (2012)
20. Mao, Q., Wang, C., Jin, H., Li, Y.: Research on internet public opinion cluster model of cellular automata based on fuzzy inference. *J. Chin. Comput. Syst.* **38**(7), 1479–1484 (2017)
21. Qiu, X., Xiaohu, T., Liao, W.: Seir microblog public opinion communication model with positive and negative feedbacks. *Comput. Modernization* **2018**(2), 48–52 (2018)
22. Rappoport, A.: *Theory of Self-Reproducing Automata* (1966)
23. Rui-Qi, Y., Yue-Xia, Z.: Research on IC-SEIR public opinion propagation model based on complex network. *Meas. Control Technol.* **37**(11), 78–83 (2018)
24. Shang, S., Shi, M., Shang, W., Hong, Z.: Research on public opinion based on big data. In: IEEE/ACIS International Conference on Computer & Information Science (2015)
25. Shi, R., Chen, F., Zhang, J.: Prediction of online public opinion based on combination grey model. *J. Intell.* **V37**(7), 105–110 (2018)

26. Sun, J.C., Zhou, R., Pei-Yue, L.I., Tian-Liang, L.U.: Research on the prediction of network public opinion based on recurrent neural network. *Inf. Sci.* **36**(8), 118–122, 127 (2018)
27. Tian, Y., Yuan, W., Shao, L.: Online public opinion risk warning based on Bayesian network modeling. *Lib. Inf. Serv.* **26**(2), 9.1–9.4 (2012)
28. Wang, C., Mao, Q., Xiang, T., Deng, C.: Mobile cellular automata of individualized network public opinion clustering model and simulation. *Comput. Eng. Appl.* **52**(19), 122–127 (2016)
29. Xiao, B.: Hot topic real-time detection technology study and application. Dissertation, Beijing Univ. Post Telecommun. (2014)
30. Yixue, X., Ye, Y., Wencai, Z., Yuexin, L.: The research on abnormal data monitoring and application of network public opinion facing big data. *J. Mod. Inf.* **38**(324), 82–87 (2018)
31. Yong-Yang, Y.U., Zhang, M.Z., Liu, C.Y., Bao-Hua, S.I.: A study on public opinion evolutionary model based on agent. *Comput. Simul.* **25**(9), 9–12 (2008)
32. Li, Y.-Y.: Research on network public opinion spread based on decision theory cellular automata. *Microelectron. Comput.* **33**(6), 29 (2016)
33. You, D., Chen, F.: The literature review about the prediction of network public opinion in China. *Inf. Sci.* **12**, 158–162 (2016)
34. You, D., Chen, F.: The literature review about the hotspot topic detection of network public opinion in China. *J. Mod. Inf.* **3**, 167–173 (2017)
35. You, X., Liu, Q.: Research on microblogging information dissemination prediction based on infectious disease model. *Comput. Appl. Softw.* **33**(5), 53–56 (2016)
36. Yu, W., Li, J.: Study on Wechat public opinion transmission mechanism basing on adaptive neuro fuzzy inference system and cellular automata. *Inf. Res.* **4**, 7–10 (2016)
37. Yu, Y., Zhang, M., Liu, C., Luo, P., Cao, Y.: Factors analysis and modeling research of public opinion evolutionary model based on crisis events. In: National Simulator Academic Conference (2007)
38. Zeng, Z., Li, R.: A survey of research on dissemination model of network public opinion. *J. CAEIT* **2016**(6), 24–29, 38 (2016)
39. Zeng, Z., Huang, C.: Research on public opinion heat trend prediction model of emergent infectious diseases based on BP neural network. *J. Mod. Inf.* **38**(323), 39–46+54 (2018)
40. Zhang, H.P., Chen, Q.H.: Research on the prediction of network public opinion based on grey Markov model. *Inf. Sci.* **36**(2), 75–79 (2018)
41. Zhang, L., Chang, S., Jin, Y., Goh, M., Wu, Z.: Cross-network dissemination model of public opinion in coupled networks. *Inf. Sci.* **451–452**, 240–252 (2018)
42. Zhe, F., Hao, Z., Qiang, C., Liu, S.: Application of naive Bayes classifier in stampede risk early-warning of large-scale activities. In: International Conference on Industrial Informatics-computing Technology (2017)



Discretionary Access Control Method to Protect Blockchain Privacy

Jie Yang, Min-Sheng Tan^(✉), and Lin Ding

School of Computer, University of South China, Hengyang 421001, China
tanminsheng65@163.com

Abstract. Blockchain technology has been widely concerned by scholars and industry since it was put forward, and Banks, Internet of Things, Supply Chain, Government and Medical Industry have proposed using blockchain technology to solve their problems, respectively. However, there are some difficulties in the deployment of blockchain products. One important reason is privacy protection. In order to protect blockchain privacy, discretionary access control method is proposed, and the corresponding model and algorithm are given. Encryption algorithm is used to encrypt the blockchain transaction transactions to privacy transactions. The encryption key and access rights are encapsulated by Lagrange polynomial to form secret information sent to authorized users. Extracting enough secret information, authorized user groups work together to calculate the decryption key, and then obtain the transaction transactions plaintext and finally implement consensus mechanism to verify the transaction. Secret information safely self-destruct immediately if exceed effective time. Authorized users and effective time are entirely determined by the owner of the transaction. This paper realizes key distributed securely, achieves discretionary access control and fine-grained access control and provides strong privacy protection.

Keywords: Privacy · Blockchain · Discretionary access control

1 Introduction

Bitcoin has attracted the attention of many scholars since it was put forward. Blockchain technology is the underlying technology of encrypting encrypted digital currency. It is composed of distributed database system (also known as distributed ledger), peer-to-peer network (P2P) and applications. It has been applied to banking, Internet of Things (IoT), key supply chain, government, medical and other industries. The ledger is completely open, and users' privacy is protected only through virtual name, which hides identity information to some extent.

Privacy in blockchain [1–3] mainly considers transaction privacy and identity privacy. Transaction privacy mainly refers to the content of transaction transactions including transaction amount or transaction mode only accessed by designated users [3]. Identity privacy mainly refers to the inability to track the relationship between participants and infer the relationship between participants' real identity and transactions.

With the increasing of blockchain technology application, the privacy problems revealed behind it become more and more serious. Scholars have found that trading chart analysis [2, 5], network graph analysis [4, 5], trading fingerprint identification [6], DoS attack [7], address clustering [5, 8], Sybil attack [9] and other methods can achieve the de-anonymity of Bitcoin.

In order to protect users' privacy, mixing services divided into centralized mixing services and decentralized mixing services, ring signature and non-interactive zero-knowledge proof were proposed.

The structure of centralized mixing services [3, 10] is shown in Fig. 1.

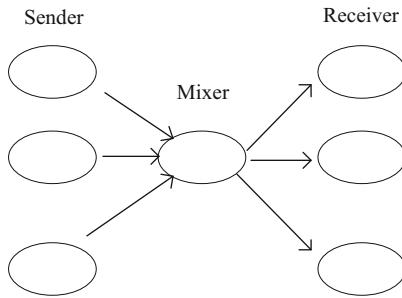


Fig. 1. Architecture of centralized mixing services

The sender encrypts the message(M) with receiver's public key(K_{PR}), encrypts the ciphertext and the receiver's address(R) with the mixer's public key(K_{MR}), then sends it to the mixer. The mixer sends the message decrypted with his private key(K_{MS}) to the receiver. At last the receiver decrypts the ciphertext with his private key(K_{RS}) to get the M. The whole process is expressed as follows:

$$E_{K_{MP}}(E_{K_{RP}}(M), R) \rightarrow D_{K_{MS}}(E_{K_{MP}}(E_{K_{RP}}(M), R)) \rightarrow D_{K_{RS}}(E_{K_{RP}}(M))$$

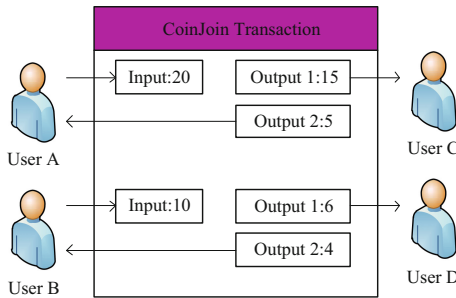


Fig. 2. Decentralized mixing services [3]

Centralized mixing services protect identity privacy, but needed to wait for enough participants to online perform interactive mixing services, so the delay is quite high and the sender needs to pay an expensive cost. Its privacy security depends on the loyalty of the mixer. Decentralized mixing services (as shown in Fig. 2 [3]) is divided into Coinjoin [11] and Secure Multi-Party Computation (MPC) [12], removing third-party mixer, but there is still high latency, don't protect transaction privacy and don't provide fine-grained access control.

Monero [13] represented using ring signature technology uses digital signature technology rather than any central manager, and protect transaction privacy and identity privacy at the same time. However, Feng Q [3] point out that it requires thousands of bytes of space to storage transaction transactions and there only limited external output in actual transactions, as the size of signatures is proportional to the number of participants.

Zerocoin [14] uses non-interactive zero-Knowledge proof to hide the relationship between payment source and transaction to protect users' privacy. Zerocash [15] improves Zerocoin [14], providing both identity privacy and transaction privacy. It achieves strong anonymity and provides the highest level of privacy protection so far, but at the expense of the high computational cost to generate transaction proof.

In order to solve the privacy problem of blockchain, this paper combining encryption algorithm, and authorization strategy proposes security discretionary access control method (SDAC) and implements the corresponding algorithms, which simply and efficiently achieve transaction encryption, fine-grained autonomous access control and access time control, thus realizing strong privacy protection of blockchain. The contributions of this paper are as follows:

- An effective authorization method is designed to realize blockchain discretionary access control.
- The number of elements in the authorized users' set can be controlled by trader to realize fine-grained access control.
- For the first time, the simple and efficient algorithms are used to encrypt blockchain transaction transactions while protecting both transaction privacy and identity privacy.

2 Basic Knowledge for SDAC

2.1 Threshold Secret Sharing

Secret sharing is an important issue in the field of information security, and an important method for key management. Shamir [16] first proposes threshold secret sharing method (t, n) ($0 < t \leq n$). Secret S is divided into n parts, which are shared by n participants. Each participant keeps one part. Only when more than t participants cooperate with each other, the secret S can be recovered. When less than, it cannot.

2.2 Lagrange Polynomial

A polynomial in the form:

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 \quad (1)$$

is called Lagrange polynomial. N different points can reconstruct an $n - 1$ Lagrange polynomial:

$$F(x) = \sum_{k=0}^{n-1} l_k(x)y_k \quad (2)$$

where,

$$l_k(x) = \prod_{0 \leq j \leq n-1, j \neq k} \frac{x - x_j}{x_k - x_j} \quad (3)$$

3 SDAC Core Goals and Related Assumptions

In this section, the basic definitions, core goals and assumptions of SDAC are given in turn.

3.1 SDAC Basic Definition

- (1) Definition 1. Privacy Transactions: It denotes an encrypted data structure consisting of input and output. Detailed data structure is given in Sect. 5.1.
- (2) Definition 2. Blockchain Self-Destroy Object (C_{sdo}): It denotes an encrypted string used to encapsulate secret information and reconstruct the decryption key, and may be leaked during the transmission in P2P network.
- (3) Definition 3. Validity Period: It denotes a lifetime and authorized users can access data objects, during it, but beyond the critical point, immediately cannot. SDAC method protects blockchain privacy security during and after the lifetime of self-destructive objects.

3.2 SDAC Core Goals

- (1) Discretionary Access Control. It refers to that the owner of transaction transactions decides to authorize users who can scan it without relying on any other entity or user, but unauthorized users cannot.
- (2) Fine-grained Access Control. A transaction can be visited by a user set, and different transaction transactions can be visited by different user sets. The number of elements in the authorized user sets can go from zero to any value.

- (3) Strong privacy protection. Protect both transaction privacy and identity privacy at the same time.
- (4) Low Computability and Efficiency. Transaction generated is more efficient than Monero. Computational cost of SDAC method is lower than Zerocash.

3.3 SDAC Assumptions

- (1) Blockchain Client Security and Trusted. Blockchain client can execute script program and consensus mechanism correctly.
- (2) Authorized Users Trusted. Authorized users are related to transaction. In order to ensure their own benefits, they are credible during the validity period.
- (3) Cipher and Cryptographic Algorithm Trusted. They are the basis of this paper.

4 SDAC Model and Description

4.1 SDAC Model

The SDAC model is shown in Fig. 3. The model consists of three entities: privacy owner, users of the system and potential attackers.

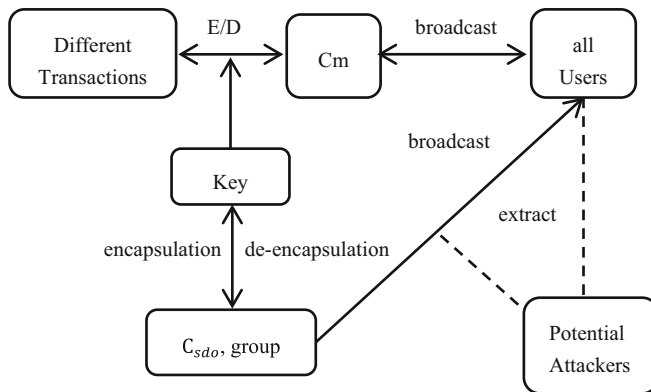


Fig. 3. SDAC model

- Privacy Owner: Sender and receiver of transaction.
- All Users: All participants in blockchain system, which are divided into authorized users and unauthorized users. Authorized users are allowed to access privacy transaction transactions, responsible for verifying transactions and implementing consensus mechanism. The $R = \{r_i | i \in N\}$ denotes the set of authorized users, which can be encrypted to *group*.

- **Potential Attackers:** All users in the system are likely to be attackers at different time. Authorized users attempt to save C_{sdo} to recover the decryption key at any time. Other users attempt to launch various attacks on P2P networks and authorized users in order to get C_{sdo} .

The first stage: Transaction transactions encrypted, key encapsulated and distributed phase (corresponding to the right and down direction's arrow in Fig. 3). The privacy owner divides the transaction transactions according to different access rights, encrypts the transactions with the key to form a privacy transaction and broadcasts it to the blockchain system. The encryption algorithm uses the Advanced Encryption Standard (AES). The privacy transactions with the same access rights use the same key and with different access rights use different keys. The keys are encapsulated to form C_{sdo} and then send the C_{sdo} to authorized users.

The second stage: Key de-encapsulated, transaction transactions decrypted, and consensus mechanism implemented phase (corresponding to the arrow up and left in Fig. 3). This stage mainly is traversed phase by the authorized users (reverse process of the first stage). Authorized users get decryption key through a series of processing, then decrypt transaction transactions to plaintext and then implement consensus mechanism.

4.2 SDAC Description

Transaction Establishment: The traders make a deal, give the parameter τ , call $\text{setup}(\tau)$ to generate the plaintext of the transaction transactions locally.

Generate the Key: The traders give the security parameter κ and Ke which is the receiver key of the previous round of generating privacy transactions, call $\text{setkey}(\kappa, Ke)$, generate the receiver key Ke' , and at last generate the secret information S which is presented access rights.

Generate Privacy Transactions: Call $\text{Esecret}(m, S)$, encrypt the transaction transactions plaintext into Privacy Transactions Cm and broadcast it to the whole blockchain system.

Authorizing Access: Giving the R , threshold δ and time stamp t , call $\text{SDACAR}(R, \delta, S, t)$ to get C_{sdo} , call $\text{SDACE}(R)$ to get $group$ and then broadcast C_{sdo} and $group$ to the whole blockchain system. Because secret S has been encrypted by access user's public key, unauthorized user(s) cannot decrypt it, thus achieving strong discretionary access control.

Transaction Authentication: Authorized user(s) take out $\text{Hash}(source)$, if it is the same as some transaction's hash, then continue to perform the following operations, otherwise, judge it is false transactions and vote to refuse it. Look up the global book-keeping, if the $\text{Hash}(source)$ is the same as $\text{Hash}(source)$ of other privacy transactions, judge it is double-spent attack and vote to refuse it too. Call $\text{SDACgetkey}(C_{sdo}, group)$ function, reconstruct secret S , call decryption algorithm, get transaction plaintext, and then implement consensus mechanism.

5 SDAC Algorithms

SDAC combines blockchain, authorization strategy and information encryption to achieve security discretionary access control method for blockchain. The main symbols and description of SDAC algorithm are shown in Table 1.

Table 1. Main symbols in SDAC Algorithms

Symbol	Description	Symbol	Description	Symbol	Description
In	Transaction input	Out	Transaction output	E	Encryption algorithm
Hash	Hash function	Ke/Ke'	Key	D	Decryption algorithm
Change	Change output	sign	Transaction's signature	ni/Ni	Input/output amount

5.1 SDAC Data Structure

For simplicity, the transaction transactions plaintext m in SDAC is similar to Bitcoin, as shown in Fig. 4. The ini ($i < N+$) is the total benefit of UserA through every mining or trading. The input and output meet:

$$\text{sum}(ni) = \text{sum}(Nj) + \text{num} (i, j \in N +) \quad (4)$$

The m is consist of $\text{Hash}(\text{source}), \text{Time}, ni, \text{Sign}, Fi, Ni, pb, Ti$, namely:

$$m = (\text{Hash}(\text{source}), \text{Time}, ni, \text{Sign}, Fi, Ni, pb, Ti) \quad (5)$$

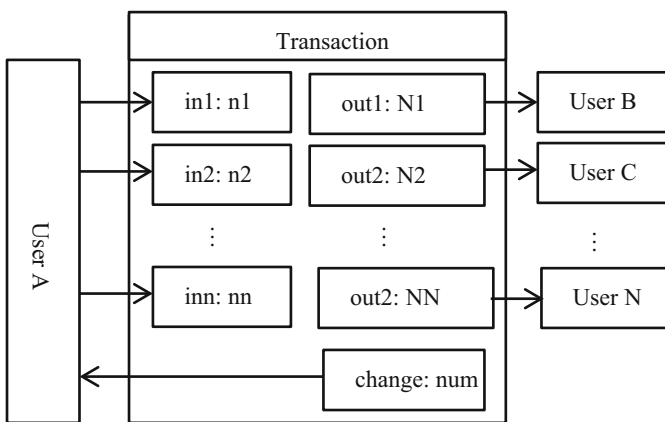


Fig. 4. Transactions

where, $\text{Hash}(\text{source})$ denotes the hash value of the source, Time denotes the time when the transaction transactions is generated, Sign is the sender's signature of the transaction transactions, Fi denotes that the input comes from the Fi th output of the previous transaction transactions, pb denotes receivers' public key, Ti denotes that this is the Ti th output.

Cm denotes Privacy transactions, which consist of input and output. The input data structure of Cm in SDAC method is shown in Fig. 5. The output structure of Cm is shown in Fig. 6. $E_{Ke}()/E_{Ke'}()$ denotes that using key Ke/Ke' to encrypt.

$\text{Hash}(\text{source})$	$E_{Ke}(\text{Time})$	$E_{Ke}(\text{ni})$	$E_{Ke}(\text{Sign})$	$E_{Ke}(\text{Fi})$
------------------------------	-----------------------	---------------------	-----------------------	---------------------

Fig. 5. Structure of input

$E_{Ke'}(\text{Ni})$	$E_{Ke'}(\text{pb})$	Ti
----------------------	----------------------	-------------

Fig. 6. Structure of output

5.2 SDAC Algorithms Constructions

- (1) Transaction establishment algorithm: $\text{setup}(\tau) \rightarrow m$.
- (2) Randomized algorithm: $\text{Random}() \rightarrow (0, 1)^\lambda$.
- (3) Key generation algorithm: $\text{setkey}(\kappa) \rightarrow S$.

$\text{setkey}(\kappa, Ke) \rightarrow S$

Input: κ, Ke

Output: S

1 $\text{Random}() \rightarrow Ke'$

2 $S = (Ke, Ke')$

- (4) Privacy transactions generation algorithm:
- $Esecret(m, S) \rightarrow Cm$
- .

$Esecret(m, S) \rightarrow Cm$

Input: m, S **Output:** Cm $Cm = (\text{Hash}(source), E_{Ke}(Time), E_{Ke}(ni), E_{Ke}(Sign), E_{Ke}(Fi), E_{Ke'}(Ni), E_{Ke'}(pb))$ 1 $E_{Ke}(Time)$ 2 $E_{Ke}(ni)$ 3 $E_{Ke}(Sign)$ 4 $E_{Ke}(Fi)$ 5 $E_{Ke'}(Ni)$ 6 $E_{Ke'}(pb)$

- (5) Authorized user sets encryption algorithm:
- $SDACE(R) \rightarrow group$
- .

$SDACE(R) \rightarrow group$

Input: R **Output:** $group$ 1 $\text{Random}() \rightarrow \text{key}$ 2 $R = E_{key}(R)$

- (6) Authorization algorithm:
- $SDACAR(R, \delta, S, t) \rightarrow C_{sdo}$

$SDACAR(R, \delta, S, t) \rightarrow C_{sdo}$

Input: R, δ, S, t **Output:** C_{sdo} $C_{sdo} = \{CS_i | i \in N^* \wedge i \leq \|R\|\}$ 1 **for** each r_i **do**2 $f_i(pb_i) = a_{\delta-1}pb_i^{\delta-1} + \dots + a_1pb_i + S$ 3 **end for**4 $d_i = \text{EECC}_{pb_i}(f_i(pb_i), pb_i, key)$ 5 $CS_i = (d_i, t)$

(7) Key recovery algorithm: $\text{SDACgetkey}(C_{sdo}, group) \rightarrow S$

 $\text{SDACgetkey}(C_{sdo}, group) \rightarrow S$

Input: $C_{sdo}, group$ **Output:** S pr denotes private key

```

1 get current time  $ct$ 
2 if  $ct < t$ 
3   for each  $r_j$  do
4     for each  $CS_i$  do
5        $((f_i'(pb_i), pb_i', key') = DeECC_{pr_i}(d_i)$ 
6         if  $pb_j = pb_i'$ 
7            $key = key'$ 
8            $f_j(pb_j) = f_i'(pb_i)$ 
9            $R = D_{key}(group)$ 
10        end if
11      end for
12    end for
13    for each  $r_i$  do
14       $l_i(0) = \prod_{0 \leq k \leq \delta-1, i \neq k} \frac{-x_i}{x_k - x_i}$ 
15       $S = \sum_{i=0}^{\delta-1} f_i(pb_i) l_i(0)$ 
16    end for
17  else
18    delete  $C_{sdo}, group$ 
19  end if

```

(8) Plaintext recovery algorithm: $\text{Dsecret}(Cm, S) \rightarrow m$

 $\text{Dsecret}(Cm, S) \rightarrow m$

Input: Cm, S **Output:** m

```

1  $D_{Ke}(E_{Ke}(Time))$ 
2  $D_{Ke}(E_{Ke}(ni))$ 
3  $D_{Ke}(E_{Ke}(Sign))$ 
4  $D_{Ke}(E_{Ke}(Fi))$ 
5  $D_{Ke'}(E_{Ke'}(Ni))$ 
6  $D_{Ke'}(E_{Ke'}(pb))$ 

```

6 SDAC Comprehensive Analyses

SDAC method encrypts transaction transactions' data structure of blockchain. Comparing with other methods, we analyzed the advantages and disadvantages of this paper shown in Table 2.

Table 2. SDAC compared with other schemes

Method	Strong privacy	Delay	Key/evidence management	Discretionary access control	Fine-grained access control
Coinjoin	No	High	Complex	No	No
MPC	Yes	High	Simple	No	No
Menoro	Yes	High	Complex	No	No
Zerocash	Yes	High	Complex	No	No
SDAC	Yes	Lower	Complex	Yes	Yes

- (1) Security. The security of SDAC depends on the security of cryptography. An attacker may capture C_{sdo} when it is in the P2P network communication and launch a Sybil attack. Even if achieving the attack, the attacker can recover the S using ECC decryption algorithm only if he gets at least δ different authorized users' private key and then uses AES decryption algorithm and S to get transaction transactions plaintext. Both encryption methods can effectively resist known attacks. According to modern cryptography, Both AES algorithm and ECC algorithm can resist the existing attacks under the existing conditions if the private key doesn't be leaked. So SDAC method is security.
- (2) Strong privacy. Strong privacy need consider both transaction privacy and identity privacy.

For the sender:

$$E_{Ke}(Time, ni, Sign)$$

For the receiver:

$$E_{Ke'}(Ni, pb)$$

So, the transaction transactions content and transaction amount are hidden, that is SDAC method provides transaction privacy protection.

For the keys:

$$S = (Ke, Ke')$$

$$f_i(pb_i) = a_{\delta-1}pb_i^{\delta-1} + \dots + a_1pb_i + S$$

Where, $i \in \{i | 0 \leq i \leq ||R||\}$.

$$\forall f_i(pb_i), \exists \text{EECC}_{pb}(f_i(pb_i))$$

For different transaction:

$$S \neq S'$$

$$f_i(pb_i) \neq f'_i(pb_i)$$

$$\forall pb_i, \exists \text{EECC}_{pb}(f_i(pb_i)) \neq \text{EECC}'_{pb}(f_i(pb_i))$$

To every user, different transaction has different keys, and encrypted amount is different. So, the relationship between participants can't be tracked and the relationship between participants' real identity and transactions can't be inferred, that is SDAC method provides identity privacy protection.

So, SDAC method achieves strong privacy protection.

- (3) Delay. Transactions do not require third party trusted institutions, and there is no waiting delay caused by online mixing. There is no need to compute public functions used for encryption, so there is no computation delay caused by multi-party secure computing. There is no no computation delay caused by calculating evidence of non-interactive zero knowledge. The owner only needs to sign the transactions once using the Elliptic Curve Digital Signature Algorithm (ECDSA), so the efficiency of signature is higher than that ring signature. The owner encapsulates the key to C_{sdo} with Lagrange polynomial and then encrypts it into C_{sdo} by ECC, and authorizes the user de-encapsulates C_{sdo} and decrypt C_m , so calculation delay is caused.
- (4) Key management. With SDAC method, using different secret key every time, the owner need store a large number of keys, which caused complex key management. In order to reduce it, they can delete it after transaction transactions confirmed.
- (5) Discretionary access control and fine-Grained access control.

$$E_S(m) = C_m$$

$$f_i(pb_i) = a_{\delta-1}pb_i^{\delta-1} + \dots + a_1pb_i + S$$

$$\text{EECC}_{pb}(f_i(pb_i)) = f'_i(pb_i)$$

$$\forall r_i \in R, \exists \text{DECC}_{pr}(f'_i(pb_i)) = f_i(pb_i)$$

$$\forall r_j \notin R, \text{DECC}_{pr}(f'_i(pb_i)) = f_j(pb_j) \neq f_i(pb_i) (j > 0)$$

$$S' = \sum_{j=0}^{\delta} l_j(pb_j)f_j(pb_j)$$

$$f_j(pb_j) \neq f_i(pb_i)$$

$$S' \neq S$$

$$D_{S'}(C_m) \neq m$$

Namely, unauthorized users cannot scan transaction transactions.

$\forall r_j \in R$ is determined by the owner, so SDAC can achieve discretionary access control.

$$\| R \| \geq 0 \wedge \| R \| \in N$$

Namely, SDAC can achieve fine-Grained access control.

- (6) Low computability and efficiency. The computability and efficiency of SDAC method depend on the computability and efficiency of cryptographic algorithm. The method only use ECDSA once, needn't sign by all participants, which have to in ring signature method, so the size of storage space is smaller than it and the output of transaction transactions don't limit by the number of participants. The method only uses AES algorithm to encrypt and decrypt transaction transactions and authorized users set once, only uses ECC algorithm to encrypt and decrypt C_{sdo} once, respectively. AES algorithm has the characteristics of high efficiency and fast speed. ECC algorithm operates on keys and secret components, having with only a few bytes. From the perspective of cryptography, under the same conditions, the AES algorithm and ECC algorithm working together are two orders of magnitude better than non-interactive zero-Knowledge proof in terms of computational complexity and efficiency.

7 Conclusion

Based on blockchain privacy protection, combining AES, ECC encryption algorithm, ECDSA, Lagrange polynomial and authorization strategy, this paper proposed the SDAC method and implements the corresponding algorithms. SDAC method encrypts the transaction transactions data structure of blockchain, and then transmit the encrypted and encapsulated key to authorized users. They decrypt and de-capsulate to get the key then recover the transaction transactions to implement consensus mechanism. SDAC method can realize fine-grained access control, discretionary access control transaction transactions and strong privacy of blockchain, thus achieving the goal of design protection. Compared with Menoro, SDAC method is more efficient to generate transactions. Compared with Zerocash, its computational cost is lower. The next step is to reduce the complexity of key management.


Acknowledgment. This work was supported by Project 61403183 of the National Science Foundation of China, Project 2017JJ4048 of the Hunan Provincial Natural Science Foundation of China, Project 18A230 of the Hunan Provincial Education Office Science Research of China, Project 20183350502 and 20191550502 of the Hunan Provincial Finance Office Science Research of China.

References

1. Bertram, S.: A privacy-preserving system for data ownership using blockchain and distributed databases. arXiv preprint [arXiv:1810.11655](https://arxiv.org/abs/1810.11655) (2018)
2. Chen, L.: Unraveling blockchain based crypto-currency system supporting oblivious transactions: a formalized approach. In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, pp. 23–28. ACM, Abu Dhabi (2017)
3. Feng, Q.: A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* (2018)
4. Koshy, P., Koshy, D., McDaniel, P.: An analysis of anonymity in bitcoin using P2P network traffic. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 469–485. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45472-5_30
5. Reid, F.: An analysis of anonymity in the bitcoin system. In: Altshuler, Y., Elovici, Y., Cremers, A., Aharony, N., Pentland, A. (eds.) Security and Privacy in Social Networks, pp. 197–223. Springer, New York (2013). https://doi.org/10.1007/978-1-4614-4139-7_10
6. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp. 34–51. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39884-1_4
7. Biryukov, A.: Bitcoin over tor isn't a good idea. In: 2015 IEEE Symposium on Security and Privacy, pp. 122–134. IEEE (2015)
8. Liao, K.: Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin. In: 2016 APWG Symposium on Electronic Crime Research (eCrime), pp. 1–13. IEEE (2016)
9. Bissias, G.: Sybil-resistant mixing for bitcoin. In: Proceedings of the 13th Workshop on Privacy in the Electronic Society, pp. 149–158. ACM (2014)
10. Chaum, D.: Untraceable electronic mail, return addresses and digital pseudonyms. In: Gritzalis, D.A. (ed.) Secure Electronic Voting, pp. 211–219. Springer, Boston (2003)
11. Joinmarket-Coinjoin. <https://bitcointalk.org/index.php?topic=919116>. Accessed 2016
12. Ziegeldorf, J.H.: Coinparty: secure multi-party mixing of bitcoins. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, pp. 75–86. ACM (2015)
13. Monero Homepage. <https://getmonero.org/>. Accessed 10 Sept 2019
14. Miers, I.: Zerocoin: anonymous distributed e-cash from bitcoin. In: 2013 IEEE Symposium on Security and Privacy, pp. 397–411. IEEE (2013)
15. Sasson, E.B.: Zerocash: decentralized anonymous payments from bitcoin. In: 2014 IEEE Symposium on Security and Privacy, pp. 459–474. IEEE (2014)
16. Shamir, A.: How to share a secret. *Commun. ACM* **22**(11), 612–613 (1979)



Secure Healthcare Data Aggregation Scheme for Internet of Things

Muhammad Azeem and Ata Ullah 

Department of Computer Science, National University of Modern Languages,
Islamabad 44000, Pakistan
muhammadazeem0493@gmail.com, aullah@numl.edu.pk

Abstract. Internet of things (IoT) involves massive number of smart devices that can communicate across different networks to exchange data. IoT enabled smart healthcare data is aggregated for transmitting to FoG server. Healthcare data is sensitive in nature, so there is a need to provide protection against various security attacks. This paper presents a secure healthcare based data aggregation (SHDA) scheme to transmit sensitive data from sensor nodes to collector nodes that further transmit to the FoG node. It includes a proposed model for data collection from sensing devices and aggregate at collector nodes. Next, we present the message receiving algorithm at collector node and message extraction algorithm at FoG node. SHDA is simulated using NS2.35 in Fedora Core 16 where TCL is used for node deployment and C language is used for message handling among devices. AWK script are used to get the results of simulations from trace files. Results prove the dominance of our scheme as compared to counterparts in terms of communication cost, computation cost and energy consumption.

Keywords: Privacy · Security · Healthcare · Data aggregation · FoG computing · IoT

1 Introduction

The evolution of healthcare Internet of things (IoT) introduce an interconnection between patient, medical professionals, medical sensors and trusted servers [1]. A healthcare IoT improve the quality and efficiency of patient medical treatment [2, 3]. Smart sensing devices and medical instruments and wearable medical devices are helpful for remotely monitoring healthcare data in smart healthcare IoT network [4]. Medical cyber physical system composed of a network of medical sensing devices and provides high quality of healthcare services [5]. In IoT enable smart healthcare based WSNs are helpful in monitoring patient health. Sensing devices are used for measuring patient health like temperature, blood pressure, glucose and heartbeat [6]. Patient sensitive data aggregated through smart wearable sensing devices and this aggregated after processing received to doctor or medical consultant to observe the present health condition of patient. Sensing devices are broadly appropriate in physical world scenarios [7, 8].

In IoT based healthcare system, FoG node basically a device with capability of temporarily data storage, data computation and network connectivity. FoG layer provide low latency and high response time in this way increasing the capability of healthcare systems [9]. In FoG based healthcare architecture sensing nodes aggregate patient data and transmit this collected data on FoG server and after some processing on locally store data. FoG server upload this locally store and processed data on cloud server [10]. FoG computing provides local data analysis on aggregated data from smart sensing devices. In smart healthcare architectures implementation of FoG node reduce computation overhead at cloud server [11]. Middleware between cloud and IoT devices known as FoG is a right choice when services require fast response, data filtration, pre-processing, security and privacy [12].

In smart healthcare technology provides mechanism to remotely monitor healthcare data from wearable sensors. In this way security and privacy are backbone of the smart healthcare so security threads and privacy requirements are the primary challenges in smart healthcare [13]. Technologies like smart phones and wearable devices turned healthcare into smart personal healthcare [14, 15]. In IoT based WSNs mobile phones gain a lot of attention worldwide. Mobile phones used sensor node and collector node but mobile phone as a sensor node is a challenging due to mobility of sensor nodes. On the other-hand mobile phone is a right choice to use as a collector node that helps to easily communicate with medical consultants and doctors [16]. IoT smart healthcare applications provide benefit for personal human healthcare. On the other-side security and privacy are still challenging issue in smart personal healthcare [17]. In healthcare scenario secure data aggregation and data transition to the trusted server are still challenging issue. In wireless body area network sensing devices are attached to the body of the patient and these devices aggregate secure data and transfer over the server and medical professional access this data in this scenario remotely secure data transmission and privacy of the patient and medical professional are the main challenges in remote healthcare [18].

The main problem is secure data aggregation from smart devices (SDs) to FoG node. In aggregation scenario, collection and transmission of data are challenging issues and security of data in healthcare also a challenging task because while aggregating and sharing data high risk of security threads. This paper introduces a FoG based secure healthcare based data aggregation scheme. In our work, peer to peer communication involves wearable SDs that exchange data to collector nodes (CNs). Next, the CNs share data to FoG server efficiently to reduce communication cost. Moreover, FoG node sends query request through CNs and the SDs that have responded to fulfill query scenario.

This paper presents a proposed scheme on privacy preserved and secure healthcare data aggregation FoG based scheme. Our proposed work is simulated using NS2.35 in Fedora Core 16. TCL and C languages are used for node deployment and message sharing. We formulated AWK script to get the results of simulations from trace files. Our main contributions in this work are as follow.

- (1) We have explored an extensive amount of literature to discuss different schemes for data aggregation. Schemes are categorized into secure aggregation schemes and secure healthcare based schemes.

- (2) Next, we present the secure healthcare based data aggregation scheme (SHDA). It formulates a system model where sensing devices and FoG nodes are shown.
- (3) Next, we propose Message Receiving Algorithm (MRA) for collector node and Message Extraction Algorithm (MEA) for FoG node.
- (4) Finally, simulation scenario is explored to extract results.

Rest of the paper is organized as follows; Sect. 2 explores the literature review for various secure healthcare data aggregation schemes. In Sect. 3, we present our proposed model for SHDA along with message receiving and extraction algorithms. Section 4 explores results and analysis whereas Sect. 5 concludes our work.

2 Literature Review

In this section, we discuss various privacy preserved secure aggregation schemes and also healthcare based secure aggregation scheme. In this way, we further divided this section into two sections first section contain secure aggregation schemes and second section contain healthcare base secure data aggregation schemes.

2.1 Secure Data Aggregation Schemes

In this section, we discussed data aggregation schemes. In discussion, we briefly describe the main key features of these schemes and their contributions in physical world. This portion includes only secure data aggregation schemes. We also discussed methods and techniques of secure data aggregation schemes.

Huang et al. [19] formulate a control and secure data access scheme. It depends upon ciphertext attribute based encryption and attribute based signature in IoT enabled FoG computing. In attribute based data encryption scenario, sensing nodes share ciphertext to FoG server. FoG server perform encryption and decryption data and further upload data to cloud server and in data receiving perspective a user can access data whose attribute satisfy the required policies. The system provides secure data access control and secure update ciphertext. Wang et al. [20] introduce a secure aggregation scheme (ASAS). This proposed architecture using pseudonyms and homomorphic encryption to preserved the privacy of aggregated data and protect the identity of sensing nodes. This scheme provides low computational overhead at cloud server and saves bandwidth between FoG and cloud servers. In contrast energy consumption and communication cost increased. End nodes anonymously share data to the FoG server and while preserving the integrity of received data from end nodes and share data to the cloud server.

Guan et al. [21] discussed a device oriented privacy preserved data aggregation scheme. This work provides pseudonym certificate autonomous update and privacy for aggregated data. In limited devices scenario, it provides high performance. In this formulated work, End nodes aggregate data from smart devices and share this data to the FoG node and it performs local processing on data and share this locally processed data to the cloud server. On Cloud server further processing and analysis are performed. Independent certificate services like trusted certification and local certification

authority both of them provide secure and privacy preserved data collection. Lu et al. [22] proposed a lightweight and privacy preserved data aggregation scheme. In this system to aggregate data at one device combine homomorphic encryption and Chinese Remainder Theorem. At network edges one-way hash chain technique is used to filter aggregated data from false data injection attacks. In this way network filter data locally at the edge devices and send it to the control center. Sensing devices are subdivided according to their functionality. proposed scheme efficient because of low computational and communication cost.

2.2 Healthcare Based Secure Data Aggregation Schemes

In this section, we discussed data aggregation schemes. In discussion, we briefly describe the main key features of these schemes and their contributions in physical world. This portion includes only secure healthcare based data aggregation schemes. We also discussed methods and techniques of schemes as follows.

Ullah et al. [23] introduces an efficient healthcare data aggregation scheme. It uses secure heterogeneous IoT based compression mechanism. Secure data transfer from sensing node to collector node and message receiving algorithm used to receive data at collector node. Compression performed on received data at collector node in this way reduce data size and low energy consumption for communication. This work use peer to peer communication between sensing nodes and node to node between collector nodes. Data received from sensing nodes is transmit to the FoG node and at FoG node message extraction algorithm use to collect data from collector nodes and after collecting data at FoG node in specific time stamp perform some local processing on aggregated data and then share this processed data over the cloud server. Hamza et al. [24] presents a lightweight authentication scheme for smart healthcare system. Proposed work focus on the security of healthcare system and using HMAC to authenticate the collected data during data transmission. In system model wearable sensor nodes attached with the patient body and this aggregated data send on edge node and edge node further share this data with the base station or FoG server. In this way for secure data aggregation proposed scheme provide authentication for sensitive healthcare data both at sensing devices and FoG server. This scheme only applicable for devices security of healthcare system. Mahmood et al. [25] introduces secure authentication and prescription safety scheme. It ensures security and privacy of both patient and medical consultants while remotely conversation. It also provides anonymity and untraceability of patient and doctor during session key generation and secure data transmission to the reliable server. Proposed work uses symmetric key to authenticate the participants and provide secure data transmission between patient and the medical consultant. Moosavi et al. [26] presents an efficient and secure authorization and authentication architecture for healthcare. Privacy and security plays a vital role while transmission of patient sensitive medical healthcare data. The aim of their work is the secure authentication and authorization of the remote patients and healthcare professionals. Proposed work used distributed smart healthcare gateway to authenticate and authorized the remote users in this way reduce the overhead of medical sensors so they are not performing these security protocols. Proposed architecture is more secure than the centralized delegated architecture because between smart healthcare gateway and

medical sensor nodes it uses secure key management scheme and it depend upon the DTLS handshake protocol. Proposed solution provide scalable and reliable security for end-to-end healthcare systems.

Haiping et al. [27] introduces healthcare system (HES) framework that collect data from the medical sensors of wireless body area network. This collected data transmit through the wireless sensor network and this medical data through gateway uploaded in the wireless personal area network. The main features of proposed work are easily deployed wireless sensor networks, direct communication between edge devices and medical devices and privacy preserving approach. HES framework involves the GSRM scheme for secure data transmission and key distribution and HEBM scheme expert system analyze medical data and formulate the results automatically and also provide privacy for medical data. Yang et al. [28] formulate a lightweight break glass access control (LiBAC) system this system provides to paths one for normal condition and other for emergency situation for accessing encrypted healthcare data. In normal condition attribute based access policy user use secret key access and decrypt the medical data. On the other-hand in emergency condition break glass access is a password based access and password set by a patient shared with the emergency contact persons (ECP) in this way these person decrypt secret key using password and timely decrypt the patient medical data. Proposed framework is lightweight so consume less space and low transmission overheads.

3 Proposed Solution

We present the system model and proposed secure data aggregation algorithm. We also present a smart healthcare based secure data aggregation scheme. In our case proposed work reduce storage cost and computation cost at cloud server comparing proposed schemes with those schemes discussed in literature review section.

3.1 System Model

In our proposed system model, we present a communication architecture for smart sensing devices in smart healthcare scenarios and elaborate it in Fig. 2. Proposed healthcare model consist of different types of wearable smart sensing devices (SD). Like peer to peer communication SD aggregate medical data and transmit sensitive data to an assigned collector nodes (CN). Suppose in our work all SD may not transmitting data in cyclic way and may be transmit data on request of FoG server or selected threshold delay. It helps to avoid sensing hindrance in case of large no of sensing devices exchange sensitive healthcare data. In this model, medical SD sending sensitive data to CN and collector nodes sending received data to the FoG server. In Fig. 1, we only show four CNs to elaborate basic concept of CN to SD data aggregation and CN to CN data aggregation. In physical world scenario large number of CN are present and some CN nodes directly send collected data to the FoG server. CN1 and CN3 are directly send data to the FoG server. On the other-hand, if CN cannot send data directly to the FoG server so aggregated data is send to the FoG server through neighboring CN. For example, we assume CN2 can exchange data with CN4 and CN4 used as an

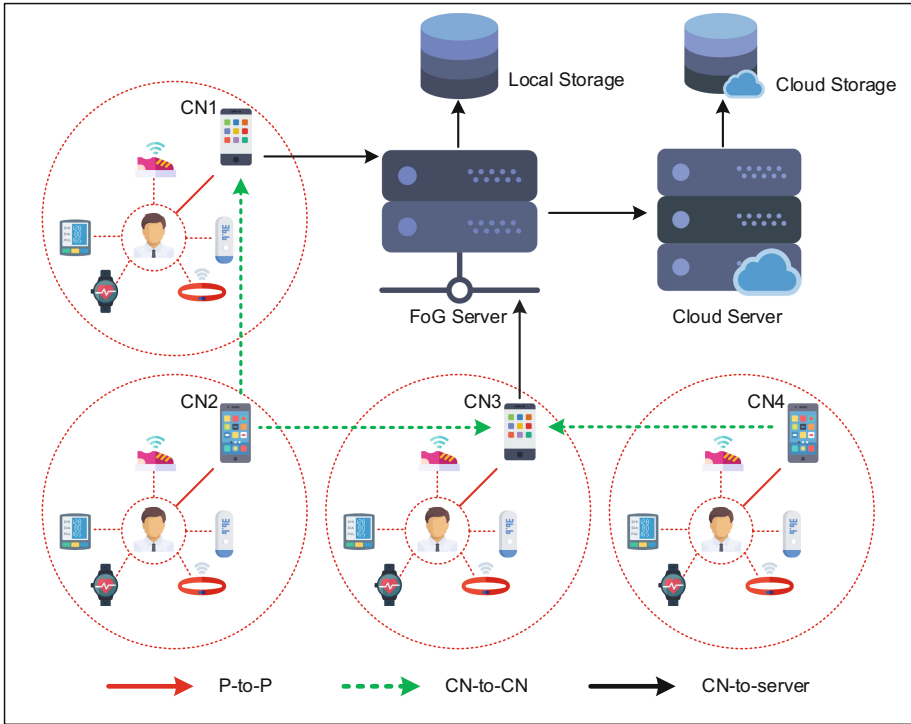


Fig. 1. System model for FoG-oriented smart data aggregation in IoT

intermediate node and transfer this data to the FoG server in this way CN4 also directly get data from the SD and also exchange data with the neighboring CNs. In peer to peer communication scenario, if intermediate CNs are far away from the FoG server and size of data carrying by intermediate nodes increased after sending from any individual node in this way communication cost highly increased. On the other-side data mostly not compressed it increases the over-head at FoG and Cloud server. We assume if devices transmit the data in cyclic way and large amount of devices transmitting healthcare sensitive data it will cause hindrance in sensing procedure. It's a challenging issue to formulate a green sensing mechanism to avoid sensing hindrance.

In our proposed model, Collector nodes received the aggregated data and moves towards sensor nodes. FoG part in data aggregation. In this scenario, records are easily maintaining on the basis of device ID in FoG server.

3.2 Secure Healthcare Based Data Aggregation (SHDA) Scheme

In our proposed section, we formulate solution for identified problem by presenting secure healthcare data aggregation scheme. Our proposed work further divided into three phases SD sensing data and transfer to CNs, message receiving at CN and extraction at base station. We elaborated our proposed scenario with two algorithms

first message receiving algorithm at CN and message extraction algorithm at FoG node. In this section Table 1, shows the list of notations.

Table 1. List of notations

Notations	Description
ID_{SD_i}	ID of sensing devices
HP_V	Healthcare parameter values
TS_{SD_i}	Sensing devices time stamp
n	Total number of SDs transmit data to CN
C_i	Ciphertext at SDs
M_i	Decrypted message sending from sensing devices to CN
$H(C_v)$	Hash of concatenated values
A_m	Aggregated message at CN
M_{FS}	Decrypted message from CN to FoG node
$List_{M_{SD_i}}$	List of messages from sensing devices
$E_{k_{SD_i-CN}}$	Symmetric key between CN and sensing devices
$E_{k_{CNi-FS}}$	Symmetric key between FoG node and CN

FoG server formulate data according to the required format and upload to the cloud server after aggregating data from multiple regions in certain threshold time. In Phase-1 sensing devices share sensing data to the CN. In this way, SDs encrypting data using preloaded keys and share these keys with FoG node and start sharing data to CNs while doing this only those SDs share data which satisfied the required conditions. ANs directly share data with FoG server only when it is one-hop away from FoG server. otherwise CNs share data with intermediary CN to transmit data over FoG server. An intermediate CN collect data and use delimiter to differentiate with its own data and aggregated data from other CN.

In our proposed SHDA scheme, sensor nodes collect healthcare parameter values (HP_V). Cipher text $C_i = E_{k_{SD_i-CN}}\{ID_{SD_i}, HP_V, TS_{SD_i}, H(ID_{SD_i}||HP_V||TS_{SD_i})\}$ is obtained by using symmetric key. It concatenates $ID_{SD_i}||HP_V||TS_{SD_i}$ values and sensor nodes send data at CN. In phase-2, we introduce MRA at CN which shown in Algorithm 1. It received message from sensing nodes and also received from the other aggregated nodes. In Algorithm 1, CN receives the message from all sensor nodes. In message receiving algorithm decrypt the ciphertext (C_i) to get $ID_{SD_i}, HP_V, TS_{SD_i}$ as M_i . It also concatenate values. After that calculate the time stamp of data ($TS_{CN} - TS_{SD_i}$) $< \Delta t$. If condition true so message is fresh otherwise discard it. In case, condition is true calculate the hash of the received parameters $H'(C_v)$ equals $H(C_v)$. In this way, if condition false so message discarded because of data integrity violation. On the other-hand, if condition true aggregated message concatenate with M_i to get aggregated message at collector node (A_m).

 Algorithm No. 1 : Message Receiving Algorithm (MRA) at CN

Initialize $A_m = \text{null}$

1. Decrypt C_i to get $M_i = \{ ID_{SD_i}, HP_V, TS_{SD_i}, H(C_v) \}$ from SD
2. If $(TS_{CN} - TS_{SD_i}) < \Delta t$ then
3. If $H'(C_v)$ equals $H(C_v)$ then
4. $A_m = A_m \parallel \text{"."} \parallel M_i$
5. Else
6. Message discarded because of integrity violation
7. End if
8. Else
9. Discard outdated message
10. End if

In phase-3, introduces proposed message extraction algorithm at FoG node shown in Algorithm 2. In this proposed algorithm, $C_{CNq} = E_{k_{CNi-FS}} \{ ID_{CNq}, A_m, TS_{CNq}, H(ID_{CNq} \parallel A_m \parallel TS_{CNq}) \}$ Aggregated message received from the collector node at the FoG node. At FoG node while using (MEA) get M_{FS} by separating $ID_{SD_i}, HP_V, TS_{SD_i}$ and also and also $ID_{SD_i} \parallel HP_V \parallel TS_{SD_i}$ concatenate values. In next step of algorithm, we calculate the time stamp of data $(TS_{FS} - TS_{CNq}) < \Delta t$. If condition true so message is fresh otherwise discard it. In case, condition is true calculate the hash of the received parameters $H'(C_b)$ equals $H(C_b)$. In this way, if condition false so message discarded because of data integrity violation. In next step, if condition true then loop count from 1 to n and q = 1 to n and $List_{M_{SDi}}$ is a list of messages received from sensing nodes and split received data and using colon as a delimiter. In the end extract the health parameter values (HP_V) from list of messages received from sensing devices ($List_{M_{SDi}}$).

 Algorithm No. 2 : Message Extraction Algorithm (MEA) at FoG Node

Initialize $A_m = \text{null}$

1. Decrypt C_i to get $M_i = \{ ID_{SD_i}, HP_V, TS_{SD_i}, H(C_v) \}$ from SD
2. If $(TS_{CN} - TS_{SD_i}) < \Delta t$ then
3. If $H'(C_v)$ equals $H(C_v)$ then
4. $A_m = A_m \parallel \text{"."} \parallel M_i$
5. Else
6. Message discarded because of integrity violation
7. End if
8. Else
9. Discard outdated message
10. End if

4 Results and Analysis

Our work validated through simulation by installing multiple sensors in a specific area and separately formulate each type of node by placing suitable class with functions for receiving, sending, encrypt and decrypt algorithms. We simulated our proposed scheme using NS2,35 on Fedora core and TCL files have configuration of nodes, deployment of nodes. Separate classes are created using C language for applying the sending and receiving functionality of SDs and CDs and also provide functions for applying encryption and decryption. Our proposed scheme used AWK script files to attain values of results from trace files. We compared our scheme with other schemes and this comparison shows the supremacy of our scheme.

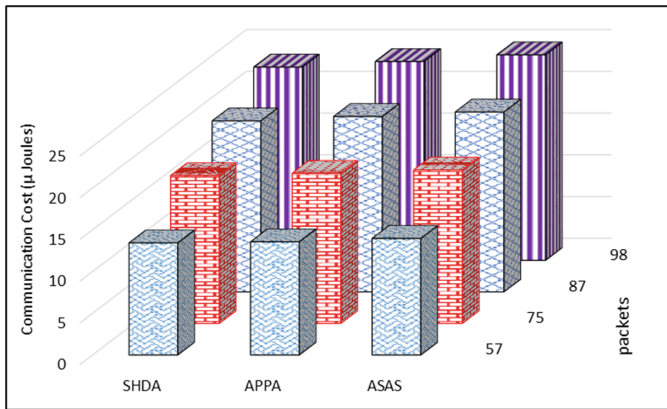


Fig. 2. Communication cost

In Fig. 2, we calculate the communication overhead at low power devices like SDs. shown the supremacy of SHDA scheme while comparing with ASAS and APPA schemes. Results prove that our proposed scheme has low communication overhead as compared with other two schemes at low power devices. Using simulated values presents the communication cost with no of packets. In Fig. 3, we calculate the computation cost in terms of data aggregation at CNs. Our proposed SHDA scheme shown supremacy in terms of computational cost while comparing with APPA and ASAS. Results of simulation show that our proposed scheme has less computation cost as compared with other two schemes. Presents the computation cost with number of smart devices. In Fig. 4, we compare energy consumption with time at CNs. Proposed scheme SHDA compare with APPA and ASAS schemes. Simulation results show the supremacy of our proposed scheme and provide less energy consumption.

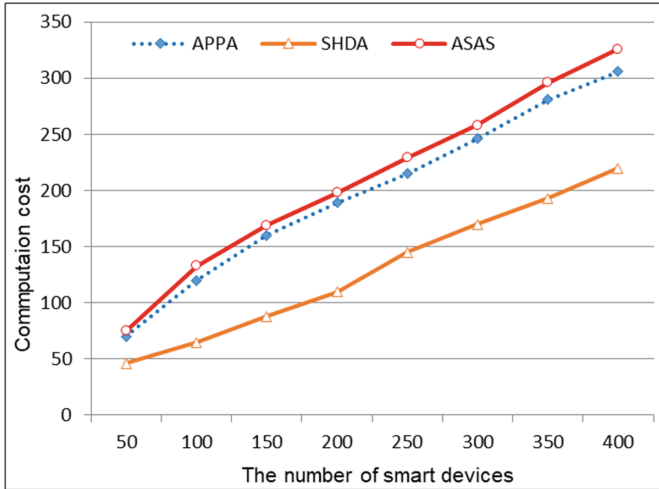


Fig. 3. Computation cost

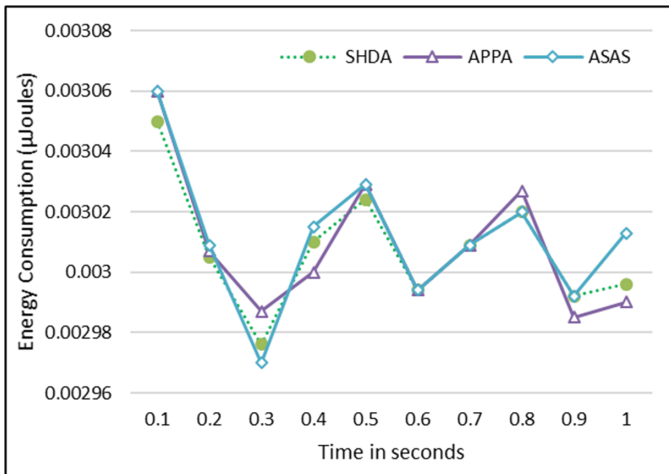


Fig. 4. Energy consumption

5 Conclusion

Our proposed SHDA scheme ensures the security of data while transmitting from SDs to CN that further transmits to FoG server. MRA and MEA algorithms receive and extract the data at collector and FoG nodes, respectively. In this case, the collector node can directly transmit to FoG node when one-hope away, otherwise, intermediate nodes are involved. During extraction, delimiter is used to differentiate between data sending devices like SDs and CN, respectively. Our proposed work validates through

simulation using NS 2.35 in Fedora Core 16. We use TCL for node deployment and for message handling we use C language. Results are extracted using AWK script from multiple trace files as per deployment scenarios. trace files using. Results prove the supremacy of proposed SHDA scheme in terms of less communication cost, less computation cost and less energy consumption.


References

1. Rodrigues, J.J.P.C., et al.: Enabling technologies for the internet of health things. *IEEE Access* **6**, 13129–13141 (2018)
2. Scarpato, N., Pieroni, A., Di Nunzio, L., Fallucchi, F.: E-health-IoT universe: a review. *Int. J. Adv. Sci. Eng. Inf. Technol.* **7**(6), 2328 (2017)
3. Yin, Y., Zeng, Y., Chen, X., Fan, Y.: The Internet of Things in healthcare: an overview. *J. Ind. Inf. Integr.* **1**, 3–13 (2016)
4. Qi, J., Yang, P., Min, G., Amft, O., Dong, F., Xu, L.: Advanced Internet of Things for personalised healthcare systems: a survey. *Pervasive Mob. Comput.* **41**(600929), 132–149 (2017)
5. Dey, N., Ashour, A.S., Shi, F., Fong, S.J., Tavares, J.M.R.S.: Medical cyber-physical systems: a survey. *J. Med. Syst.* **42**(4), 1–10 (2018)
6. Pirbhulal, S., Zhang, H., Wu, W., Mukhopadhyay, S.C., Zhang, Y.T.: Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. *IEEE Trans. Biomed. Eng.* **65**(12), 2751–2759 (2018)
7. Kulkarni, A., Sathe, S.: Healthcare applications of the Internet of Things: a review. *Int. J. Comput. Sci. Inf. Technol.* **5**(5), 6229–6232 (2014)
8. Zhu, T., Dhelim, S., Zhou, Z., Yang, S., Ning, H.: An architecture for aggregating information from distributed data nodes for industrial internet of things. *Comput. Electr. Eng.* **58**(August), 337–349 (2017)
9. Chang, V., Firouzi, F., Constant, N., Mankodiya, K., Badaroglu, M., Farahani, B.: Towards fog-driven IoT eHealth: promises and challenges of IoT in medicine and healthcare. *Futur. Gener. Comput. Syst.* **78**, 659–676 (2017)
10. Hu, P., Dhelim, S., Ning, H., Qiu, T.: Survey on fog computing: architecture, key technologies, applications and open issues. *J. Netw. Comput. Appl.* **98**, 27–42 (2017)
11. Mahmud, R., Koch, F.L., Buyya, R.: Cloud-fog interoperability in IoT-enabled healthcare solutions, pp. 1–10, December 2017 (2018)
12. Aazam, M., Zeadally, S., Harras, K.A.: Fog computing architecture, evaluation, and future research directions. *IEEE Commun. Mag.* **56**(5), 46–52 (2018)
13. Wu, W., Pirbhulal, S., Li, G.: Adaptive computing-based biometric security for intelligent medical applications. *Neural Comput. Appl.* 1–16 (2018). <https://doi.org/10.1007/s00521-018-3855-9>
14. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., Shamshirband, S.: Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egypt. Informatics J.* **18**(2), 113–122 (2017)
15. Liu, H., Yao, X., Yang, T., Ning, H.: Cooperative privacy preservation for wearable devices in hybrid computing based smart health. *IEEE IoT J.* **4662**(1), 1–11 (2018)
16. Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S.: The Internet of Things for health care: a comprehensive survey. *IEEE Access* **3**, 678–708 (2015)
17. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in Internet-of-Things. *IEEE IoT J.* **4**(5), 1250–1258 (2017)

18. Lin, H., Yan, Z., Chen, Y., Zhang, L.: A survey on network security-related data collection technologies. *IEEE Access* **6**, 18345–18365 (2018)
19. Huang, Q., Yang, Y., Wang, L.: Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things. *IEEE Access* **5**, 1–9 (2017)
20. Wang, H., Wang, Z., Domingo-Ferrer, J.: Anonymous and secure aggregation scheme in fog-based public cloud computing. *Futur. Gener. Comput. Syst.* **78**, 712–719 (2018)
21. Guan, Z., et al.: “APPA: an anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. *J. Netw. Comput. Appl.* **125**(June 2018), 82–92 (2019)
22. Lu, R., Heung, K., Lashkari, A.H., Ghorban, A.A.: A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access* **5**, 3302–3312 (2017)
23. Ullah, A., Said, G., Sher, M., Ning, H.: Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN (2019)
24. Khemissa, H., Tandjaoui, D.: A lightweight authentication scheme for e-health applications in the context of Internet of Things. In: *Proceedings of NGMAST 2015 9th International Conference on Next Generation Mobile Applications Services and Technology*, pp. 90–95 (2016)
25. Mahmood, Z., Ning, H., Ullah, A., Yao, X.: Secure authentication and prescription safety protocol for telecare health services using ubiquitous IoT. *Appl. Sci.* **7**(10), 1069 (2017)
26. Moosavi, S.R., et al.: SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput. Sci.* **52**(1), 452–459 (2015)
27. Huang, H., Gong, T., Ye, N., Wang, R., Dou, Y.: Private and secured medical data transmission and analysis for wireless sensing healthcare system. *IEEE Trans. Ind. Inf.* **13** (3), 1227–1237 (2017)
28. Yang, Y., Liu, X., Deng, R.H.: Lightweight break-glass access control system for healthcare internet-of-things. *IEEE Trans. Ind. Inf.* **14**(8), 3610–3617 (2018)



A Multi-location Defence Scheme Against SSDP Reflection Attacks in the Internet of Things

Xin Liu¹(✉) , Liang Zheng¹, Shuai Cao¹, Sumi Helal², Jiehan Zhou^{3,4}, Hunfu Jia⁵, and Weishan Zhang¹

¹ College of Computer Science and Technology, China University of Petroleum, Qingdao 266580, China

lx@upc.edu.cn

² School of Computing, Lancaster University, Bailrigg, UK

³ Information Technology and Electrical Engineering, University of Oulu, Oulu, Finland

⁴ Electrical and Computer Engineering, University of Toronto, Toronto, Canada

⁵ Nankai University, Tianjin, China

Abstract. The proliferation of the Internet of Things (IoT) has led to a rapid increase in SSDP (Simple Service Discovery Protocol) reflection attacks. However, there is very scarce work on defending these attacks, with only some engineering advices on shutting down attacked services. This paper proposes a comprehensive approach to defend SSDP reflection attacks, which is called multi-location defence scheme (MLDS). MLDS operates at multiple places, working throughout the attacking link, starting from attack sources to victims, without prior detecting attacks. Attackers usually utilized bots in a botnet to launch attacks, but bots can act as defenders to carry out defence strategies in our MLDS, which is an unconventional approach to make the defence effective. Finally, we analyzed thoroughly packet traffic situations when deploying MLDS to different defence locations.

Keywords: Denial-of-service · DRDoS · SSDP reflection attack · TTL

1 Introduction

Countless devices have connected to the Internet, leaving the Internet of Things (IoT) exposed to many security threats without proper security mechanisms. Opened services on IoT devices may be exploited to launch different malicious attacks like the Denial-of-service (DoS) attacks [11], in the format of Distributed Denial of Service (DDoS), or the distributed reflective denial-of-service (DRDoS) [1], for financial, political or purely destructive motivations. During the DoS attack, attackers disrupt services of victims, which can be targeting servers or networks.

The DDoS attack is proliferating in the Internet of Things age. These attacks usually result in heavy network traffic or heavy load on victims. On October 21st in 2016, a series of DDoS attacks caused widespread disruption of legitimate Internet activities in the US [24]. These attacks were made possible by a large number of unsecured Internet-connected devices, such as home routers and surveillance cameras. According to the statistics from Kaspersky Lab [17], 50% of DDoS attacks led to noticeable disruptions of services and 24% of DDoS attacks resulted in services being completely unavailable.

In a DRDoS attack, an attacker makes fake requests by replacing source IP address with the IP address of the selected victim. He sends those fake requests to service providers which then send service response packets to the spoofed IP address. The sizes of those response packets from service providers in DRDoS attacks are always many times larger than that of request packets. Therefore service providers are also called reflectors or amplifiers, which may be various networked devices, such as PCs, printers, routers, WiFi access points, mobile devices, cameras, and so on. Vulnerable service providers are carefully selected as amplifiers by attackers, where response packets are much larger compared with request packets.

Attackers try to find vulnerabilities in various Internet protocols or services to amplify responses from service providers in order to significantly increase communication traffic. Rossow analyzed 14 protocols susceptible to bandwidth amplifications and gave a bandwidth amplification factor (BAF) to every protocol [23]. He found that UPnP enabled hosts can respond with a reply packet per service on Simple Service Discovery Protocol (SSDP) discovery requests.

According to the bi-annual DDoS Threat Report from NSFOCUS [22], the proliferation of IoTs is responsible for increased SSDP reflection attacks. From the Akamai's report on DDoS attacks (Q3 2016 to Q2 2017), the number of DDoS reflector source IPs with different kinds of Internet protocols is shown in Table 1. SSDP is the protocol most frequently used for reflection attacks in three of the four quarters [3].

Table 1. DDoS reflector source IP count

Protocol	2016 Q3	2016 Q4	2017 Q1	2017 Q2
SSDP	120800	508434	465979	426375
NTP	409646	299855	268338	267376
SENTINEL	34488	36119	50051	59270
CHARGEN	43304	47810	38848	39792
QOTD	27556	40474	30874	30026
RPC	36011	37657	31966	29858
TFTP	16313	22458	19670	18058

SSDP is part of the Universal Plug and Play (UPnP) Protocol standard. This protocol allows Internet devices to seamlessly discover each other's services. It

uses User Datagram Protocol (UDP) as the underlying transport protocol, which is based on HTTPU (HTTP UDP). Attackers have been abusing these protocols to initiate DRDoS attacks, amplifying and reflecting network traffic to their targets. Request packets from attackers are multicasting to service providers. SSDP uses 239.255.255.250 as its target IP address, which is a local multicast IP address. The request packets from SSDP clients to SSDP servers are transferred by multicasting to 239.255.255.250:1900 in local area network.

The United States Computer Emergency Readiness Team (US-CERT) first issued a warning about SSDP in January 2014 [26], and in October 2014 it was used to generate 54 Gbps of traffic in a single attack. PLXsert has observed the first use of the DRDoS attack that abuses SSDP [2]. The threats come from millions of networked devices which can be abused as reflectors by attackers.

For a regular SSDP service (shown in the left part of Fig. 1), a request sender will receive responses from service providers. But if an attacker want to conduct a SSDP reflection attack, he will first collect vulnerable hosts/devices on the Internet as bots to establish a botnet, the attack can control the request sender and spoof the IP address of requests packets using the victim's IP address as follows (shown in the right part of Fig. 1). A botnet known as a zombie army is a number of Internet computers that, although their owners are unaware of it, have been set up to send malicious packets to attack victims, which are servers or networks on the Internet. Second, the attacker will send both commands and vulnerable device lists to those bots in the botnet. According to the commands from the attacker, each bot sends a SSDP request with forged source IP address, which is the IP address of the target, to those vulnerable devices. The actual response receiver is not the requests sender, instead the victim become the receiver. Then massive responses from those vulnerable devices will bombard the server, which leads to a peak stage when massive packets are beyond the processing capabilities of the server. And in a SSDP reflection attack, the attack will exploit lots of request sender on the Internet as bots to establish a botnet, which is a challenge, especially for a large-scale botnet.

Work on defending SSDP reflection attacks. We found only some simple suggestions: UPnP requests should be blocked or UPnP service should be disabled to reduce SSDP reflection attacks is scarce. This limits the availability of regular UPnP services. On the other hand, we can get some ideas from some work on DDoS attacks. For example, Pack et al. [20] proposed to set parameters on servers and routers to disable services when there are attacks. Yan et al. proposed an algorithm that can use different time slice allocation strategies according to the intensity of DDoS attacks to ensure protection to a normal switch under DDoS attacks [29], which work on the victim side. Peng et al. presented an approach where reflectors monitor incoming packets and warn other potential reflectors when any abnormal traffic is observed [21]. This approach works on the service provider side. These works motivate us to think an integrated approach can be used at multiple locations to design a multi-location defence scheme (MLDS), which can work collaboratively at different locations. The majority of the exist-

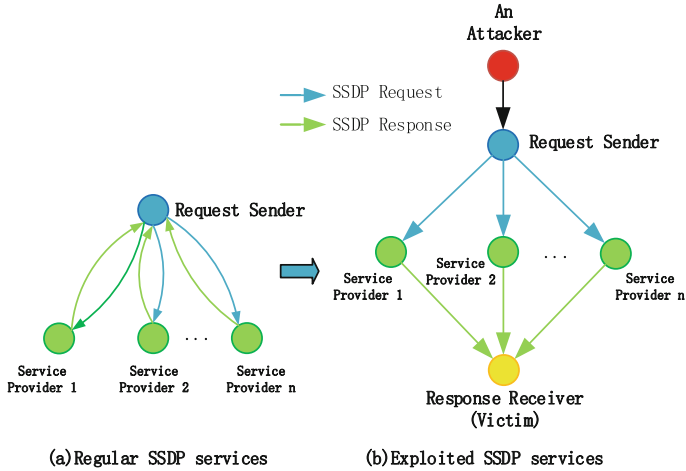


Fig. 1. Regular SSDP services (a) and exploited SSPD services with defending deployments (b)

ing defence mechanisms are designed based on the fact that attacks have to be detected. MLDS doesn't need to do this.

On the other hand, the existing defence schemes against DRDoS attacks do not consider deploying defence mechanisms to the source of attacks, because attackers are in control of the source of attacks. When we take a closer look at the SSDP reflection attacks, we can see that it is possible to deploy a defence mechanism to the source of the attack, and this will be much effective. To take the target out of service, an attacker usually utilizes a controller to instruct bots to launch an attack. The controller is under the control of the attacker for a SSDP reflection attack, but those bots exploited by the controller are not fully controlled by the attacker. This means regularly used service on those bots can be utilized to defend the victim. In MLDS, SSDP reflection attacks can be mitigated not only by reducing the amplification at reflectors and limiting the number of received response packets, but also by limiting requests at the source of attacks. We try to take full advantage of all possible resources throughout the attack link, especially the ones at the source of the attack.

The contributions of the paper include:

- We propose a comprehensive defence scheme called MLDS for SSDP reflection attacks. It has three main features:
 - MLDS working throughout the attacking link, starting from attack sources to victims
 - MLDS not depending on detecting attacks
 - MLDS is adopting an unconventional way of defence to make bots acting as defenders to carry out defence strategies, which makes MLDS very effective.

- According to the above characteristics, We thoroughly analyze traffic situations in the whole attack link when MLDS is deployed to different locations.

The remainder of the paper is as follows: Sect. 2 reviews related work on defence schemes. Section 3 presents the MLDS details, illustrates the DRDoS attack model in LANs, and then calculates the traffic for each attack location. Section 4 gives the conclusion and future work to be done.

2 Related Work

Work on defending SSDP reflection attacks is scarce. Pack et al. [20] just focused on setting parameters on servers and routers such as disabling underlying services. However, there are quite some works on defending against DDoS attacks [8, 19, 24], which can give us some hints. In this study we classify defending schemes for DDoS attacks into four categories according to the deployment location of the defending schemes.

A. Defending on routers

Ioannidis and Bellovin used Pushback added to upstream routers to drop attack packets with attack signatures that consist of selected prefixes of destination addresses [13]. If this method is used to resist SSDP attacks, dropping SSDP packets may affect normal services of UPnP.

Wang and Reiter proposed a distributed puzzle mechanism in which routers distribute puzzles to clients to require puzzle solutions to consume clients' resource, that is, clients as bots need more resources for attacks. Routers cooperate with each other to check network traffic and then defend networks against flooding attacks [27].

Pack et. al. used ACL (Access Control List) rules to distinguish attack packets from legitimate traffic based on source addresses in packets. These ACL rules were deployed on routers [20].

Dietzel et. al. proposed a blackholing technique that allows a peer via BGP (Border Gateway Protocol) to announce a prefix to another peer which then discards packets destined for this prefix among Internet Exchange Points to mitigate the effectiveness of DDoS attacks [7].

Mirkovic et al. proposed D-WARD which can gather two-way traffic statistics and detect attacks, and then adjust rate limit rules for suspected source addresses to modify associated traffic flows [18].

Chen and Park [6] proposed an Attack Diagnostic (AD) system in which DoS attacks are detected near the victim, and packet filtering is executed at the router close to the attacker. The victim can trace back attack traffic to attack sources and then issues messages that command AD-enabled routers to filter attack packets close to the source.

Huistra proposed that amplification attacks can be detected specifically by monitoring Domain Name System(DNS) packet sizes as well as the number of packets across multiple routers in which the victim and the source of the attack can be discerned [12].

Wei et al. proposed a method to locate suspicious flows on an upstream router then discard these flows on the routers [28].

B. Adding dedicated equipment

Kambourakis et al. deployed a monitor to record both DNS requests and responses using the IPtraf tool, which is a console-based network statistics utility for Linux. It collects a variety of statistics such as TCP connection packet and byte counts [15].

Kim et al. proposed PacketScore in which they prioritized packets based on a per-packet score to estimate the legitimacy of a packet given the attribute values it carries. They used a DDoS Control Server (DCS) to collect reports from routers across the Internet [16].

Saied et al. proposed a method to detect and mitigate known and unknown DDoS attacks in real time environment. They used artificial neural network (ANN) to detect DDoS attacks based on specific characteristic features (patterns) that separate DDoS attack traffic from genuine traffic [25].

Monowar et al. empirically evaluated several major information metrics such as namely, Hartley entropy, Shannon entropy, Renyi's entropy, to detect both low-rate and high-rate DDoS attacks. These metrics can be used to describe characteristics of network traffic data, and they proposed a model to detect both low-rate and high-rate DDoS attacks [5].

C. Defending at service providers

Peng et al. proposed that each potential reflector could be used to monitor incoming packets and broadcast warning messages to other potential reflectors if any abnormal traffic was detected [21].

Alqahtani et al. proposed a DDoS attack detection approach for service clouds and developed efficient algorithms to resolve the originating service for the attack. The detection approach is composed of four levels such that each level detects symptoms of DDoS attacks from its local data. The detection results of all levels are collaborated to confirm the victim and attacking services. They evaluated their proposed solution using a random dataset [4].

Uzair et al. have combined Ethereum with the traditional IoT to form a decentralized IoT infrastructure that not only prevents malicious devices from accessing servers, but also solves DDoS attacks by using static resource allocation of devices [14].

D. Defending at victims

Yan et al. proposed an effective software-defined networking controller scheduling method to mitigate DDoS attacks. The algorithm can adopt different time slice allocation strategies according to the intensity of DDoS attacks, and use SDN controllers to handle the traffic of different switches, so as to better protect the switches from DDoS attacks in the network [29].

Gilad et al. presented an approach using CDN (content distribution network) that adopts a CDN-on-Demand, software-based defence scheme for small

to medium websites to resist powerful DDoS attacks, at a fraction of the cost of commercial CDN services. When excessive load is detected, CDN-on-demand provides services to clients from proxies that are automatically deployed on various cloud service providers [10].

Attackers usually utilize a botnet to launch DRDoS attacks. From the survey, we haven't found other work that utilized bots in a botnet to defend against reflection denial-of-service attacks, as it is not a conventional approach to make the bots controlled by the controller in a botnet acting as a defender. Usually the user isn't aware that his computer is executing the controller's instruction as his computer still works well normally. Therefore, we have opportunities to utilize the communication function at bots, which is not restricted by the controller, so as to limit the number of requests sent to service providers. That is to say, we can add applications or set parameters on these bots to carry out our defence strategies. Additionally the majority of the existing defence mechanisms are designed based on the fact that attacks have to be detected. Our proposed scheme can be deployed directly to different locations without prior detecting the attacks.

3 Multi-location Defence Scheme

Intuitively, we can design an integrated defence mechanism, working throughout the attacking link, starting from the attack source to the victim. Deploying defence mechanisms to the source of attacks can make the defence very effective, because that is the place where attacks are launched. Additionally, we can make full use of limited resources in the attack sources in an unsafe environment to enhance the security of IoTs.

3.1 Deploying Defence Scheme at Multiple Locations

According to the process of a SSDP reflection attack discussed in introduction, to defend against SSDP reflection attacks, we deploy different defences schemes at multiple locations including the request sender, the service provider and the victim.

For a SSDP reflection attack, after request senders receive the instruction from the controller, they will send discovery packet requests to service providers using SSDP at an unusually high frequency, which is different from that of regular users. So it will be effective to deploy defence at request senders which are attack sources. We limit the number of requests at request senders when they are partially controlled by the controller in a preset time interval. In this way, the traffic from request senders to service providers and victims will be reduced.

After the SSDP requests are received, service providers will send their responses to the spoofed IP address, and the size of the response is many times that of the request. We set the time interval between the same two response packets to the same target at each reflector, which can limit the number of response packets sent from reflectors, and then reduce the reflectivity of service providers.

Another approach at reflectors is setting the Time-To-Live (TTL) value to a reasonable value to limit the distance the packets propagate on the Internet, which can ensure the remote responses can't reach the victim. UPnP enable seamless connection in a home network or a business network or between two home or small business networks thus allowing UPnP devices in a home or small business network discover and interact with UPnP device in another home or small business network using SSDP [9]. According to the scenarios where SSDP is applied TTLs can be set to suitable values to avoid the underlying responses reaching the victim.

When an attacker launches a SSDP reflection attack, the target of the attack is the response receiver. Therefore in our MLDS, the response receiver will drop the same packets from the same service providers with no side-effects to normal services. This can reduce the processing time of SSDP reflection attacks in MLDS.

In summary, if a node acts as a sender, or an amplifier, or a victim in different attacks at a SSDP node, we should deploy all those strategies before it joins the Internet. Each set of strategies at each kind of SSDP roles are designed as a plug-in, and these plug-ins are packaged as a MDLS package, which can be one type of software security packages downloaded easily on some official websites that issue security improvements.

To launch a massive SSDP reflection attacks, an attacker usually utilizes a lot of bots organized as a botnet. Figure 2 shows an SSDP reflection attack in LANs. If there are not enough vulnerable nodes to utilize for attackers, it is hard to organize effective attacks. There are several ways for SSDP nodes to install plug-ins, such as downloading MDLS from official websites as mentioned before or integrating MDLS into newly produced SSDP devices. Then there will have more SSDP nodes gradually which cannot be exploited by SSDP attackers. As the number of nodes equipped with MLDS increases, the number of vulnerable nodes which can be utilized by attacker will decrease. Therefore, the attackers are unable to implement an effective attack.

An attacker instructs a botnet composed by B_1, B_2, \dots, B_m to send spoofed requests simultaneously to those service providers A_1, A_2, \dots, A_k via a controller (C). Those service providers send amplified responses to the same target, leading to a dramatic increase of traffic flow. The analysis of traffic flow is detailed as follows.

- First, the attacker uses a controller (C) to instruct a botnet and command bots to send requests to service providers in an infinite loop until the victim is down.
- Next, those bots send spoofed requests simultaneously to those service providers A_1, A_2, \dots, A_k . We assume that the size of a request is t_1 and the controller commands the bots request in an infinite loop. So we can calculate the traffic from a bot TR_{fromB} using (1).

$$TR_{fromB} = n * t_1 \tag{1}$$

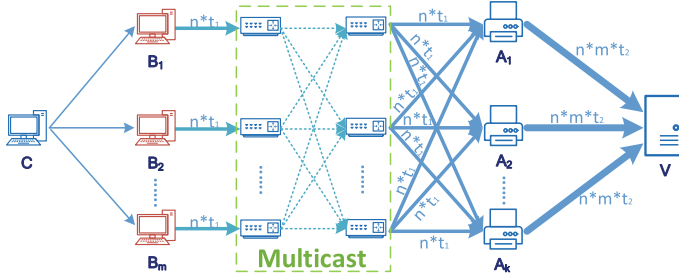


Fig. 2. Traffic flow during a SSDP reflection attack in LANs

Where n is the number of request cycles. Those bots will send spoofed requests by using multicast addresses in LANs, and then these request packets are distributed through routers to the target victim. According to a vulnerable device list the requests will be sent to multiple service providers by n times.

- Those service providers then send amplified responses to the same target, the victim (V). We set the size of the response to t_2 . Every service provider receives n requests from every bot. And there will be m bots sending amplified packets to the victim simultaneously. We can calculate the traffic from a service provider to the victim TR_{fromA} as (2).

$$TR_{fromA_i} = n * m * t_2 \tag{2}$$

The total traffic T_v for a SSDP reflection attack can be calculated as (3).

$$T_v = k * n * m * t_2 \tag{3}$$

where k is the number of the service providers.

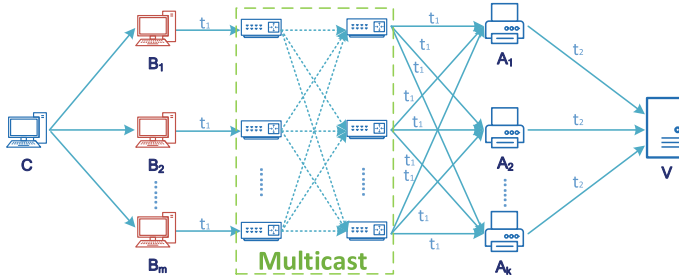


Fig. 3. The restrained attack traffic by the MLDS in LANs

From the above analysis, deploying different defence strategies to multiple locations will make the defence work efficiently in the whole attack link, from

the attack initiating source to the victim. This is the reason why we design the MLDS.

For request senders, there is no retransmission mechanism in SSDP protocol. We can limit that each bot sends a SSDP request only once within a time interval to avoid malicious requests being sent repeatedly, in order to reduce response packets.

For service providers, the number of response packets to the same target can be limited. We count the requests received from different senders with the same source IP address. The response to the target is allowed only once within a time interval.

For victims, if the same packets arrive to the same response receivers, the following packets should be discarded.

The MLDS works as follows (Fig. 3):

- MLDS at the requests sender will limit the number of requests from B_1, B_2, \dots, B_m . We add a counter to count the same requests at B_1, B_2, \dots, B_m if the port is the 1900 and the packet sent is the same as SSDP discover request. We also add a timer to record the time starting from the time when the value of the counter is 1. The initial value of the counter is set to 0. Before a bot send a request it should check the counter. If the value of the counter is 1, the request should be stopped. Otherwise the request is sent regularly. After a request is sent the counter is set to 1. When the time interval is running out, its value is set to 0.

That is, the network traffic can be restricted at the request senders. If each bot can limit their numbers to 1, each service provider will receive m requests from m bots. We can calculate the traffic from request senders to each service provider T'_{toa} as (4).

$$T'_{toa} = m * t_1 \quad (4)$$

- After a request is received, A_1, A_2, \dots, A_k can limit the number of its responses to V using the following method. We add a timer to record the time between two consecutive response packets. We set the interval threshold time between two packets. If the time is shorter than the interval threshold, the reflectors should stop the next response packets to the same target in this time interval. At the same time before an IP packet is sent, the value of TTL should be set according to the distance (how many hops) from the request sender to the service provider and the distance from the service provider to the victim. After each service provider limits their responses to V in an interval to only once, the corresponding load received at the victim from k service providers T'_v can be calculated as (5).

$$T'_v = k * t_2 \quad (5)$$

We can see that the traffic T'_v is reduced dramatically comparing with T_v .

- At the victim, We add a counter to count the same responses from the same service provider. If the value of the counter is 1, the following packets within the time interval should be discarded. If some service providers don't limit the number of responses, the victim will ensure the traffic T'_v is $k * t_2$.

4 Conclusion

The proliferation of IoTs is confronted with increasing SSDP reflection attacks. However, there are very scarce studies on a comprehensive solution for defending SSDP reflection attacks. Only some advices on disabling UPnP services exist. The work on DDoS attacks proposed some defence schemes here and there in the attack link, without considering tackling the attacks from the source end. In this paper, we propose an integrated approach called MLDS, where a multi-location defence scheme is designed and deployed to different places in the whole attack link, which can work collaboratively at different locations. MLDS does not depend on detecting attacks like other existing approaches, and resolves the defence problem from the key part by deploying defence strategies to attack sources, service providers, victims, etc. We try to make full use of all possible resources in the whole attack link, especially the resources at the source of attacks. The article show that tackling security attacks from the very beginning of attacking sources is the most effective approach, and also the integrated defence scheme in the whole attack link is a comprehensive solution which can be a reference for resolving other security attacks.

Acknowledgements. This work is supported by the Key Research Program of Shandong Province (No. 2017GGX10140), the Fundamental Research Funds for the Central Universities (19CX05027B, 19CX05003A-11) and the National Natural Science Foundation of China (61702399, 61772291, 61972215).

References

1. Distributed Reflection Denial of Service Attacks. Accessed April
2. Akamai: SSDP REFLECTION DDOS ATTACK, akamais [state of the internet]/Threat Advisor
3. Akamai: State of the internet security 4(2) (2017)
4. Alqahtani, S., Gamble, R.F.: DDoS attacks in service clouds. In: 2015 48th Hawaii International Conference on System Sciences, vol. 1, pp. 5331–5340, January 2015. <https://doi.org/10.1109/HICSS.2015.627>
5. Bhuyan, M.H., Bhattacharyya, D., Kalita, J.: An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recogn. Lett.* **51**, 1–7 (2015)
6. Chen, R., Park, J.M.: Attack diagnosis: throttling distributed denial-of-service attacks close to the attack sources. In: 14th International Conference on Computer Communications and Networks, pp. 275–280. IEEE (2015)
7. Dietzel, C., Feldmann, A., King, T.: Blackholing at IXPs: on the effectiveness of DDoS mitigation in the wild. In: Karagiannis, T., Dimitropoulos, X. (eds.) PAM 2016. LNCS, vol. 9631, pp. 319–332. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-30505-9_24
8. Douligeris, C., Mitrokotsa, A.: DDoS attacks and defense mechanisms: classification and state-of-the-art. *Comput. Netw.* **44**, 643–666 (2004)
9. UPnP Forum FROUM: UPnP remote access-connecting two home or small business networks, June 2012

10. Gilad, Y., Goberman, M., Herzberg, A., Sudkovitch, M.: CDN-on-demand: an affordable DDoS defense via untrusted clouds. In: Network and Distributed System Security Symposium (2016)
11. Handley, M., Rescorla, E., IAB: Internet denial-of-service considerations. RFC 4732, RFC Editor, January 2006. <http://www.ietf.org/rfc/rfc4732.txt>
12. Huistra, D.: Detecting reflection attacks in DNS flows. In: 19th Twente Student Conference on IT, February 2013
13. Ioannidis, J., Bellovin, S.M.: Implementing pushback: router based defense against DDoS attacks. In: Proceedings of Network and Distributed System Security Symposium (NDSS) (2002)
14. Javaid, U., Siang, A.K., Aman, M.N., Sikdar, B.: Mitigating IoT device based DDoS attacks using blockchain. In: Conference Paper, June 2018
15. Kambourakis, G., Moschos, T., Geneiatakis, D., Gritzalis, S.: Detecting DNS amplification attacks. In: Lopez, J., Hämmerli, B.M. (eds.) CRITIS 2007. LNCS, vol. 5141, pp. 185–196. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89173-4_16
16. Kim, Y., Lau, W.C., Chuah, M.C., Chao, H.J.: PacketScore: a statistics-based packet filtering scheme against distributed denial-of-service attacks. *IEEE Trans. Dependable Secure Comput.* **3**(2), 141–155 (2006)
17. Lab, K.: DENIAL OF SERVICE: how businesses evaluate the threat of DDoS attacks IT security risks special report series (2014)
18. Mirkovi, J., Prier, G., Reiher, P.: Source-end DDoS defense. In: Second IEEE International Symposium on Network Computing and Applications, pp. 171–178. NCA, IEEE (2003)
19. Mirkovic, J., Reiher, P.: A taxonomy of DDoS attack and ddos defense mechanisms. *Newsl. ACM SIGCOMM Comput. Commun. Rev.* **34**, 39–53 (2004)
20. Pack, G., Yoon, J., Collins, E., Estan, C.: On filtering of DDoS attacks based on source address prefixes. In: Securecomm and Workshops, September 2006
21. Peng, T., Leckie, C., Ramamohanarao, K.: Detecting reflector attacks by sharing beliefs. In: Global Telecommunications Conference, pp. 1358–1362 (2003)
22. Reading, D.: Report: IoT connected devices leading to rise in SSDP based reflection attacks. Accessed 21 Apr 2015
23. Rossow, C.: Amplification hell: revisiting network protocols for DDoS abuse. In: Proceedings of NDSS. Internet Society (2014)
24. Ryba, F.J., Orlinski, M., Wahlisch, M., Rossow, C., Schmidt, T.C.: Amplification and DRDoS attack defense - a survey and new perspectives. arXiv preprint (2015)
25. Saied, A., Overill, R.E., Radzik, T.: Detection of known and unknown DDoS attacks using artificial neural networks. *Neurocomputing* **172**, 385–393 (2016)
26. US-CERT: UDP-based amplification attacks (2014)
27. Wang, X., Reiter, M.K.: Mitigating bandwidth-exhaustion attacks using congestion puzzles. In: 11th ACM Conference on Computer and Communications Security, pp. 257–267 (2004)
28. Wei, W., Chen, F., Xia, Y., Jin, G.: A rank correlation based detection against distributed reflection DoS attacks. *Commun. Lett.* **17**(1), 173–175 (2013)
29. Yan, Q., Gong, Q., Yu, F.: Effective software-defined networking controller scheduling method to mitigate DDoS attacks. *Electron. Lett.* **53**(7), 469–471 (2017)



Remote Data Authentication Scheme Based Balance Binary Sort Merkle Hash Tree

Mengyu Shen, Meiliang Liu, Yang Li, Delgerbat Batbayar,
and Xuanxia Yao^(✉)

University of Science and Technology Beijing, Beijing 100083, China
yaouxuanxia@163.com

Abstract. Now cloud storage has become the preferred way for users to store large amounts of data. In order to verify the integrity of remote data, Merkle hash tree is often used to generate data fingerprints. Aiming at the shortcomings of existing common schemes for remote data authentication based on Merkle hash tree, in this paper, based on data block index number constructs the balance binary sort Merkle hash tree, and using two-layer data nodes to shorten the authentication path. At the same time, by introducing “virtual nodes” to maintain binary sort Merkle tree balance and simplify insertion; In addition, considering the requirements of sensitive information confidentiality, by group hash for sensitive information and non-sensitive information to ensure that sensitive information is not leaked in the verification process. Theoretical analysis shows that the authentication structure can fulfill the function of data integrity audit well, and support the dynamic operation of data blocks while maintaining the balance of Merkle tree.

Keywords: Cloud storage · Integrity verification · Merkle hash tree · Data fingerprint

1 Introduction

Cloud storage is a remote data backup, preserve, and management service. In cloud storage mode, users can manage data across sites and add or remove existing nodes without downloading data. At the same time, users can access data on different internet devices. Especially for enterprises, it is more convenient and secure to store data on cloud servers than store on local. When using cloud storage, data is stored encrypted [1] in the cloud, and unauthorized users cannot access data files.

While we are enjoying the convenience brought by cloud storage technology, the security and privacy of cloud storage are also widely concerned. Because user loses the control over the data stored in the cloud, the cloud storage server becomes unreliable and may corrupt or tamper with the stored data. This requires the cloud storage system to provide the integrity certificate to verify the integrity of remote data. To solve this problem, a lot of research work has been done in academia. This paper analyzes the current research results and proposes a scheme for remote data integrity verification based on balance binary sort tree Merkle hash tree constructed based on data block

index number. This scheme supports dynamic operation and simplifies part of insert operation while completing remote data integrity verification.

The rest of the paper is organized as following. The second section introduces the related work. The third section introduces the system model used for integrity verification. The fourth section gives a detail introduction for our proposed scheme. The fifth section has carried on the theory analysis to the proposed scheme. The sixth section draws the conclusion.

2 Related Work

Existing remote data integrity validation models are divided into two types according to whether or not fault tolerant processing is applied to data files, one is based on *Juels et al.* [5] give proof of data recoverability POR (Proofs Of Retrievability) scheme, and the other is a *Ateniese et al.* [4] give data hold model prove that the PDP (Provable Data Possession) scheme. The POR scheme can not only identify whether the data is corrupted, but also recover the corrupted data. POR scheme requires data blocks to be stored locally, and a large amount of computation is required to verify data locally, which will increase the bandwidth consumption of users, and the scheme does not support dynamic operation. The PDP scheme does not support the recovery of corrupted data, but it does allow a holding certificate to be generated for data block that needs to be verified to complete the remote data authentication. PDP scheme is mainly used to detect the integrity of big data files, so PDP scheme is mostly used in data integrity verification. Some authentication schemes based on Merkle hash tree under PDP scheme are discussed below.

Ateniese et al. [4] made some modifications to the PDP scheme to support dynamic operations, enabling it to support partial dynamic operation (DPDP) [11]. However, this scheme does not support the data insert. In addition, an alternative solution is used when performing the delete operation, resulting in a certain amount of storage space wasted. To support the insertion operation, the DPDP-I proposed by *Erway et al.* [7] uses an authenticated jump table based on the Merkle hash tree to verify data integrity. However, the solution does not construct a distributed Merkle hash tree, and the authentication path is too long. Each verification requires a large amount of auxiliary information support, and the calculation cost and communication overhead are large. Later, *Erway et al.* [7] constructed a DPDP mechanism (DPDP-II) using the RSA tree [4], which improved the detection probability of data integrity, but also increased the computational overhead of the cloud server. *Wang et al.* [8] proposed another PDP scheme that supports full-motion operation of data insertion. This scheme confirms the location of the data block through the Merkle authentication hash tree, and ensures the data block through the PDP scheme of the BLS signature [9]. The integrity of the content. However, most of the current PDP scheme using BLS signatures will expose the risk of revealing user data privacy when using public authentication. To solve this problem, *Wang et al.* [13] protect privacy by attaching a random number to the evidence, making it impossible for third-party auditors to know the data content and support batch audits of multiple users. However, due to the large number of data tags, their audit protocols can cause significant storage overhead on the server. *Li et al.* [14]

proposed a multi-branch path tree structure LBT based on Wang, but the shortcoming of this scheme is that in the process of generating evidence by CSP (cloud service provider), more auxiliary information needs to be generated. Complete verification. Later, Zhang et al. [16] proposed a Balanced Update Tree (UT). Each node in the UT stores a certain number of consecutive data block label sets, but the cloud storage will contain the returnable hold able certificate. All the data block tags stored by the node increase the communication overhead.

The above research results increase the reliability of remote data in some extent, and can complete the data integrity verification. However, there is a large storage or communication overhead, and none processing the sensitive data in these files. In order to solve this problem, based on the data block index to construct the balance binary sort Merkle hash tree (BSMHT), by using the two-layer data node, improve the utilization rate of the node, and combine with the position map table of PMT (Position Map Table) to complete dynamic operations, by using “nodes”, convenient in parts of the insert and delete nodes; Grouping hash the sensitive and non-sensitive information in the file improves the security of sensitive information. Theoretical analysis shows that the balanced binary sort Merkle hash tree improves the audit efficiency and saves some storage space.

3 System Model

In this paper, the authorization verification model used to do integrity verification is shown in Fig. 1. The system model consists of three parties: User, Cloud Storage Provider (CSP), and third party audit institution (TPA). The user is the data owner who owns a large amount of data and wants to store the data remotely according to their own requirements. Cloud storage providers provide users with cloud storage servers, which have huge storage spaces and can manage and operate the stored data according to the users’ requirements. Users can access or dynamically operation the required data from any device. The TPA is the third-party auditor (Third Party Auditor, TPA) that has been introduced with a certain amount of auditing knowledge to audit the remote data for users and send the final audit results to them. Third-party audits are not necessarily credible.



Fig. 1. Cloud storage model

Because the cloud server may be insecure and untrustworthy, the data stored in it may be damaged, such as the loss of remote data may be caused by the hardware problem of the cloud server or the attack of malicious users, and some remote data may be deleted by the cloud service provider without authorization. Therefore, in order to ensure the integrity of the data stored in the cloud, users need to check the remote data periodically. If a user performs the integrity verification work locally, it will require a lot of computational work and consumes a lot of resources, so it is a common practice to delegate the audit to TPA, a third party auditor.

Based on this model, TPA is always assumed to be honest during the verification, and the authentication structure is based on the balance binary sorted Merkle hash tree (BSMHT).

The symbolic abbreviations used in this section are shown in Table 1, it also included the symbolic abbreviations which to be used later.

Table 1. The symbolic abbreviations table

Symbolic abbreviations	Implication
CSP	Cloud Storage Provider
TPA	Third Party Auditor
MHT	Merkle Hash Tree
BSMHT	Balance Binary Sort Merkle Hash Tree
BBST	Basic Binary Sort Tree
SensiRoot	The Root Hash of Sensitive Information
PMT	Position Map Table
Aux	Auxiliary Certification Information
Seq	The Physical Sequence Number of Data Block in File
V	The Version of Data Block

4 Remote Data Integrity Verification Based on BSMHT

To lower the storage and communication costs and preserve the privacy of the sensitive information in file stored in cloud, a remote data integrity verification scheme based on the balance binary sort Merkle hash tree (BSMHT) is proposed. The scheme consists of the BSMHT construction, the position mapping table creation, dynamic operations on data and integrity verification four parts.

4.1 The BSMHT Construction

The BSMHT can be constructed by 3 steps.

Step 1, the sensitive information of the file is teared off.

Step 2, the sensitive and non-sensitive data blocks are hashed respectively. In order to protect sensitive information, the sensitive information itself does not participate in search verification, and only the owner of the sensitive information is visible to the sensitive information hash process, and non-relevant people is invisible.

By accumulating hash for the sensitive data blocks, it will generate a digest named SensiRoot. SensiRoot is considered as a data node with index number is 1 in BSMHT.

For non-sensitive information, using the basic idea of binary Merkle hash tree to accumulate hash. Non-sensitive data blocks form data nodes through one-way hash calculation, and the index number of each data node is numbered sequentially from 2. Every three data nodes as a group to constitute a Basic Binary Sort Tree (BBST), and the root data node of BBST corresponds to the data block with middle value of the index number. If there are less than three remaining data nodes, generating corresponding number of “virtual nodes” to form a BBST.

Step 3, BSMHT is constructed by accumulate hash of the second layer data nodes in BBST. The completed initialization BSMHT authentication structure is shown in Fig. 2.

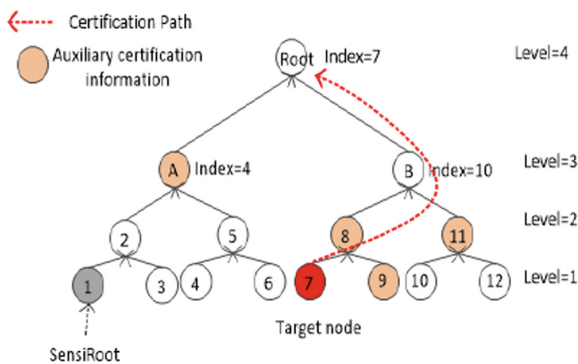


Fig. 2. BSMHT authentication structure

The structure of the data node is defined as $DataNodeStruct = (index, level, hash, calchash, LR)$.

Index is the data node index number, represents the location where the data node was inserted in BSMHT. Data nodes are numbered sequentially from 1. The index number of the BSMHT root node is equal to the minimum value of its right sub-trees index number, and the index number of the left and right sub-tree of the root node is equal to the minimum value of its right sub-tree. $rChild\{index_i\}$ represent data node index numbers collection that the right sub-tree.

$$index = \begin{cases} index, & level = 1 \text{ or, } level = 2 \\ \min(rChild\{index_i\}), & level \geq 3 \end{cases} \quad (1)$$

level represents the height of each node in BSMHT, counting from leaf node to root node from 1, increasing by 1 for each layer up. When the height is equal to 2, this node is a non-leaf node, and a data block will be stored at the same time. When the height is greater than or equal to 3, the node is a non-leaf node and does not store data blocks, is

a non-data node, the hash value is null, and the value of *calchash* is obtained through hash calculation after the hash value of the left and right child nodes is linked.

calchash represents the computed hash value of a non-leaf node.

$$calchash = \begin{cases} hash(data_i || hash_{lchild} || hash_{rchild}), level = 2 \\ hash(hash_{lchild} || hash_{rchild}), level \geq 3 \end{cases} \quad (2)$$

LR is used to indicate whether this node is the left child or the right child of the parent node. When $LR = 0$, it means that this node is the left child. When $LR = 1$, it means that the node is the right child; When $LR = -1$, the node is the root.

Definition 1. *Authentication Path:* The path defined in this scheme refers to the set of all parent nodes on the path of the i^{th} data node from bottom to root, starting from the user request verify node to the root node path of BSMHT, which is called the authentication path. The number of nodes contained in the authentication path set is the authentication path length d .

Definition 2. *Auxiliary Certification Information:* The set of all sibling nodes in the authentication path is called the auxiliary authentication information, let it named *Aux*. If the data node is a leaf node, the auxiliary authentication information needs to add its parent node.

Definition 3. *Basic Binary Sort Tree:* Every three data nodes as a group to constitute a Basic Binary Sort Tree (BBST), and the root data node of BBST corresponds to the data block with middle value of the index number.

Definition 4. *Real Node:* The node in the BSMHT where locate the data node and store the data block.

Definition 5. *Virtual Node:* The node in the BSMHT where locate the data node and non-store the data block.

4.2 Position Map Table (PMT)

The position map table (PMT) is a dynamic array structure with three dimensions, the first column is the index number (Index), the second column is physical sequence number (Seq), and the third column is data node version number (V). The relationship between Index and Seq is a mapping from the location of the data node in BSMHT to the physical sequence number of the actual location in the file. The initial value of version V is 0, and it will be added 1 for each modification of the data block. If the data block is deleted, its V will be directly set to -1 , and the Index of the deleted data block remains unchanged, while Seq is set to be an empty position, so the corresponding node in BSMHT becomes a “virtual node”. In a summary, version V has two functions: one is to record the operation times of a data block, and the other is to identify the corresponding index number in the BSMHT. If $V \geq 0$, the node is a “real node”, and if $V = -1$, the node is a “virtual node”.

There are three types of operations on PMT, include modify, delete, and insert. For example, BSMHT is shown in Fig. 2. If the data node of $Index = 12$ is a “virtual

node”, the initial PMT is shown in Fig. 3. If a data block is modified, its version is $V = V + 1$, and the corresponding data node’s hash value in BSMHT is updated at the same time, as shown in Fig. 4. If a new data block is inserted after a data block, its Index is added by 1 in order. The physical sequence number Seq is the actual position in the inserted file. Meanwhile, PMT table is updated, as shown Fig. 5. Delete a certain data block and directly set $V = -1$, as shown Fig. 6.

Index	Seq	V
1	1	0
2	2	0
3	3	0
4	4	0
5	5	0
6	6	0
7	7	0
8	8	0
9	9	0
10	10	0
11	11	0
12	0	-1

Fig. 3. Initial

Index	Seq	V
1	1	0
2	2	0
3	3	0
4	4	0
5	5	1
6	6	0
7	7	0
8	8	0
9	9	0
10	10	0
11	11	0
12	0	-1

Fig. 4. Modify

Index	Seq	V
1	1	0
2	2	0
3	3	0
4	4	0
5	5	1
12	6	0
13	7	0
6	8	0
7	9	0
8	10	0
9	11	0
10	12	0
11	13	0

Fig. 5. Insert

Index	Seq	V
1	1	0
2	2	0
3	3	0
4	4	0
5	5	1
12	6	0
13	7	0
6	0	-1
7	8	0
8	9	0
9	10	0
10	11	0
11	12	0

Fig. 6. Delete

The initialized BSMHT and PMT, together with the data blocks, are stored in the cloud.

4.3 Dynamic Operation

When performing any operation on a file, the PMT should be updated accordingly.

(1) *Modification*

According to the Seq of the data block to be modified, look up the index number of the data block in PMT table. And then, find the corresponding node in BSMHT according to the principle of the BSMHT. At last, update the corresponding fields of the node and all the hash value on the authentication path of the data node. At the same time, the version number of the data block in the PMT table will be added 1.

(2) *Deletion*

Similarly, the first thing needs to do find the index number of the data block to be deleted according to its Seq. And then, find the corresponding data node in BSMHT, set the hash value of the data node to be empty, and update all hash values on the authentication path of the data node. The Index of the data block in the PMT table remains unchanged, the Seq is set to be 0, which represents a null data block, and the version number is set to be -1 to indicate that it is a “virtual node”.

(3) *Insertion*

There are two cases for inserting a data block to a file (a data node to BSMHT).

Case 1: There is at least one “virtual node”. The data node insertion operation is simplified to be a modification operation. Firstly, find the Index of the “virtual node” in the PMT table. And then, replace the corresponding “virtual node” in the BSMHT, and to update all hash values on the authentication path of the data node. In the PMT table, the version number of the data block is set to be 0.

Case 2: No “virtual node”. It is necessary to add two new “virtual nodes” to form a basic binary sort tree with the data node to be inserted. If the index number of the node to be inserted node is n , the index numbers of the two new “virtual nodes” are $n + 1$ and $n + 2$. Algorithm 1 illustrates how to insert a node and adjust the BSMHT structure to be balance (Table 2).

Table 2. Insert BBST and adjust BSMHT algorithm.

Algorithm 1: insert BBST and adjust BSMHT algorithm

Step1: Generate two “virtual node”, and use the data node to be inserted and the two “virtual nodes” to form a basic binary sort tree BBST.

Step2: If the root index number of BBST is odd, go to step 3, otherwise, go to step 4. to find the insert position of BBST. If it is odd, do step 3. If even, do step 4;

Step3: Use the BBST to be inserted and the last BBST in BSMHT as children to generate a new non-data node N. Then go to step 5.

Step4: Use the BBST to be inserted and the parent node of last BBST in BSMHT as children to generate a new non-data node N.

Step5: If there are any nodes in the same layer as the non-data node N but not been accumulated, calculate the distances between N and each of these nodes, and generate the distance set, named set_1 .

Step6: If nodes in the next layer of non-data node N are not accumulated, calculate the distance between all nodes in the same layer as node N and each node in the next layer of N, and generate the distance set, named set_2 ; If the number of nodes in the next layer of non-data node N and without accumulate hash is more than 2, the node distance between each node in the next layer of N is calculated to produce another distance set, named set_3 ;

Step7: Take the minimum value of node distance set in set_1 , set_2 and set_3 . Then select the two nodes with the minimum node distance to generate new non-data node N'. Let N to be N'.

Step8: Repeat steps 5, 6, and 7 until BSHMT has only one root node.

4.4 Integrity Verification Process

In this paper, use data possession verification based BSMHT scheme to verify remote data integrity. When CSP is not trusted and user has no local backup, verify integrity of the data stored in cloud server. Remote data integrity verification process consists of preparation phase, challenge response phase, audit phase, and update verify phase.

Suppose that the file F has been divided into sensitive and non-sensitive information parts, and these two parts are separated into independent data blocks. The sensitive data blocks are accumulated hash, to generate sensitive data digest named *SensiRoot*; For the non-sensitive data blocks, using one-way hash function to get the hash value. And for the file F , has $F = (m_1, m_2, \dots, m_y)$, and $m_1 = \text{SensiRoot}$. Take $m_j \in \mathbb{Z}_p$, p is a big prime number. The bilinear mapping is $e : G \times G \rightarrow G_T$ and hash function is $H : \{0, 1\}^* \rightarrow G$, g is a generator of G .

Preparation Phase: First, user uses sensitive data digest *SensiRoot* and non-sensitive data block hash values to construct BSMHT. The BSMHT's root node of is the data fingerprint of the entire file. Then, initial the PMT. Finally, user sends the BSM-HT, PMT, and data blocks to CSP, and delete the local store information at the same time. The detail process is as follows.

- (1) User uses asymmetric encryption algorithms to generate a pair of public and private key (sk, pk) , pick a random number $\mathbb{Z}_p \rightarrow a$, calculate $g^a \rightarrow v$. Let its private key is $sk = a$, and public key is $pk = v$.
- (2) For the given file $F = (m_1, m_2, \dots, m_y)$, and $m_1 = \text{SensiRoot}$. User pick a random element $u \leftarrow G$, and generate signature σ_j for each data block hash value, and $\sigma_j \leftarrow (H(m_j) \cdot u^{m_j})^a$, signature set represented is $\phi = \{\sigma_j\}$, $1 \leq j \leq y$.
- (3) For the file F , user constructs the basic binary tree (BBST) by using three data blocks, and uses BBST to construct the BSMHT. The root node of BSMHT is denoted as R , R is the data fingerprint of the whole file F ; Then initial PMT, get the physical location Seq and version number V of each data block, where $1 \leq Seq \leq y$. BSMHT data node stores the hash value $H(m_j)$ of data blocks, where $j = 1, 2, \dots, y$. User uses the private key sk to sign the root node R : $sig_{sk}(H(R)) \leftarrow (H(R))^a$.
- (4) User send the about information Eq. 3 to CSP, and delete the local information.

$$\{F, BSMHT, PMT, \phi, sig_{sk}(H(R))\} \quad (3)$$

Challenge-Response Phase: TPA initiates a challenge request to the CSP to verify data integrity. CSP receives the challenge, then generates and sends the evidence to TPA. The detail process is as follows.

- (1) According to physical location Seq , get the Index number and version number V of the challenge data blocks, and the Index number set of the challenge data blocks is $I = \{s_1, s_2, \dots, s_n\}$, $s_1 \leq i \leq s_n$, the version numbers set of the challenge data blocks is $B = \{b_1, b_2, \dots, b_n\}$, $b_1 \leq b \leq b_n$. And each $i \in I, b \in B$, TPA picks a random element $x_i \leftarrow \mathbb{Z}_p$. Define challenge information is Eq. 4, the i in challenge information represents the verified data blocks location in file F .

$$chal = chal\{(i, x_i, b)\}_{s_1 \leq i \leq s_n, b_1 \leq b \leq b_n} \quad (4)$$

- (2) TPA sends the challenge information Eq. 4 to CSP, and posts requests to verify data integrity.
- (3) According i find all the corresponding data blocks in the BSMHT, to form data block set μ , and data blocks aggregated signature is σ .

$$\mu = \sum_{i=s_1}^{s_n} x_i m_i b \in Zp, b_1 \leq b \leq b_n \quad (5)$$

$$\sigma = \prod_{i=s_1}^{s_n} \sigma_i^{x_i} \in G \quad (6)$$

- (4) CSP uses auxiliary certification information $\{Aux_i\}_{s_1 \leq i \leq s_n}$ to generate evidence pro , and responds the TPA's challenge.

$$pro = \left\{ \mu, \sigma, \{H(m_i), Aux_i\}_{s_1 \leq i \leq s_n}, sig(H(R)) \right\} \quad (7)$$

Audit Phase: TPA receives the evidence pro , which is CSP returned, verify pro , determine the file F of user stored in the CSP whether is complete. According to the received auxiliary information $\{H(m_i), Aux_i\}_{s_1 \leq i \leq s_n}$, TPA calculates BSMHT's root, and denoted as R. Then verify the Eq. 8 is true:

$$e(sig_{sk}(H(R)), g) = e(H(R), g^a) \quad (8)$$

If the Eq. 8 is not true, the verify fails, otherwise, verify that the following Eq. 9 is true:

$$e(\sigma, g) = e\left(\prod_{i=s_1}^{s_n} H(m_i)^{v_i}, u^a, v\right) \quad (9)$$

Update-Verify Phase: When user modify, delete, and insert data blocks in the file F, the data blocks version number V is added 1. After a dynamic update, CSP processes the user's update request, and sends new evidence to TPA. Then TPA on behalf of user, to completes the updated data blocks verify.

- (1) According to data block's physical sequence number in PMT, user updates the data blocks, and generates new information $(m_i^*, \sigma_i^*, B_i^*)$ of the updated data blocks, where B is version number of updated data block.
- (2) User sends the new update information to CSP. Then CSP uses the new update information to find the index number of the data blocks by searching in PMT, the index number is the data block location in BSMHT. CSP updates the data blocks version number in PMT. And CSP generates new evidence pro_{new} for the updated data blocks, and sends pro_{new} to TPA.

- (3) According to the evidence $\{H(m_i^*), Aux_i^*\}$ in pro_{new} , TPA calculates the new BSMHT's root, denote it as R_{new} , verify whether the Eq. 10 is true, if equal, the data blocks are successfully updated, and TPA sends result to the user. Otherwise, the data blocks are unsuccessfully updated.

$$e(\text{sig}_{sk}(H(R_{new})), g) = e(H(R_{new}), g^a) \quad (10)$$

5 Performance Analysis

5.1 Theoretical Analysis

In order to analyze the verification efficiency of BSMHT, it will be compared with the traditional MHT.

- (1) In traditional MHT, data nodes are only stored in leaf nodes, but BSMHT has two-layer data nodes. When the data block number is n , and each data block size is m , the traditional MHT's height is $\lfloor \log_2(n+1) \rfloor$, and the BSMHT's height is $\lfloor \log_2(\frac{2n}{3} + 1) \rfloor$. The BSMHT's storage space is reduced by $\frac{n}{3} * m$.
- (2) In traditional MHT, searches a data block by comparing hash value. But in the BSMHT searches a data block by the index number, the search process is the same as the binary search. When the number of need authenticated data blocks is equal, the traditional MHT's average authentication path length is $\lfloor \log_2(n+1) \rfloor$, but in the B-SMHT, because the second layer data node exists, $\frac{1}{3}n$ data nodes's authentication path length is $\lfloor \log_2(\frac{2n}{3} + 1) \rfloor - 1$, $\frac{2}{3}n$ data node's authentication path length is $\lfloor \log_2(\frac{2n}{3} + 1) \rfloor$. So the BSMHT's average authentication path length is $\lfloor \log_2(\frac{2n}{3} + 1) \rfloor - \frac{1}{3}$. The BSMHT's time complexity of finding a data node is reduced by $n \log_2\left(\frac{n}{2n+3} + 1\right) + \frac{n}{3}$.
- (3) When doing insert operation, MHT is not always balanced, but BSMHT has "virtual node", there are $\frac{2}{3}$ data blocks insert operation will be replace operation which only needs to update the hash value, and not require adjust tree structure. If the number of insert data nodes is p , the traditional MHT needs to perform p insert operations, but the BSMHT only needs to perform $\frac{p}{3}$ the insert operations.
- (4) The scheme uses BSMHT as the authentication structure and carries out authentication process based on PDP protocol. The comparison with other classical based on PDP protocols are as Table 3.

Table 3. Authentication feature compare based on PDP protocols

Protocol	Public verification	Privacy	Dynamic
[4]	NO	NO	NO
[11]	NO	NO	YES
[7]	NO	NO	YES
[8]	YES	NO	YES
[13]	YES	YES	YES
[9]	YES	NO	YES
This text	YES	YES	YES

5.2 Experimental Analysis

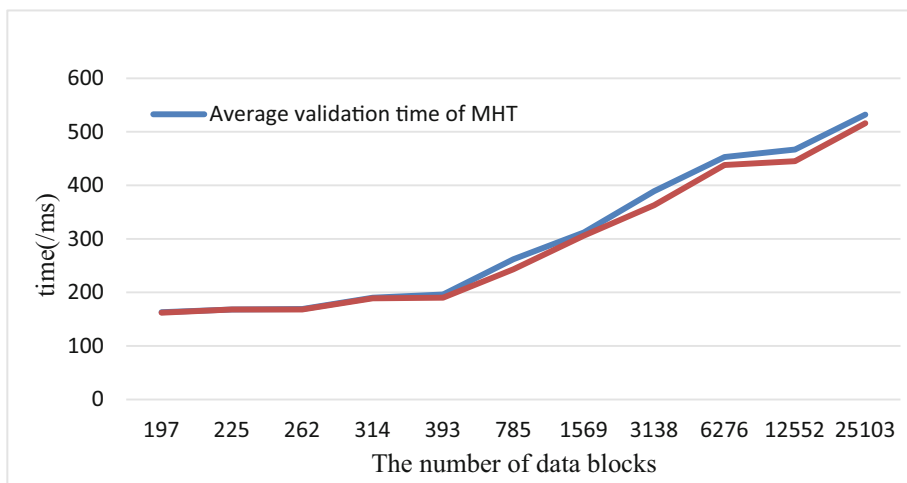
In order to verify the efficiency of use BSMHT to verify integrity in this chapter, the verification time is compared with that of the traditional Merkle hash tree. The experiment uses ECC asymmetric encryption to sign data blocks, and uses SHA-256 to accumulate hash to generate data fingerprint. And computer configuration is Inter-(R) Core(TM) i5-4200U CPU @ 1.6 GHz 2.30 GHz and RAM is 4 GB, Windows 10 operation system is 64bits. In the experiment all data blocks were verified. The verification program run time of 1000 times as an experiment. Run 10 times experiments and record the average.

Experiment: The effect of the number of data blocks on the integrity verification time. In this experiment we use the file of 3.06 GB, and perform respectively fixed-size partitions of 128 KB, 256 KB, 512 KB, 1 MB, 2 MB, 4 MB, 8 MB, 10 MB, 12 MB, 14 MB, 16 MB. The number of data blocks increases linearly with the size of the block. The experiment shows, regardless of the time required to sign the data block, as the number of data blocks increases, the time to validate all data blocks increases. In the case of a smaller number of data blocks, use MHT and BSMHT as authentication structures, the verification time of the two authentication structures can be considered almost the same.

But as the data blocks's number continues to grow, uses BSMHT as the authentication structures spent time has decreased compared with use the traditional Merkle hash tree. Because BSMHT adopts double-layer data node, in the case of larger number of data blocks, the height of authentication tree structure is effectively reduced, a third of the blocks of authentication paths are shortened. At the same time, due to the binary balanced tree structure, the search efficiency of the data block is also reduced. The experimental data are shown in Table 4, and the line diagram of the experimental results is shown in Fig. 7.

Table 4. Validation time required for different numbers of data blocks

The size of data blocks	The number of data blocks	Average validation time of MHT (/ms)	Average validation time of BSMHT (/ms)
16 MB	197	163	162
14 MB	225	168	168
12 MB	262	167	168
10 MB	314	190	189
8 MB	393	196	190
4 MB	785	262	243
2 MB	1569	312	306
1 MB	3138	389	363
512 KB	6276	453	438
256 KB	12552	467	445
128 KB	25103	532	516

**Fig. 7.** Validation time comparison

6 Conclusion

In this paper, first tear off sensitive information for a file, and then based on data block index to construct BSMHT, and generate data fingerprint. Meanwhile, by using PDP model, complete remote data integrity verification. Theoretical analysis shows that the remote data integrity verification scheme improves the verify efficiency in some extent, and reduces the tree structure adjusted times during a node inserted. In order to completely exclude the behavior of cheat user caused by TPA, block-chain will be introduced to store the data fingerprint instead of TPA. Based on the block-chain's characteristics of decentralization, tamper resistance and traceability, the integrity and

authenticity of data fingerprint will be guaranteed. At the same time, the verification process will be simplified. And it will ensure that the user has the right to independently complete the data verification.

References

1. Rafaeli, S., Hutchison, D.: A survey of key management for secure group communication. *ACM Comput. Surv.* **35**(3), 309–329 (2003)
2. Li, H., Sun, W.H., Li, F.H., Wang, B.: Secure and privacy-preserving data storage service in public cloud. *J. Comput. Res. Dev.* **51**(1), 1397–1409 (2014)
3. Xue, M., Xue, W., Shu, J.W., et al.: A secure storage system over cloud storage environment. *Chin. J. Comput.* **38**(5), 987–998 (2015)
4. Ateniese, G., Burns, R., Curtmola, R., et al.: Provable data possession at untrusted stores. In: *ACM Conference on Computer and Communications Security*, pp. 598–609. ACM (2007)
5. Juels, A., Kaliski, B.S.: PORs: proofs of retrievability for large files. In: *ACM Conference on Computer and Communications Security*, pp. 584–597. ACM (2007)
6. Cash, D., K upc u, A., Wichs, D.: Dynamic proofs of retrievability via oblivious RAM. In: Johansson, T., Nguyen, P.Q. (eds.) *EUROCRYPT 2013*. LNCS, vol. 7881, pp. 279–295. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_17
7. Erway, C., Kupccu, A., Papamathou, C., et al.: Dynamic provable data possession. In: *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS2009)*, Chicago, USA, pp. 213–222 (2009)
8. Wang, C., Wang, Q., Ren, K., Lou, W.: Ensuring data storage security in cloud computing. In: *Proceedings 17th International Workshop Quality of Service (IWQoS 2009)*, pp. 1–9, July 2009
9. Wang, Q., Wang, C., Li, J., Ren, K., Lou, W.: Enabling public verifiability and data dynamics for storage security in cloud computing. In: Backes, M., Ning, P. (eds.) *ESORICS 2009*. LNCS, vol. 5789, pp. 355–370. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04444-1_22
10. Zhou, E., et al.: An improved data integrity verification scheme in cloud storage system. *Acta Electronica Sinica* **42**, 150–154 (2014)
11. Ateniese, G., Di Pietro, R., Mancini, L., et al.: Scalable and efficient provable data possession. In: *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks*, Istanbul, Turkey, pp. 1–10 (2008)
12. Shacham, H., Waters, B.: Compact proofs of retrievability. *J. Cryptol.* **26**(3), 442–483 (2013)
13. Wang, C., Wang, Q., Ren, K., et al.: Privacy-preserving public auditing for data storage security in cloud computing. **62**(2), 525–533 (2010)
14. Li, Y., Yao, G., Lei, L., et al.: LBT-based cloud data integrity verification scheme. *J. Tsinghua Univ.* **65**, 504–510 (2016)
15. Mao, J., Zhang, Y., Li, P., et al.: A position-aware Merkle tree for dynamic cloud data integrity verification. *Soft. Comput.* **11**(8), 1–14 (2015)
16. Zhang, Y., Blanton, M.: Efficient dynamic provable possession of remote data via update trees. *ACM Trans. Storage (TOS)* **12**(2), 9 (2016)
17. Liu, C., Chen, J., Yang, L.T., et al.: Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates. *IEEE Trans. Parallel Distrib. Syst.* **25**(9), 2234–2244 (2014)

18. Ateniese, G., Burns, R., Curtmola, R., et al.: Remote data checking using provable data possession. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **14**(1), 1–34 (2011)
19. Zou, J., Sun, Y., Li, S.: Dynamic provable data possession based on ranked Merkle hash tree. In: *International Conference on Identification*. IEEE Computer Society (2016)
20. Ni, J., Yu, Y., Mu, Y., et al.: On the security of an efficient dynamic auditing protocol in cloud storage. *IEEE Trans. Parallel Distrib. Syst.* **25**(10), 2760–2761 (2014)
21. Wang, H.: Proxy provable data possession in public clouds. *IEEE Trans. Serv. Comput.* **6**(4), 551–559 (2013)
22. Su, D., Liu, Z.: New type of Merkle hash tree for integrity audit scheme in cloud storage. *Comput. Eng. Appl.* **54**(1), 70–76 (2018)
23. Liu, W.L., Li, H., Jin, D.X.: Research on digital fingerprinting generation scheme and key algorithm. *Netinfo Secur.* **2**, 66–70 (2015)
24. Haohua, M., Bo, C., Hui, Y., et al.: A Merkle-tree based cloud storage data hold check scheme. *Comput. Digit. Eng.* (2017)
25. Tan, S., Jia, Y., Han, W.: Research and development of provable data integrity in cloud storage. *Chin. J. Comput.* **38**(1), 164–177 (2015)
26. Li, H., Lu, R., Zhou, L., et al.: An efficient Merkle-tree-based authentication scheme for smart grid. *IEEE Syst. J.* **8**(2), 655–663 (2014)
27. Lang, W., Chen, K.: Research on the dynamic multi-copy provable data possession scheme based on map version table. *Netinfo Secur.* **1**, 18–23 (2016)
28. Fu, D.-L., Peng, X., Chen, G.-X., et al.: Remote attestation mechanism of platform configuration based on dynamic Huffman tree. *J. Comput. Appl.* **32**(8), 2275–2279 (2012)
29. Ji, R., Mu, N., Liao, X.: A novel privacy-preserving data integrity verification by partial delegation. In: *8th International Conference on Information Science and Technology*, 30 June–6 July 2018, Granada, Cordoba, and Seville, Spain (2018)
30. Atighehchi, K., Bonnezeze, A., Risterucci, G.: New models for efficient authenticated dictionaries. *Comput. Secur.* **1**(53), 203–214 (2015)



An Efficient Hybrid Encryption Scheme for Large Genomic Data Files

Yatong Jiang¹, Tao Shang¹(✉) , Jianwei Liu¹, Zongfu Cao²,
and Yunxiao Geng³

¹ School of Cyber Science and Technology, Beihang University, Beijing, China
shangtao@buaa.edu.cn

² National Research Institute for Health and Family Planning,
No. 12 Dahuisi Road, Beijing, China
caozongfu@nrifp.org.cn

³ Aviation Industry Development Research Center of China,
No. 14 Xiaoguangdongli Anwai, Chaoyang District, Beijing, China
yngeng@126.com

Abstract. With the rapid development of genomic sequencing technology, the cost of obtaining personal genomic data and analyzing it effectively has been gradually reduced. The analysis and utilization of genomic data have gradually come into the public view, the privacy leakage of genomic data has aroused the attention of researchers. Genomic data has unique format and a large amount of data, but the existing genetic privacy protection schemes often fail to consider security, availability and efficiency together. In this paper, we analyzed widely used genomic data file formats and designed a hybrid encryption scheme for large genomic data files. Firstly, we designed a key agreement protocol based on RSA asymmetric cryptography. Secondly, we used AES symmetric encryption to encrypt the genomic data by optimizing the packet processing of files and multithreading encryption, and improved the usability by assisting the computing platform with key management. Software implementation indicates that the scheme can be applied to the secure transmission of genomic data in the network environment and provide an efficient encryption method for the privacy protection of genomic data.

Keywords: Genomic data · Privacy protection · Key agreement protocol · Hybrid encryption

1 Introduction

With the development of big data era, biology information technology is developing rapidly, and the research, analysis and utilization of human genes are developing at an unprecedented speed. Genome is the carrier of biological genetic information, containing important genetic information of humanbeings. Genome

sequencing technology can analyze and calculate specific DNA (DeoxyriboNucleic Acid) sequences in the genome, laying a foundation for further research and utilization. GWAS (Genome-wide association study) provides more possibilities for the research of genomic data, and can help human beings know themselves better by exploring genes. However, GWAS is characterized by huge data volume and complicated and difficult data processing. It is a feasible method to send genomic data to big data platform for analysis and calculation. While big data provides support for bioinformatics research, it also hides unprecedented data security threats. The disclosure or improper use of genomic data will not only violate the personal privacy of data providers, but also cause national and social problems. Therefore, the privacy protection of genomic data is an important link in GWAS. Domestic and foreign researchers pay great attention to the security of genomic data. The privacy attack and protection methods of genomic data have gradually become the focus of research.

Researchers have found that publicly available genetic data can be traced back to the private information of a genetic data provider, and even the phenotype characteristics of the data provider can be recovered from the genotype characteristics. In 2008, Homer et al. [1] proposed that high-density SNP (Single Nucleotide Polymorphism) genotyping microarrays can accurately and reliably determine whether a particular individual exists in a given complex genomic DNA mixture. On this basis, Wang et al. [2] proposed two attack methods based on genome-wide association study of public data in 2009. The second is an integer programming attack, in which an allele pair at a given locus is known to restore all of an individual's SNPs. In 2013, Gymrek et al. [3] demonstrated that the family name can be recovered from an individual's genome by analyzing short tandem repeats on the Y chromosome and querying the genealogical database. The combination of last names and other types of metadata, such as age and state, can be used to triangulate the identity of a target. A key feature of the technology is that it relies entirely on free, publicly accessible Internet resources. In 2017, Lippert et al. [4] proposed a method for phenotype prediction that matches phenotype data with personal-level genotype data from whole-genome sequencing (WGS).

The privacy protection methods of genomic data can be divided into three categories, namely access control, data protection with distortion and data protection without distortion. Inaccurate privacy protection methods include data anonymity, differential privacy protection technology, etc. The undistorted privacy protection method is based on cryptography encryption algorithms, including symmetric and asymmetric key encryption schemes, homomorphic encryption and other encryption methods. Access control is an effective means to protect data security. Access rights can be distributed to users with different permissions through attributes or groups applied by users. It can also be used to protect the privacy of genomic data. However, in GWAS analysis, fine-grained partitioning will make access control complex, and large-data level access control will cause security problems due to coarse-grained user groups. Data anonymity includes the k -anonymity model proposed by Sweeney [5], the k -anonymity model

improved by Williams [6] and Samarati [7], the l -diversity model proposed by Machanavajjhala et al. [8], the t -closeness model proposed by Li et al. [9], and the DNALA method for identity tracking attacks. Differential privacy protection is mainly based on k -means method, which distorts data by adding noise. Johnson et al. [10] studied genomic data analysis based on differential privacy technology in GWAS. Encrypting genomic data and storing or uploading ciphertext to cloud computing platform is an important method to protect data without distortion. Ayday et al. [11] encrypted genome data based on homomorphic encryption and proxy reencryption and then uploaded it to the cloud platform. Cristofaro et al. [12] designed a method to protect genomic data privacy based on homomorphic encryption. Chen et al. [13] proposed a privacy protection scheme for sorting short gene data fragments in the cloud environment based on hash function. The existing genomic data privacy protection scheme has low efficiency and practicability.

In this paper, we propose an efficient and secure hybrid encryption scheme for genomic data files to achieve the privacy protection of genomic data.

2 Related Works

We analyzed genomic data file formats and studied cryptography for encryption.

2.1 Genomic Data Format Analysis

Genomic data is mainly used to record DNA, protein sequences, gene expression and other information, from which the biological information of different individuals can be analyzed and the genetic information database of organisms can be constructed. Genomic data format is more diverse, generally can be divided into the original genomic data files and processed files to record mutation information. Original genomic data files, such as Fast, Fastq and other formats, are unprocessed individual genomic data, containing all the DNA information of an individual, with large data volume and file volume, which is the general storage format of genomic data. The processed genomic data file, such as VCF (Variant Call Format), extracts the mutation site information from the original genomic data file for processing. The file in this format is small in size and does not have all the genotypes of individuals, and is only used for the analysis of mutation sites.

Fastq File Analysis. Fastq is a text-format file that stores biological sequences and their corresponding mass fractions, as well as identifier sequences associated with the DNA sequence, which is the standard format for high-throughput sequencing data. There are three types of sequences in this type of file: identifier sequence, DNA sequence and mass fraction sequence. The identifier sequence records the sequencing information, the DNA sequence represents the sequencing result, and the mass fraction sequence represents the estimation of the correctness of the base sequencing result. Every four lines the Fastq file describe a set of sequencing sequence information, and the recording example is shown in Fig. 1.

```
@SEQ_ID
GATTGGGGTTCAAAGCAGTATCGATCAAAATAGTAAATCCATTTGTTCAACTCACAGTTT
+
!' '*(((***+))%%%++) (%%%) . 1***-+*'') **55CCF>>>>>CCCCCCC65
```

Fig. 1. The example of Fastq file

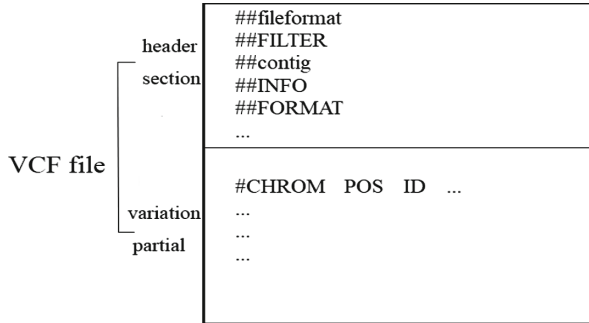


Fig. 2. Basic structure diagram of a VCF file

VCF File Analysis. VCF is a text file which is used to describe single nucleotide polymorphism (SNP), InDel, genomic structure variation (SV) and other variants. The VCF file uses utf-8 encoding and consists of two main parts: the title part and the variation record part. The header part is the annotation information beginning with “##”, while the variation record part is prefixed with “#” to record the specific mutation information on specific sites. The basic structure is shown in Fig. 2.

The fileformat line indicates which version of the VCF specification the file conforms to, the filter line displays the filter information applied to the data, the contig line contains the name, length, and some other information of the contig, the format line and info line explain the FORMAT and INFO column of variation record in the VCF file.

As shown in Fig. 3, for the records of each variable sites, the information is presented in a number of column structures. The first eight columns of the record represent the attributes observed at the variable sites. When the file contains multiple samples, the data represents the average of the data obtained from that site. Column 9 (format column), column 10 and beyond (sample column) contain specific information about the sample level.

2.2 RSA Asymmetric Encryption Algorithm

RSA algorithm is the most widely used asymmetric encryption algorithm at present. The security of RSA algorithm is based on the mathematical problem of large integer factoring. RSA algorithm is described as follows:

#CHROM	POS	ID	REF	ALT	QUAL	FILTER	INFO	FORMAT	HG01914	HG01985
1	10177	rs367896724	A	AC	100	PASS	AA= unknown(NO_COVERAGE);A			
1	10235	rs540431307	T	TA	100	PASS	AA= unknown(NO_COVERAGE);A			
1	10352	rs555500075	T	TA	100	PASS	AA= unknown(NO_COVERAGE);A			
1	10505	rs548419688	A	T	100	PASS	AA=. ;AC=1;AF=0.000199681;			
1	10506	rs568405545	C	G	100	PASS	AA=. ;AC=1;AF=0.000199681;			
1	10511	rs534229142	G	A	100	PASS	AA=. ;AC=1;AF=0.000199681;			
1	10539	rs537182016	C	A	100	PASS	AA=. ;AC=3;AF=0.000599042;			
1	10542	rs572818783	C	T	100	PASS	AA=. ;AC=1;AF=0.000199681;			
1	10579	rs538322974	C	A	100	PASS	AA=. ;AC=1;AF=0.000199681;			
1	10616	rs376342519	CCGCCGTTGCCAAAGGCCGCCCG	C	100	PASS	AC=5034;			
1	10642	rs558604819	G	A	100	PASS	AA=. ;AC=22;AF=0.00419329;			
1	11008	rs575272151	C	G	100	PASS	AA=. ;AC=445;AF=0.0880591;			
1	11012	rs544419019	C	G	100	PASS	AA=. ;AC=445;AF=0.0880591;			
1	11063	rs561109771	T	G	100	PASS	AA=. ;AC=15;AF=0.00299521;			
1	13011	rs574746232	T	G	100	PASS	AA=T ;AC=3;AF=0.000599042;			
1	13110	rs540538026	G	A	100	PASS	AA=g ;AC=136;AF=0.0267572;			

Fig. 3. Records of VCF variable sites

Key Generation. Select two secret large primes p and q , calculate the big integer $n = p \cdot q$, $\phi(n) = (p - 1)(q - 1)$, where $\phi(n)$ is the Euler function of n . Then, pick an integer e , satisfying $1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$. Calculate d , satisfying $d \cdot e \equiv 1 \pmod{\phi(n)}$, i.e., d is the multiplicative inverse element of e under modulo $\phi(n)$. Since e is coprime with n , it can be known from modular computation that its multiplicative inverse element must exist. Take $\{e, n\}$ as the public key and $\{d, n\}$ as the private key.

Encryption. Firstly, the plaintext bit string is grouped so that the decimal number corresponding to each group is less than n , i.e., the group length is less than $\log_2 n$. Then for each clear text group m , do the encryption operation:

$$c \equiv m^e \pmod{n} \tag{1}$$

Decryption. The decryption operation of the ciphertext packet is:

$$m \equiv c^d \pmod{n} \tag{2}$$

2.3 AES Symmetric Encryption Algorithm

AES is a block encryption algorithm with relatively high efficiency and security, which is one of the most popular symmetric encryption algorithms. Here we use the AES128 algorithm, which has a 128 bits key. In the algorithm, the packet length is fixed at 128 bits and the input packet is represented by a 44 matrix of 16 bytes (8 bits per byte). AES algorithm is implemented by multiple rounds of basic round transformation iteration, the number of rounds required increases with the selected key length. When the key length is 128 bits, the number of iteration rounds is 10.

Since the original key is usually short, if the algorithm needs to carry out multiple rounds of iteration, it is necessary to conduct key expansion operation on the initial seed key. Like the input grouping, the key is represented in a matrix of bytes, four bytes for each column of the matrix forming a word. After

key expansion, the key of 128 bits was eventually extended to a key sequence containing 44 words, in which each 4 words form a set of round keys, which were used in the initial and subsequent 10 rounds of iteration round key addition. While encryption, an initial round of key addition is required first, followed by 10 rounds of basic round transformation. Round transformation is expressed as: $Round(State, RoundKey)$. $State$ is the round message matrix, which can also be called the state matrix, $RoundKey$ is the round key matrix obtained through key expansion.

2.4 MD5 Hash Algorithm

Message Digest (MD) algorithms are a series of commonly used hash functions and MD5 is the fifth version. The MD algorithm takes the plaintext information of any length as input, and after 512 bits of packet filling and 4 rounds of logical operations, finally maps to a 128 bit numeric string as the message digest:

$$MD = H(m) \quad (3)$$

As a one-way hash function, MD5 has the characteristics of antigen image attack and anti-collision attack, which can be used to ensure the integrity of message transmission, and is an important message authentication tool. MD5 has the characteristics of compressibility and fast running speed, which is suitable for the efficient encryption requirements proposed in this paper.

3 Hybrid Encryption Scheme

We designed a scheme that encrypts the compressed genomic data to ensure the security of data in the transmission process and realize the privacy protection of genomic data. According to the binary characteristics of the encrypted genomic data and the demand for the encryption transmission efficiency, AES symmetric encryption system is used to encrypt the genomic data. In order to further improve the security of the transmission process, RSA asymmetric encryption algorithm is used to encrypt the AES key. Besides, we use MD5 hash function to guarantee integrity and correctness of the key. The scheme framework is shown in Fig. 4.¹

3.1 Key Agreement Protocol

In order to ensure the security of AES encryption key between two parties that trust each other, a key agreement protocol based on RSA asymmetric encryption was designed. Meanwhile, we also use MD5 one-way hash function to ensure the integrity of the key. The agreement is shown in Fig. 5.

¹Here K is the AES encryption key, K_p is the public key of RSA, K_s is the private key of RSA, m is the plaintext, $H(\bullet)$ represents the hash value.

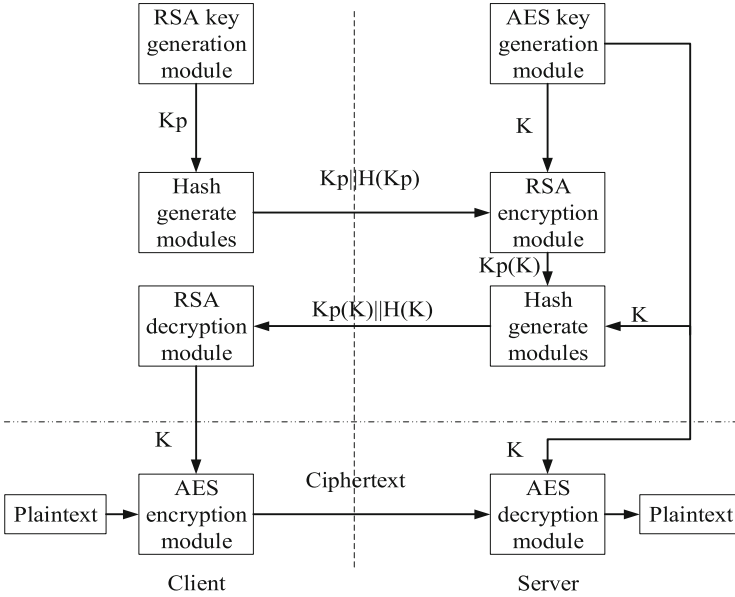


Fig. 4. Design of encryption scheme

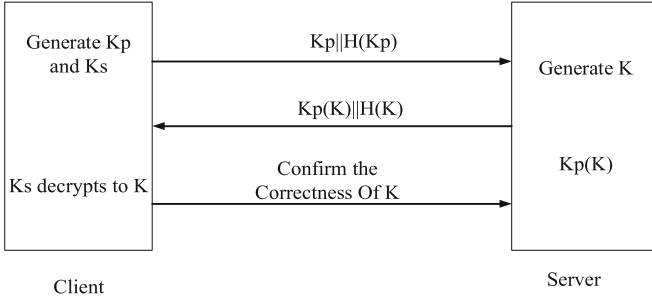


Fig. 5. Key agreement protocol

The protocol is described as follows:

Step 1: the client generates the RSA public key K_p and private key K_s sends the public keys K_p and user id id to the server.

Step 2: the server generates a AES encryption key K and a hash value $H(K)$ of the transmitted encryption key.

Step 3: the server encrypts K with the received public key K_p and sends $K_p(K) || H(K)$ to the client.

Step 4: after receiving the $K_p(K) || H(K)$ of the server, the client uses the private key K_s for decryption to get the value of K , and calculates whether $H(K)$ is consistent with the received hash value. If so, the key is transmitted correctly.

Based on BAN logic [14], we formally proved the protocol. Let A represent the client and B represent the server, then we formally describe the protocol as follows

$$A \rightarrow B : \{K_p, H(K_p), id\}$$

$$B \rightarrow A : \{\{K\}_{K_p}, H(K)\}$$

Initialization assumptions are as follows

$$B \vdash A, A \vdash B, B \mapsto K$$

$$A \mapsto K_p, A \mapsto K_p^{-1}$$

The objectives of the agreement are as follows

$$A \vdash B \xleftrightarrow{K} A$$

$$B \vdash A \xleftrightarrow{K} B$$

The proof is as follows

Proof.

$$\therefore B \vdash A \mid \sim K_p$$

$$\therefore B \vdash A \xleftrightarrow{K_p} B$$

$$\therefore A \vdash B \mid \sim \{K\}_{K_p}$$

$$\therefore A \vdash B \xleftrightarrow{\{K\}_{K_p}} B$$

$$\therefore A \mapsto K_p^{-1}$$

$$\therefore A \vdash B \xleftrightarrow{K} A$$

$$\therefore B \mapsto K \& B \vdash A$$

$$\therefore B \vdash A \xleftrightarrow{K} B$$

After the key agreement, both parties have a common encryption key K and can begin to encrypt the data file and then transmit the ciphertext. In order to ensure the security of genomic data, the key can be updated after a transmission.

3.2 AES Encryption

Data sent from a client to a server will go through compression module, encryption module and transmission module. At the client, Fastq files are compressed into GTZ files, and the binary files of GTZ are input into the encryption module. The encrypted binary files are obtained through key K encryption, and then output to data transmission. In the server, after receiving the encrypted binary file through network transmission, input it into the decryption module, decrypt it through the key K to get the GTZ file, and output it to the decompression module. After decompression with reference, get the original Fastq file, which can be used for subsequent data analysis. The encryption flowchart is shown in Fig. 6.

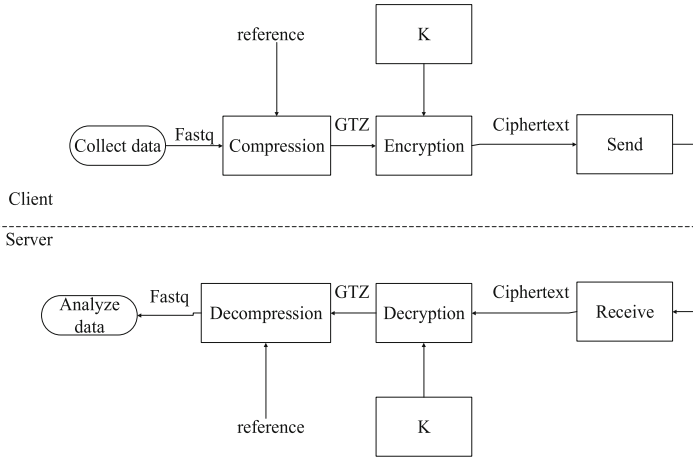


Fig. 6. AES encryption and decryption flowchart

Reading the Genomic Data Files. Considering the format of genomic data files, we read the files by converting them to bytes stream rather than reading in characters directly. Because genomic data files are large, typically 1–2 GB, reading the entire file into a byte stream takes up a lot of running memory. When reading the files into the AES module, we read the groups of 1 MB for reducing the memory usage.

Padding the Plaintext. AES is a block cipher system with block length of 128 bits (16 bytes). When we convert a genomic data file into a byte stream, the size of the input data is not necessarily multiple of the block length, so we need to pad in the last block length of the input text. When decrypting, remove the populating data at the end of the decrypted result according to the same pattern, and it can be successfully decrypted. Here we use the following padding methods.

During encryption, the length of clear text is denoted as len . If it is not an integer multiple of 16, the padding length is $16 - len \% 16$, where the last padding byte is used to record the padding length, and the other few bytes are padded with 0. If it is exactly an integer multiple of 16, the desired padding length is 16 and all bytes are padded with 0.

During decryption, the padding length is determined by the the last byte of the decrypted result, and then the corresponding byte is removed according to the padding length to ensure that the decryption result is completely consistent with the original data.

Key Management. In order to make our scheme more practical, we provide key management module. We add an input parameter in the client, provided by the client input user id id , and name the key file according to the id . The

encryption module needs to input the *id* parameter too, the encrypted file also named by the user id *id*. In this way, there is a direct correlation parameter between the key file and the encrypted file, and the user id can be used for key management on the computing platform. Key management can avoid the case that the key and the file to be decrypted cannot correspond, and ensure the one-to-one correspondence between the key and the encrypted file, so as to realize saving as the ciphertext and decrypting according to needs.

4 Implementation of Encryption Scheme

We have programmed the scheme and put forward some methods to optimize the encryption efficiency.

4.1 Development

The encryption scheme was developed under ubuntu16.04 by python3.7.

We developed a total of seven modules, i.e., AES key generation module `Keygen_AES.py`, AES encryption module `encrypt_aes.py`, AES decryption module `decrypt_aes.py`, RSA key generation and encryption module `Encrypt_RSA.py`, RSA decryption module `Decrypt_RSA.py`, MD5 hash value generation module `md5.py`, socket transport module `server.py` and `client.py`.

The development architecture is shown in Fig. 7.

Key Agreement Protocol. Call random module to generate 16-byte RSA public key and private key and 128-bit AES key, call hashlib module to calculate the hash value of the key, use Socket transmission module to establish TCP connection to achieve key agreement.

The process of establishing TCP connection with Socket module can be divided into three steps: server monitoring, client request and connection confirmation. The specific process is described as follows:

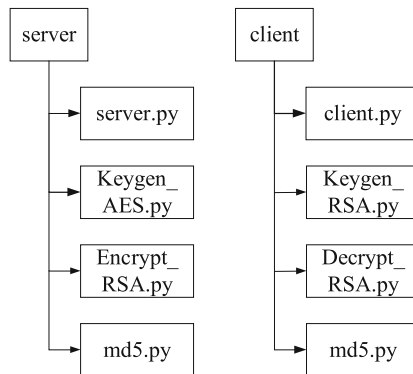


Fig. 7. Development architecture diagram

Server listening: the server first creates a socket, starts waiting for a connection, and call real time monitoring for connection requests from the client.

Client request: the client creates a socket and makes a connection request by sending a RSA public key K_p to the corresponding IP address and port of the server-side socket.

Connect confirm: the server-side socket detects a connection request sent by a client socket and creates a new thread that replies to the request and sends back the AES key encrypted by K_p as a response message. The client receives this description and confirms it, completing the connection.

The key agreement protocol is developed by encapsulating RSA encryption and decryption and MD5 hash generation in socket communication.

AES Encryption and Decryption Module. Using binascii module to convert the genomic data file into byte stream reading into the encryption module, which is grouped according to the size of 16bit, and read into the key file. Numpy module is called for encryption and decryption operation, and then the byte stream after encryption and decryption is written into the genomic data file again through decimal conversion. The encryption development process is shown in Fig. 8.

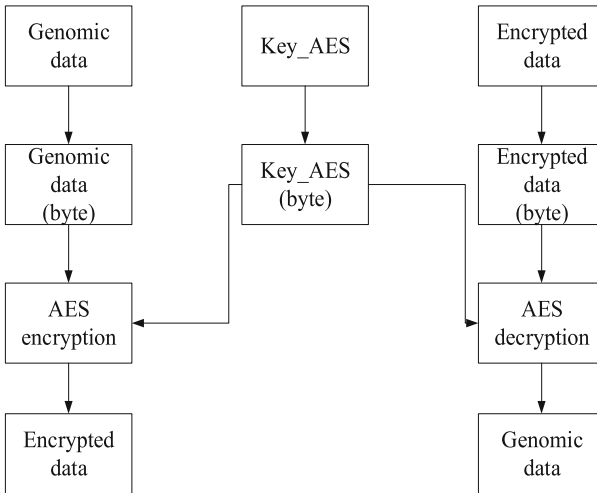


Fig. 8. Encryption development flowchart

To achieve AES encryption, we have to achieve round transformation. The round transformation (except the last one) consists of four different basic functions: SubBytes, ShiftRows, MixColumns, AddRoundKey. The four internal functions of the basic round transformation are developed as follows:

Step1: SubBytes is a constant matrix, which is mapped in the following way: extracting the high 4 bits and the low 4 bits as the row value and column value from the round message matrix, and the elements of corresponding row are found in the s-box as the output elements, and finally the substituted matrix is obtained.

Step2: ShiftRows is operated on each row of the round message matrix, which is essentially a substitution password: each row of the matrix is cyclically shifted by a certain length with a different amount of displacement, so that the positions of elements in each row are rearranged, while the elements themselves do not change. For row $i (i = 0, 1, 2, 3)$ in the round message matrix, each element loops $4 - i$ bytes to the right.

Step3: MixColumns operates on each row of the round message matrix, essentially a multiple table substitution password with a fixed key that multiplies with a specific matrix to increase the obfuscation of the message. For a column in the round message matrix, it is expressed as a cubic polynomial in galois field $GF(2^8)$:

$$s(x) = s_3x^3 + s_2x^2 + s_1x + s_0 \tag{4}$$

Multiply this polynomial with a fixed cubic polynomial $c(x)$ under modulus $x^4 + 1$ to get the output column:

$$c(x) \cdot s(x) \text{mod}(x^4 + 1) \tag{5}$$

Where the fixed polynomial is (whose coefficients are all elements in galois field $GF(2^8)$):

$$c(x) = c_3x^3 + c_2x^2 + c_1x + c_0 = '03'x^3 + '01'x + '02' \tag{6}$$

Step4: Each element in the round message matrix and each element in the corresponding round key matrix are added bit-by-bit binary operation to ensure the secret random distribution characteristics required by the message data. Using the above steps, for a given plaintext m , the ciphertext is calculated by AES encryption function E and key K :

$$c = E(K, m) \tag{7}$$

For ciphertext, the plaintext can also be obtained by AES decryption function D and the same key K calculation:

$$m = D(K, c) \tag{8}$$

The development of encryption and decryption module is completed by adding user id in AES encryption module.

4.2 Optimization

In order to improve the efficiency and usability of the scheme, we optimize the mixed encryption scheme.

Multiprocess Optimization. Using AES symmetric encryption system to encrypt and decrypt genomic data have a lot of computation going on in the program. In practice, it is necessary to process genomic data on a large scale and run the program for a long time. Considering that AES is a block cipher algorithm, and the encryption (or decryption) of each group is independent, multi-process means can be introduced into the encrypting and decrypting programs to achieve the parallel operation of multiple computer processors, so as to achieve the purpose of accelerating the speed of data processing.

After multi-process optimization, the encryption and decryption time is shortened by about 5 times, and it takes 40 min to encrypt 200 MB genomic data files. For practical applications, it is still less efficient, but this encryption algorithm occupies less memory, and the size of the generated encryption file is the same as the original file, without increasing the transmission time.

AES Encryption Optimization. The original version of the algorithm used the numpy module to achieve the AES128 algorithm. Due to the efficiency problems of the python language and the optimization problems of the algorithm itself, this encryption method requires a long time. We improved the algorithm by calling crypto module which is write by C to realize efficiency algorithm, used EBC mode for encryption and decryption.

This method greatly reduces the encryption time, and only needs 10s to encrypt 266 MB files. However, the problem with this method is that it occupies a large amount of running memory, which is about 4–5 times of the file size, and the encrypted file becomes twice as big as the original one.

5 Scheme Analysis

We used the implemented and optimized scheme to conduct encryption test on the genome data files, and conducted security analysis and efficiency analysis on the test results.

5.1 Security Analysis

To ensure the security of encryption, the most important thing is to ensure the security of the key. We used RSA public key K_p encryption AES key K to ensure the security of AES key K , avoiding the transmission of K plaintext in the network environment. RSA private key K_s will only be stored in the client local, can not be accessed by untrusted third party, RSA encryption algorithm based on the problem of large integer factoring, recovering the private key K_s by the public key K_p takes a lot of computation even if $K_p(K)$ is intercepted by the attacker is not unable to obtain the key K . This agreement can guarantee the security of the AES key, further ensure the security of genomic data.

AES algorithm supports variable key length, which is generally recognized as the encryption algorithm with high security at present. Under the current computing power, no very effective attack method has been found. AES is designed

with a wide trajectory strategy, which is a design strategy for differential analysis and linear analysis, and has a significant effect in resisting differential cryptography and linear cryptography. As long as the security of the AES key is ensured, the AES encryption algorithm is secure. This scheme uses RSA to encrypt the AES key.

RSA security is based on the difficulty of large integer decomposition. So far, there is no effective algorithm that can realize large integer factoring. Therefore, under the premise of protecting the private key, the attack on RSA algorithm can only rely on key exhaustion. Since RSA's addition and decryption are all exponential operations, the key exhaustive computation is huge and the computation speed is very slow, the attack difficulty is very high, the security index is very high. In addition, this scheme updates the key in each transmission. Even if the key in the transmission process is leaked, it will not affect the subsequent encryption transmission and can maximize the security of encryption transmission.

5.2 Usability Analysis

MD5 hash function is used to calculate the hash value of key and plaintext when transmitting encryption key and encrypted ciphertext. After the key and plaintext are obtained through decryption, the integrity of the key and plaintext can be verified to prevent data errors caused by the loss of byte stream in the transmission process and ensure the usability of genetic data.

5.3 Efficiency Analysis

The computer used in the test is an eight-core processor, i.e., eight processes are opened for parallel computing. We take a 1 MB file as the test object to conduct multi-process encryption and decryption tests. The results are listed in Table 1.

Table 1. Multi-process test results

Process	1	2	4	8
Encryption takes	35.1 s	18.6 s	9.4 s	7.5 s
Decryption takes	80.9 s	47.9 s	21.1 s	17.5 s

It can be seen from the results that the speed of encrypting and decrypting increases significantly when the number of parallel processes changes from 1 to 4, and the time spent is approximately linear with the number of processes. Processes from 4 to 8 increased speed, but not significantly. When the number of parallel processes is set above 8, the speed of the program does not increase. Considering that the server in the actual application might be multi-core, the code was improved to automatically detect the number of CPU and start all processes.

In addition to multi-process optimization, we ended up using the crypto library to implement AES encryption. We use a 266 MB genomic data file to test the efficiency of the scheme. The AES algorithm using the numpy module takes 40 min to encrypt, but the memory footprint is small. The encryption time of AES algorithm using crypto module is 10s, performing multiple rounds of encryption calculations takes memory footprint 12 MB. It can be seen from the test results that AES algorithm using crypto library can meet the actual use requirements of encrypted genomic data in terms of encryption efficiency and memory occupancy. The test result is listed in Table 2.

Table 2. Algorithm and memory optimization test results

Library	Performance			
	Size	Time	Memory usage	Operating rate
Numpy	266 MB	43.0 min	10.0 MB	Slower
Crypto	266 MB	10.2 s	1.2 GB	Superior

Since there are not many researches on the method of hybrid encryption of genomic data files directly, we have selected the latest queryable genomic data privacy protection protocol EPISODE proposed by Schneider et al. [15] for comparison. The results are shown in Table 3. The EPISODE solution is queryable, and we know that this encryption operation is time consuming. Our solution does not provide ciphertext queryability and is therefore more efficient for larger genomic data files.

Table 3. Hybrid encryption vs. EPISODE

Library	Performance			
	Size	Time	Security	Query ability
Hybrid encryption	1.0 MB	7.2 s	Yes	No
EPISODE	1.0 MB	4.0 min	Yes	Yes

6 Conclusion

In this paper, we analyzed the genomic data file format and designed a hybrid encryption scheme based on AES and RSA for genomic data files. We implemented the hybrid encryption scheme and tested the efficiency of the scheme by using genomic data. Compared with AES encryption scheme that is not specifically used for genomic data files, the encryption time of this scheme is reduced by twice, and this scheme uses RSA encrypt AES key, which is more secure

than general AES encryption software. The scheme successfully completes the encryption and decryption of genomic data, which has specificity, high operation efficiency and good practicability. It provides a feasible scheme for the encryption of genomic data and is of great significance to the privacy protection of genomic data.

Acknowledgment. This project is supported by the National Key Research and Development Program of China (No. 2016YFC1000307), the National Natural Science Foundation of China (No. 61571024, No. 61971021) and Aeronautical Science Foundation of China (No. 2018ZC51016) for valuable helps.

References

1. Homer, N., et al.: Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays. *PLoS Genet.* **4**, e1000167 (2008)
2. Wang, R., Li, Y.F., Wang, X.F., Tang, H.X., Zhou, X.Y.: Learning your identity and disease from research papers: information leaks in genome wide association study. In: *Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, vol. 10, no. 1145, pp. 534–544* (2009). <https://doi.org/10.1145/1653662.1653726>
3. Gymrek, M., McGuire, A.L., Golan, D., Halperin, E., Erlich, Y.: Identifying personal genomes by surname inference. *Science* **339**(6117), 321–324 (2013). <https://doi.org/10.1126/science.1229566>
4. Lippert, C., et al.: Identification of individuals by trait prediction using whole-genome sequencing data. *PNAS* **114**(38), 10166–10171 (2017). <https://doi.org/10.1073/pnas.1711125114>
5. Sweeney, L.: k-anonymity: a model for protecting privacy. *Int. J. Uncertainty Fuzziness Knowl.-Based Syst.* **10**(05), 557–570 (2002). <https://doi.org/10.1142/S0218488502001648>
6. Nyholt, D.R., Yu, C., Visscher, P.M.: On Jim Watson’s APOE status: genetic information is hard to hide. *Eur. J. Hum. Genet.* **17**(2), 147–149 (2009). <https://doi.org/10.1038/ejhg.2008.198>
7. Samarati, P., Sweeney, L.: Generalizing data to provide anonymity when disclosing information. In: *PODS*, p. 188 (1998). <https://doi.org/10.1145/275487.275508>
8. Machanavaajhala, A., Kifer, D., Gehrke, J., Venkatasubramanian, M.: L-diversity: privacy beyond k-anonymity. *TKDD* **1**(1), 3 (2007). <https://doi.org/10.1109/ICDE.2006.1>
9. Li, N., Li, T., Venkatasubramanian, S.: Closeness: a new privacy measure for data publishing. *IEEE Trans. Knowl. Data Eng.* **22**(7), 943–956 (2010). <https://doi.org/10.1109/tkde.2009.139>
10. Johnson, A., Shmatikov, V.: Privacy-preserving data exploration in genome-wide association studies. In: *Proceeding of the 19th ACM SIGKDD International Conference on Knowledge/Discovery and Data Mining*, pp. 1079–1087. ACM (2013). <https://doi.org/10.1145/2487575.2487687>
11. Ayday, E., Raisaro, J.L., Hubaux, J.P.: Personal use of the genomic data: privacy vs. storage cost. In: *Proceeding of IEEE Global Communications Conference, Exhibition and Industry Forum*, pp. 2723–2729 (2013). <https://doi.org/10.1109/GLOCOM.2013.6831486>

12. Cristofaro, E.D., Faber, S., Tsudik, G.: Secure genomic testing with size- and position-hiding private substring matching. In: Proceedings of the 12th ACM Workshop on Privacy in the Electronic Society, pp. 107–118. ACM (2013). <https://doi.org/10.1145/2517840.2517849>
13. Chen, Y., Peng, B., Wang, X., Tang, H.: Large-scale privacy-preserving mapping of human genomic sequences on hybrid clouds. In: Proceeding of the 19th Network and Distributed System Security Symposium, San Diego, California, USA (2012)
14. Burrows, M., Abadi, M., Needham, R.: A logic of authentication. *SIGOPS Oper. Syst. Rev.* **23**(5), 1–13 (1989). <https://doi.org/10.1145/77648.77649>
15. Schneider, T., Tkachenko, O.: EPISODE: efficient privacy-PreservIng similar sequence queries on outsourced genomic DatabasEs? In: Asia CCS 2019 Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, pp. 315–327 (2019). <https://doi.org/10.1145/3321705.3329800>



Sentiment Analysis of Text Classification Algorithms Using Confusion Matrix

Babacar Gaye^(✉) and Aziguli Wulamu

School of Computer and Communication Engineering,
University of Science and Technology, Beijing, China
babacargaye92@gmail.com

Abstract. Sentiment analysis on text mining has a vital role in the process of review classification. Text classification needs some techniques like natural language processing, text mining, and machine learning to get meaningful knowledge. This paper focuses on performance analysis of text classification algorithms commonly named **Support vector machine, random forest and extreme Gradient Boosting** by creating confusion matrices for training and testing applying features on a product review dataset. We did comparison research on the performance of the three algorithms by computing the confusion matrix for accuracy, positive and negative prediction values. We used unigram, bigram and trigrams for the feature extraction on the three classifiers using different number of features with and without stop words to determine which algorithms works better in case of text mining for sentiment analysis.

Keywords: Confusion matrix · Classification · SVM · Random forest · XGBoost · Sentiment analysis

1 Introduction

Recently, researches about natural language processing and text mining became very important because of the increase of sources that gives electronic datasets according to [1] many text mining procedures are required to analyze data on social media and e-commerce websites for the identification of different patterns on texts. We classify the documents based on categories that are predefined for text classification. We use a corpus to be the primary structure for management and representation a collection of the dataset. All preprocessing data techniques can be performed on the corpus. The performance of a document classification technique is acquired by creating the confusion matrix on training and testing datasets. The latest news and discoveries in the field of exchange of information and opinions carve the way of computer applications designed for the analysis and detection sentiments expressed on the Internet. Presented in the literature under the name opinion mining and sentiment analysis, sentiment analysis is used among others for the detection of opinions on websites and social networks, the clarification on the behavior of consumers, product recommendation and explanation of the election results. It is used to look for evaluative texts on the Internet

such as criticism and recommendations and analyze automatically or manually feelings that are there expressed to understand public opinion better. It has already been demonstrated in previous studies that feelings of Analysis prove particularly attractive for those who have an interest in knowing the public, it whether for personal, commercial, or political reasons. Thus, many systems Autonomous have already been developed for automatic sentiment analysis. In this research paper, we made a comparative study of three machines learning algorithms which are Support vector machine, random forest, and extreme Gradient Boosting for classification and made the confusion matrix results.

2 Literature Reviews

The most used algorithm for document classification is called Support Vector Machines. The main feature of Support Vector Machines is to build a hyperplane between the classes that provide maximum margins and use these cut off points for text classification. For feature two-dimensional case the created hyper plane is a straight line. The main advantage of Support Vector Machines is that it can create datasets with many attributes with less overfitting than other methods [2, 5]. Nevertheless, SVM classification has speed limitations during both training and testing phases [3]. XGBoost was designed for speed and performance using gradient-boosted decision trees. It represents an element for machine boosting, or in other words applying to boost the machines, initially made by Tianqi Chen [4] and further taken up by many developers. RF is an ensemble of classification that proceed by voting the result of individual decision trees. Several techniques and methods have been suggested by researchers in order to grow a random forest classifier [7]. Among these methods, the authors method has gained increasing popularity because it has higher performance against other methods [8].

In [10], the author considered sentimental classification based on categorization aspect with negative sentiments and positive sentiments. They have experimented with three different machine learning algorithms which are Naive Bayes classification, Maximum Entropy and Support Vector machine, classification applied over the n-gram techniques.

In [6] they have used balanced review dataset for training and testing, to identify the features and the score methods to determine whether the reviews are negative or positive. They used classification to classify the sentences obtained from web search through search query using the product name as a search condition.

3 Implementation Procedure

(See Fig. 1).

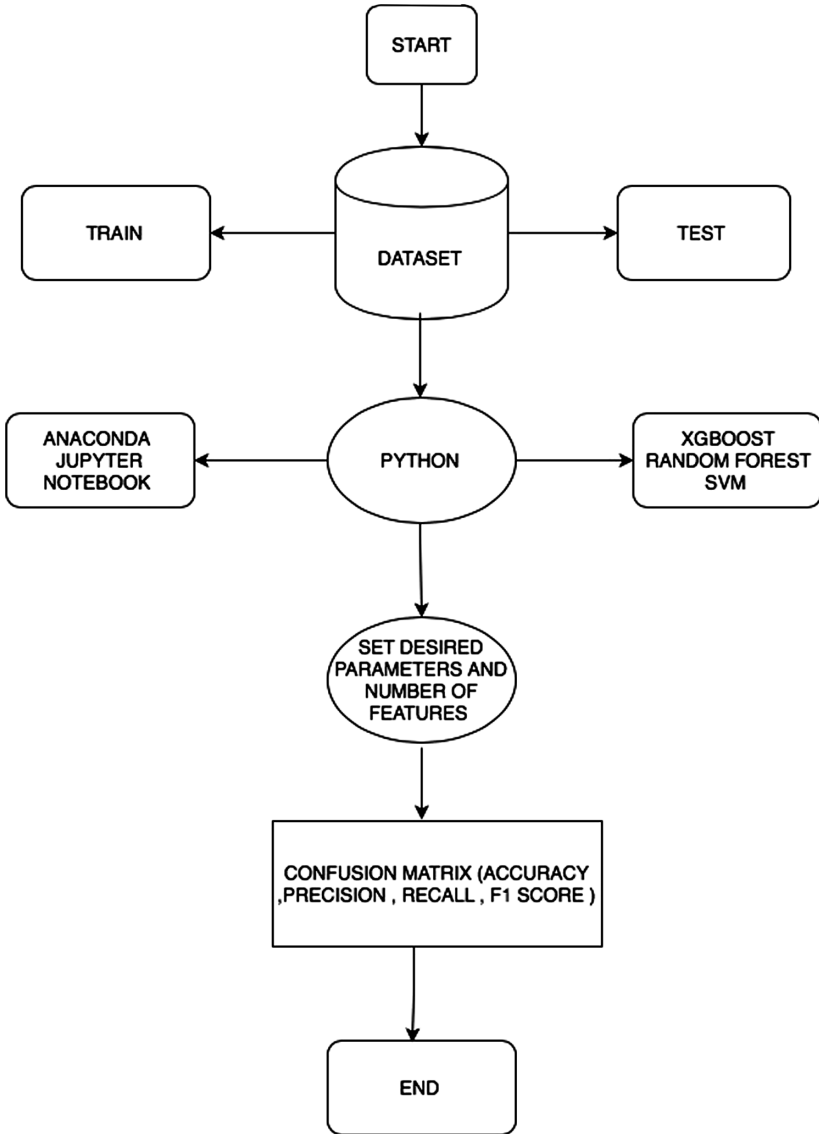


Fig. 1. Implementation flowchart

3.1 Dataset

(See Table 1).

```
create dataframe from csv file
data = FeatureExtraction(r'tweet_product_company.csv')
data.data.head()
```

Table 1. Dataframe

	Tweet	Brand	Label	clean_tweet
0	.@wesley83 I have a 3G iPhone. After 3 hrs twe...	iPhone	Negative	I have a g iphone after hrs tweeting at it was...
1	@jessedee Know about @fludapp ? Awesome iPad/i...	iPad or iPhone App	Positive	Know about awesome ipadiphone app that you wil...
2	@swonderlin Can not wait for #iPad 2 also. The...	iPad	Positive	Can not wait for also they should sale them do...
3	@sxsxw I hope this year's festival isn't as cra...	iPad or iPhone App	Negative	I hope this year festival is not as crashy as...
4	@sxtxstate great stuff on Fri #SXSW: Marissa M...	Google	Positive	Great stuff on fri marissa mayer google tim or...

3.2 Feature Extraction

Feature extraction relates to dimension reductions. It is a technique for dimension reduction that can reduce an initial dataset into groups for data processing. When the dataset one usually input to an algorithm is being processed, it can be converted into less data and information. This procedure is named feature extraction.

The extracted features ought to contain all needed information from the inputted data so that the experimentation procedure can be done by using reduced representation instead of the complete initial dataset.

Term occurrence ($To_{t,d}$): $To_{t,d}$ of term t in document d is defined as the number of times that a term t occurs in document d .

$$To_{t,d} = n_{t,d}$$

Term Frequency: $To_{t,d}$ is the normalized form of $To_{t,d}$ to prevent a bias towards very long documents in order to measure the importance of the term t within the particular document d .

$$TF_{t,d} = \frac{n_{t,d}}{\sum_k n_{k,d}}$$

Inverse Document Frequency (idf_t): Estimate the rarity of a term in the whole document collection. (If a term occurs in all the document, 0 will be the Tfidf.)

$$idf_t = \log \frac{|D|}{|\{d : t \in d\}|}$$

With $|D|$: The total number of documents in the corpus

$|\{d : t \in d\}|$: The number of the document where the term t appears i.e. ($n_{t,d} \neq 0$).

Term Frequency-Inverse Document Frequency (TFidf_{t,d}):

Finally, the tf-idf of the term t in document d is computed as follows:

$$TFidf_{t,d} = Tf_{t,d} * idf_t$$

Evaluation Method:

- Precision: the Precision is the fraction of retrieved values that are relevant. It encompasses all retrieved values and only considers the topmost results returned by the system at a cut-off point. This kind of measure is named Precision [9].

$$Precision = \frac{\text{relevant value} + \text{retrieved value}}{\text{retrieved value}}$$

- Recall: Recall is the fraction of the relevant value plus de retrieved value divided by the relevant value. In the classification binary, recall is called sensitivity [9]. It is trivial to get the recall of 100% by returning all values in response to the query. Recall equation is defined by:

$$recall = \frac{\text{relevant value} + \text{retrieved value}}{\text{relevant value}}$$

- F1-score: F1 score can be seen as a the average weight of the precision and recall, the F1 score task 1 as best value and the 0 as least value. The contribution of the precision and the recall to the F1 score are equal. The formula for the F1 score is:

$$F1 \text{ score} = 2 * \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}}$$

3.3 Confusion Matrix

The methods for the classification of the review dataset can be obtained by the terms frequencies of correctness by computing statistical measures that are True Positives,

True Negatives, False Positive and False Negatives. These are the elements of the Confusion Matrix which is a table that has been generated for a classifier on a binary dataset and can be used to justify the performance of a classifier.

Precision and Recall performances of their experimentation have been tested so that they can predict the false data and the correct data. The assessment is made with Confusion Matrices in which True Positive rate is a definite class and it is considered a positive class. True Negative rate is considered a class negative. False Positive rate is a negative class Classified as a positive and neutral classes, False Negative rate is a definite class that is classified as a negative and neutral class.

3.4 Classification Model

The way the dataset was used in the model of our experiment is represented by the classification methodology in Fig. 2 as well as the flow of work chart in Fig. 3 This review dataset included test and train data types. Both datasets were used in our model. The dataset was split into test and train type datasets. Both datasets were first concatenated to make the data into one file. Python was used as the environment in which this combined data had to run. Moving further, the XGBoost, RF and SVM packages were downloaded on the Anaconda software, which has in-built packages. Using Python, the required packages had to be called. The dataset was opened on the Python on jupyter notebook platform and, by setting various parameters related to, the code was run on the three machine learning algorithms on a product review dataset. The results included confusion matrix, Precision, accuracy and we used matplotlib to draw the results.

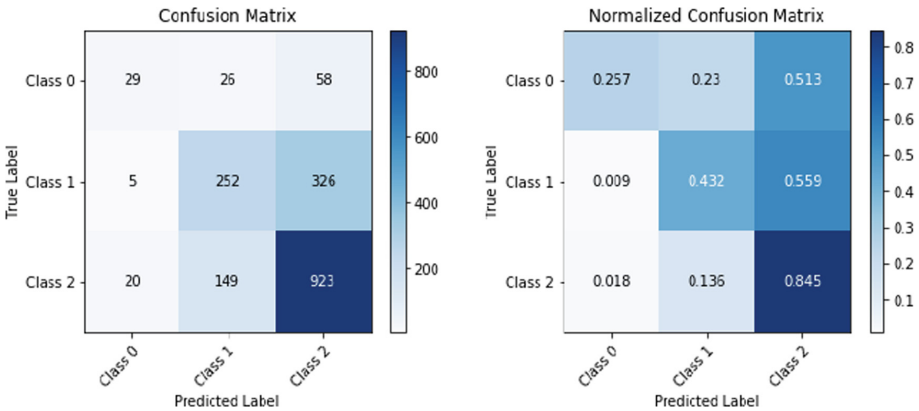


Fig. 2. XGBoost classifier confusion matrix

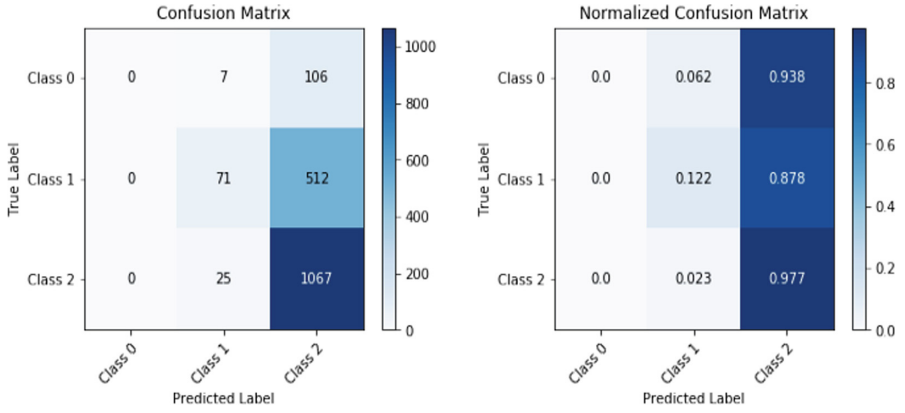


Fig. 3. Support vector machine confusion matrix

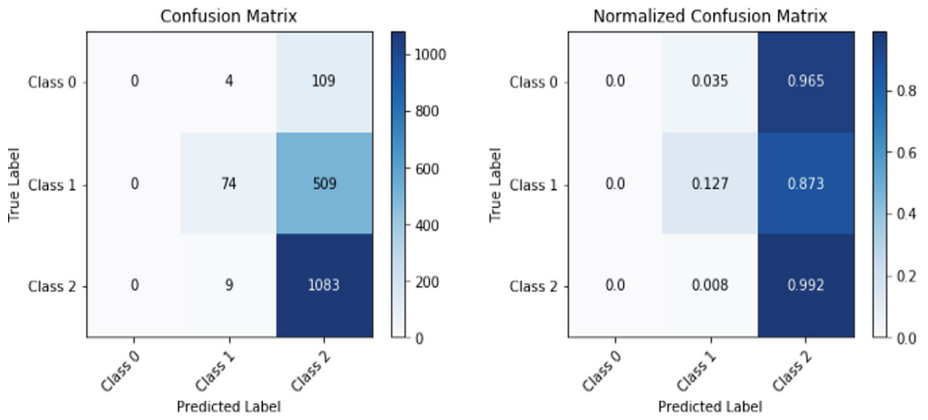


Fig. 4. Random forest classifier confusion matrix

4 Results

In this part we presented the best results for the confusion matrices of our implementation which is for the bigram with stop words using 200 features.

```
xgb_bigram_with_stop_words_200_features
=====

acc: 0.6733780760626398
report:          precision    recall  f1-score   support

      0          0.54         0.26         0.35         113
      1          0.59         0.43         0.50         583
      2          0.71         0.85         0.77        1092

    micro avg          0.67         0.67         0.67        1788
    macro avg          0.61         0.51         0.54        1788
weighted avg          0.66         0.67         0.65        1788
```

```
svm_bigram_with_stop_words_200_features
=====

acc: 0.6364653243847874
report:          precision    recall  f1-score   support

      0          0.00         0.00         0.00         113
      1          0.69         0.12         0.21         583
      2          0.63         0.98         0.77        1092

    micro avg          0.64         0.64         0.64        1788
    macro avg          0.44         0.37         0.33        1788
weighted avg          0.61         0.64         0.54        1788
```

```

rf_bigram_with_stop_words_200_features
=====
acc: 0.6470917225950783
report:          precision    recall  f1-score   support

           0           0.00      0.00      0.00         113
           1           0.85      0.13      0.22         583
           2           0.64      0.99      0.78        1092

   micro avg           0.65      0.65      0.65        1788
   macro avg           0.50      0.37      0.33        1788
weighted avg           0.67      0.65      0.55        1788

```

For this research we did the confusion matrix using the unigram, bigram and trigram for the entire three-machine learning algorithm. We used different sets of selected features with and without stop words respectively 100, 200, 300.

From all these 3 classifiers we choose the one that has the highest accuracy and presented it in the figure. Our results have shown that the classifier works better for bigram with stop words using 200 features.

5 Comparative Analysis

After plotting this confusion matrix, the values which are obtained for all our four classes are used to calculate the accuracy of the algorithm's prediction. As a result, the bar graph that has been plotted are for the actual results and predicted results for all classes that are positive, negative, and neutral (Fig. 5).

Confusion matrices of all the algorithms been obtained, we calculated the score for the accuracy. The best performing algorithm will be best at predicting and that model will be considered for further for the Sentiment analysis tasks. We did a comparative analysis for the three machine learning algorithms, and the results are shown in Fig. 4. On top as per the results obtained, the support vector machine is getting the lowest accuracy, and the random forest comes on the second position. As per the results, the XGBoost is getting the highest accuracy. The calculation of accuracy value of Analysis towards the SVM method's result that was done using need to have the accuracy, Precision, and recall performance evaluation from the experiment with the confusion matrix method. The evaluation done by using Confusion Matrix includes the following indicators: True Positive Rate (TP rate), True Negative Rate (TN Rate), False Positive

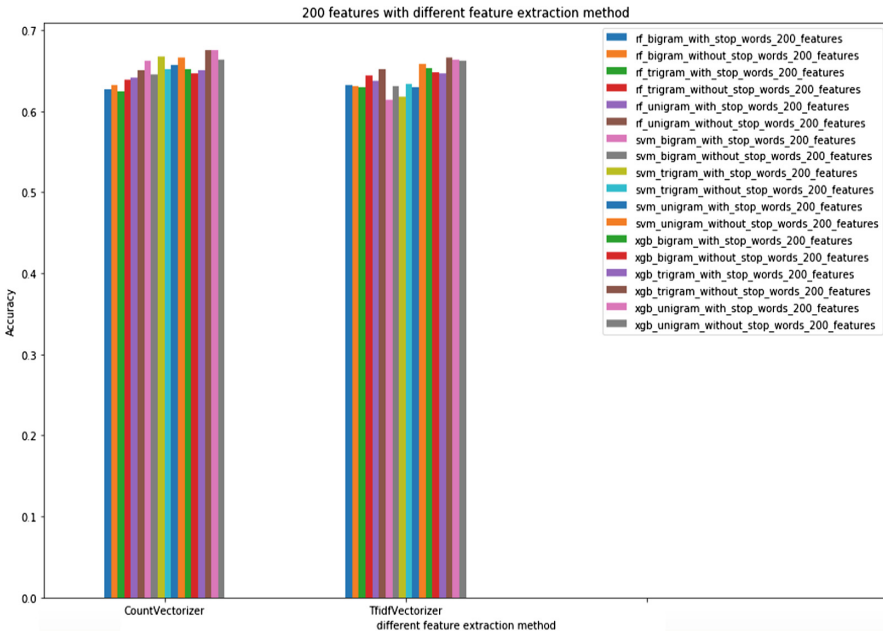


Fig. 5. Confusion matrices bar plot

Rate (FP Rate) and False Negative Rate (FN rate). The TP rate is the percentage of the positive class, which was classified as the positive class, whereas the TN rate is the percentage of the class negatively classified as a negative class. FP rate is class negative, which is classified as the positive class. The FN rate is a class positive that is classified as a negative class.

6 Conclusion

In Sum, a comparative analysis of the performance of the support vector machine, random forest, XGBoost review classification techniques is presented in this paper. All the results were found using the Python package and the implementation of the document classification techniques was done using the anaconda Jupiter notebook libraries. Sentimental Analysis of reviews Classification Algorithms using Confusion Matrix indicated that XGBoost has a better performance better classification than support vector machine and random forest. There is a large need in the industry for use of Sentiment Analysis because every company wants to know how consumers feel about their services and products. In future work, different types of approaches, such as machine learning and products reviews should be combined in order to overcome their challenges and improve their performance by using their merits. In order to get a better understanding of natural language processing, a complete knowledge as well as reasoning methods that originates in human thoughts and psychology will be needed.

References

1. Irfan, R., et al.: A survey on text mining in social network. *Knowl. Eng. Rev.* **30**(2), 157–170 (2015)
2. Nugroho, A.S., Witarto, A.B., Handoko, D.: Support Vector Machine Teoridan Aplikasinya dalam Bioinformatika 1 (2003)
3. Kim, J., Kim, B.-S., Savarese, S.: Comparing image classification methods nearest neighbor, support vector machines. *Applied Mathematics in Electrical and Computer Engineering*. ISBN 978-1-61804-064-0
4. Brownlee, J.: A gentle introduction to XGBoost for applied machine learning. *Mach. Learn. Mastery*. <http://machinelearningmastery.com/gentle-introduction-xgboost-applied-machine-learning/>. Accessed 2 March 2018
5. Xia, R., Zong, C., Li, S.: Ensemble of feature sets and classification algorithms for sentiment classification. *Inf. Sci.* **181**(6), 1138–1152 (2011)
6. Dave, K., Lawrence, S., Pennock, D.M.: Mining the peanut gallery: opinion extraction and semantic classification of product reviews. In: *Proceedings of the 12th International Conference on World Wide Web*, pp. 519–528. ACM (2003)
7. Dietterich, T.G.: An experimental comparison of three methods for constructing ensembles of decision trees: bagging, boosting, and randomization. *Mach. Learn.* **40**(2), 139–157 (2000)
8. Banfield, R.E., Hall, L.O., Bowyer, K.W., Kegelmeyer, W.P.: A comparison of decision tree ensemble creation techniques. *IEEE Trans. Pattern Anal. Mach. Intell.* **29**(1), 173–180 (2007)
9. Tang, D., Wei, F., Yang, N., Zhou, M., Liu, T., Qin, B.: Learning sentiment-specific word embedding for twitter sentiment classification (2014)
10. Pang, B., Lee, L.: A sentimental education: sentiment analysis using subjectivity summarization based on minimum cuts. In: *ACL 2004 Proceedings of the 42nd Annual Meeting on Association for Computational Linguistics (2004)*. Article no. 271



On the Constructions of Bigraphical Categories

Dong Xu^(✉) and Xiaojun Li

School of Computer Engineering and Science, Shanghai University,
Shanghai 200444, People's Republic of China
dxu@shu.edu.cn

Abstract. Bigraph was proposed as a formal theoretical model in attempt to provide a rigorous platform for designing, simulating and analyzing ubiquitous computing systems. As the mathematical basis of bigraphs, bigraphical categories become important aspects of their theory and they are related to precategory, category, s-category, wide category and symmetric partial monoidal category. However, we detect trouble spots in the construction of bigraphical quotient category and illustrate that not all s-category can be converted to the symmetric partial monoidal category by the support quotient. Both support quotient and lean-support quotient, hence, are not always the symmetric partial monoidal category. And, likewise, the quotient wide s-category may not be the wide symmetric partial monoidal category in general. Also, quotient wide reactive system may not be abstract, consequently for the same reason. Therefore, we must make clear what conditions on s-category allow us to obtain a symmetric partial monoidal category, and ensure that the behavioral congruence is preserved for the abstract bigraphical reactive system.

Keywords: Category theory · Bigraph · Bigraphical category · Theory of computation

1 Introduction

With the rapid development of network computing and its applications, many interactive agents are increasingly distributed in the world which can be artificial or can be natural. It is important that these networks of agents can be modeled and they can be understood. Robin Milner's purpose was to describe in the book [1] just such a model, and he did so by presenting a unified and rigorous structural theory, based on bigraphs, for systems of interacting agents. This bigraphical theory bridges the existing theories of concurrent processes and the aspirations for ubiquitous systems whose enormous size challenges our understanding. Bigraphical reactive systems (BRSs) can define the dynamics of process and the theory has a very powerful axiomatic system which can help us effectively reason and validate the behavior of these agents distributed in the Cyber-physical world. For example, bigraphical reactive systems are used to model ubiquitous systems, capturing mobile locality in the place graph and mobile

connectivity in the link graph. Moreover, bigraph and its corresponding theories become a meta-theory encompassing existing calculi for concurrency and mobility. Nowadays, some of bigraph theories are applied on some topics that include ubiquitous computing, context-aware systems [2], etc. Christos Tsigkanos, et al. presented a bigraph based tool for engineering topology aware adaptive security in cyber-physical systems [3]. Steve Benford, et al. gave a model of an example ubiquitous system using the mathematical formalism of bigraphs [4]. Christos Tsigkanos, et al. explored the use of bigraphical reactive systems to model the topology of cyber and physical spaces and their dynamics [5]. Ahmed Taki Eddine Dib, et al. proposed a bigraphs based formal modelling approach for the specification of multi-agent system architectures and their reconfiguration [6]. Chris Stary, et al. demonstrated the utility of handling of system-of-systems based on bigraphs [7], and so on.

Both the theory and applications of bigraphs, however, are still far to being mature and fully useful. We find that there are some problems in the bigraphical category theory and they are given in this paper. For example,

- (1) Can the support quotient functor of s -categories ensure that the support quotient $\mathbf{C} \stackrel{\text{def}}{=} \mathbf{C}/\simeq$ must be a symmetric partial monoidal (spm) category?
- (2) Can the lean-support quotient functor of bigraphical s -categories ensure that the lean-support quotient $\text{BG}(\mathcal{K}) \stackrel{\text{def}}{=} \text{BG}(\mathcal{K})/\simeq$ must be a spm category?

Below we first briefly describe the preliminaries of bigraphs and bigraphical categories necessary to this paper in Sect. 2. Some problems in bigraphical categories are depicted in Sect. 3. Section 4 concludes the paper finally.

2 Preliminaries

For the sake of making the paper complete, we will give a brief introduction to Milner's theory of bigraphs and refer to some references for more details about the theory. A reader familiar with bigraphs should be able to skip this subsection without compromising the understanding of the remainder of the paper.

2.1 A Brief Introduction of Bigraphs

A bigraph consists of two sub-graphs - a place graph and a link graph - that are independent from each other while based on the same node set, which is the reason why it is called a bigraph. The place graph describes the location of the nodes, whereas the link graph describes the connectivity of them. Figure 1 gives an example of bigraphs - bigraph F , and Fig. 2 shows its place graph and link graph respectively.

A basic signature takes the form (\mathcal{K}, ar) . The \mathcal{K} is a finite set of elements related to signature such that $\kappa ::= \kappa | \kappa : n$ for each $\kappa \in \mathcal{K}$, where κ is a kind of node called control in bigraphs, $n \in \mathbb{N}$, where \mathbb{N} denotes natural number. So, a basic signature has a set \mathcal{K} whose elements are kinds of node called controls, and a map $\text{ar}: \mathcal{K} \rightarrow \mathbb{N}$

assigning an arity, a natural number, to each control. Signatures make the bigraphs represent the model's formal entities. We shall soon see that bigraphs over a given basic signature form an s-category. Also, we will see how the concrete place graphs, link graphs and bigraphs over a basic signature each form a category of a certain kind.

2.2 A Brief Introduction of Bigraphs

In general, a category \mathcal{C} consists of a collection of objects and a collection of arrows. Each arrow f has an object $\text{dom}(f)$, called its domain, and an object $\text{cod}(f)$, called its codomain. The collection of all arrows with domain I and codomain J is written $\mathcal{C}(I \rightarrow J)$, or just $(I \rightarrow J)$. If the collection of arrows is actually a set then we call it the homset of I and J . Each object has an identity arrow. Arrows must then satisfy associative law and identity law.

It follows that the objects or arrows of a category are usually not required to constitute a set. In fact, some categories are too complex for either their arrows or their objects do not form sets. A category is called *small* category if its objects and arrows constitute sets; otherwise it is *large* category [8]. For example, the category of sets (Sets) itself is a large category because its objects are all sets and its arrows are total functions between sets, and composition of arrows is the function composition in set theory. Identity arrows are identity functions.

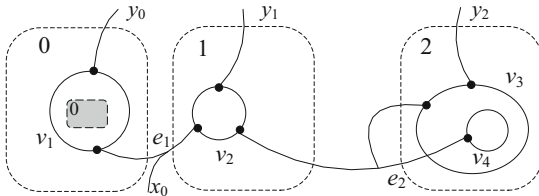


Fig. 1. An example of bigraph (F).

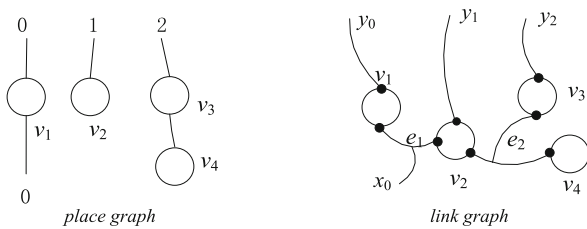


Fig. 2. The place graph and link graph of the bigraph (F).

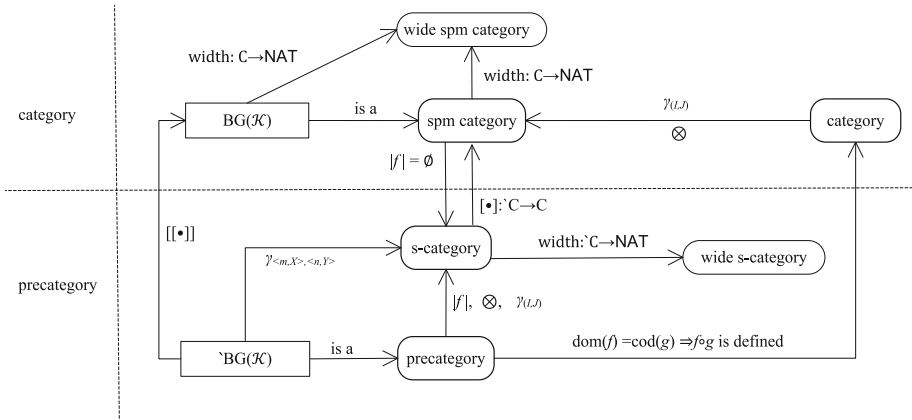


Fig. 3. The relationship of the bigraphical categories.

2.3 Bigraphical Categories

Robin Milner introduced basic category theory into bigraphs in order to classify bigraphs and to develop some their theories [9]. The category defined for bigraph is obviously small category because the definition of category wherein says explicitly their objects and arrows constitute sets respectively.

There are four kinds of category which are category, symmetric partial monoidal category (spm) category, precategory and s-category. According to the definition of support-equivalent class, we have the following proposition.

Proposition 1. The support-equivalent relation defined in s-category, denoted \simeq , is a congruence relation.

According to the existing theories of bigraphical category, the relationship of the bigraphical categories is shown in Fig. 3 and their essential properties can be summarized as the following properties.

- (1) Generally, both precategory and s-category are not yet category.
- (2) Any spm category must be a category actually.
- (3) For a precategory $\setminus C$, it can be transformed into a s-category if we assign each arrow of $\setminus C$ a finite support, and the composition and tensor product are well defined.
- (4) A s-category is *wide* if it is equipped with a functor $\text{width}: \setminus C \rightarrow \text{NAT}$. The elements of NAT are finite ordinals. Similarly, there are width functors for spm category and bigraphical category $\text{BG}(\mathcal{K})$.

In addition, there are two properties which give rise to some problems as follows.

- (5) There is a support quotient functor of s-categories: $[\cdot]: \setminus C \rightarrow C$, where $C \stackrel{\text{def}}{=} \setminus C / \simeq$ is an spm category.
- (6) There is a lean-support quotient functor of bigraphical s-categories: $[[\cdot]]: \setminus \text{BG}(\mathcal{K}) \rightarrow \text{BG}(\mathcal{K})$, where $\text{BG}(\mathcal{K}) \stackrel{\text{def}}{=} \setminus \text{BG}(\mathcal{K}) / \simeq$ is an spm category.

For the Property (5), the support quotient functor of s-categories, however, can't ensure that $\underline{\mathcal{C}}/\simeq$ must be a spm category. Also, the lean-support quotient functor of bigraphical s-categories can't ensure that $\text{BG}(\mathcal{K}) \stackrel{\text{def}}{=} \text{BG}(\mathcal{K})/\simeq$ must be a spm category after analyzing Property (6). The reasons will be discussed in detail in Sect. 3.

3 Discussions

Let's recall how the quotient category is constructed in general category theory firstly and compare it with the construction of support quotient category.

3.1 The Comparison of the Two Kinds of Quotient Category

Let \sim be a congruence relation on the arrows of a category \mathcal{B} . Define the quotient category \mathcal{B}/\sim as follows.

- (1) The objects of \mathcal{B}/\sim are the objects of \mathcal{B} .
- (2) The arrows of \mathcal{B}/\sim are the congruence classes of arrows of \mathcal{B} .
- (3) If $f : A \rightarrow B$ in \mathcal{B} , then $[f] : A \rightarrow B$ in \mathcal{B}/\sim .
- (4) If $f : A \rightarrow B$ and $g : B \rightarrow C$ in \mathcal{B} , then $[g] \circ [f] \stackrel{\text{def}}{=} [g \circ f] : A \rightarrow C$ in \mathcal{B}/\sim .

We justify the definition by a theorem.

Theorem 1. The quotient category \mathcal{B}/\sim is a category. Its construction defines a functor: $\mathcal{F} : \mathcal{B} \rightarrow \mathcal{B}/\sim$.

Now, we compare the definitions of \mathcal{C}/\simeq and \mathcal{B}/\sim , and show them in Table 1.

Table 1. The comparison of the two quotient categories

\mathcal{C}/\simeq	\mathcal{B}/\sim
\simeq is a congruence relation	\sim is a congruence relation
\mathcal{C} is only a s-category	\mathcal{B} is a category
$[g] \circ [f]$ is not always defined	$[g] \circ [f]$ is always defined
\mathcal{C}/\simeq is not always a category.	\mathcal{B}/\sim must be a category.

Consequently, we conclude theorem 2.

Theorem 2. The support quotient category \mathcal{C}/\simeq is not always a category.

Proof. In fact, if $f : A \rightarrow B$ and $g : B \rightarrow C$ in \mathcal{C} , $g \circ f$ is defined iff $|g| \# |f|$ (i.e. $|g| \cap |f| = \phi$). On the other hand, if $[f] : A \rightarrow B$ and $[g] : B \rightarrow C$ in \mathcal{C}/\simeq , but $|g' \cap |f'| \neq \phi$ for any $g' \in [g], f' \in [f]$, then $[g] \circ [f]$ is not defined. It results that \mathcal{C}/\simeq is not a category. Of course, \mathcal{C}/\simeq is not a spm category. □

For the *lean*-support quotient $BG(\mathcal{K}) \stackrel{\text{def}}{=} \backslash BG(\mathcal{K}) / \cong$, we can get the similar conclusion.

3.2 The Quotients in Bigraphical Dynamics

The bigraphical dynamics are studied at the general level of s -categories. The corresponding theory was first developed for a concrete wide reactive systems (WRS), based on an s -category, and transferred finally to its quotient abstract WRSs based upon an spm category. There, the quotient wide s -category $C \stackrel{\text{def}}{\backslash} C / \equiv$, where \equiv is an abstraction on $\backslash C$, is a wide spm category. It gives rise to some problems. This brings us to our two problems.

Problem 1. *What conditions on a concrete wide s -category can make $C \stackrel{\text{def}}{\backslash} C / \equiv$ be a wide spm category?*

Problem 2. *What conditions on a concrete WRS $\backslash C(\mathcal{R})$ can make $C(\mathcal{R})$ be an abstract WRS $C(\mathcal{R})$?*

The similar question lies in transferring the transition system to the quotient abstract bigraphical reactive system (BRS), via the *lean*-support quotient functor. It turns out that we must impose some restrictions on the constructions of quotient categories.

4 Conclusions

Certain kinds of *category* are served to classify bigraphs and to develop some of their theory. Any useful experiments are those carried out with real applications, involving real users and an assessment of their experience. We argue that the bigraphical categories are not complete. Future work is to define precise formal models for bigraphical categories.

References

1. Milner, R.: The Space and Motion of Communicating Agents. Cambridge University Press, Cambridge (2009)
2. Birkedal, L., Debois, S., Elsborg, E., Hildebrandt, T., Niss, H.: Bigraphical models of context-aware systems. In: Aceto, L., Ingólfssdóttir, A. (eds.) FoSSaCS 2006. LNCS, vol. 3921, pp. 187–201. Springer, Heidelberg (2006). https://doi.org/10.1007/11690634_13
3. Tsigkanos, C., et al.: Ariadne: topology aware adaptive security for cyber-physical systems. In: IEEE/ACM 37th IEEE International Conference on Software Engineering (2015)
4. Benford, S., et al.: On lions, impala, and bigraphs: modelling interactions in physical/virtual spaces. ACM Trans. Comput.-Hum. Interact. **23**(2), 9 (2016)
5. Tsigkanos, C., et al.: On the interplay between cyber and physical spaces for adaptive security. IEEE Trans. Dependable Secure Comput. **15**(3), 466–480 (2016)
6. Dib, A.T.E., et al.: Specification and verification of reconfigurable multi-agent system architectures. Multiagent Grid Syst. **12**(2), 105–124 (2016)
7. Sary, C., et al.: System-of-systems support—a bigraph approach to interoperability and emergent behavior. Data Knowl. Eng. **105**, 155–172 (2016)

8. Barr, C., Wells, M.: *Category Theory for Computing Science*. Prentice Hall, Upper Saddle River (1990)
9. Milner, R.: *Bigraphical categories*. In: Bravetti, M., Zavattaro, G. (eds.) *CONCUR 2009*. LNCS, vol. 5710, pp. 30–36. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04081-8_3



A Distributed Data Collection System for Traffic Images

Wen Bo^{1,2}, Hongju Yang¹, Jiaojiao Xiao², Liangyan Li²,
and Changyou Zhang^{2(✉)}

¹ School of Computer and Information Technology, Shanxi University,
Taiyuan, Shanxi, People's Republic of China

² Laboratory of Parallel Software and Computational Science,
Institute of Software, Chinese Academy of Sciences,
Beijing, People's Republic of China
changyou@iscas.ac.cn

Abstract. With the development of intelligent traffic system, high-definition cameras are spread along the urban roads. These devices transmit real-time captured images to data center for multi-purpose usability, but these bring higher requirements on network and storage capacity of the traffic images collection system. To address these problems, we proposed a compressed representation method for traffic images and collection system architecture. Firstly, the method proposed in this paper designed a distributed data collection system for traffic images based on edge computing mode. Secondly, we studied on the image feature representation methods for vehicle type/version retrieval, and formed a compressed representation method based on structural relationships selections. In this method, the retrieval precision reaches to 97.78% with the recall ratio of 90%, which proved the usability in this image collection system. Finally, we set up an analysis model based on Petri-net to observe the system requirements on storage, computing and transmission with different setting parameters. This model is powerful on finding bottlenecks of system in early stage and keeping balance in multi-aspects. The simulation experiments show that the data volume needs to be transported and preserved was compressed to 1/2250 comparing to the method of original images and the system transport delay was reduced more than 1/9 of original method. The experimental result showed that compared with the original collection method, the amount of data to be transmitted and stored was compressed by 1/2250, and the system transmission delay of the system was reduced to 1/9.15. This distributed data collection method and system proposed in this paper provided a novel referable revolution for traffic images processing system in intelligent traffics.

Keywords: Traffic images · Data collection · Vehicle type retrieval · Edge computing · Petri-net

1 Introduction

In the dynamic environment of photographing traffic images, a large number of real-time, high-speed and uninterrupted data flows are generated at traffic checkpoints. As a result, the opportunities and problems are caused by data. According to Cai, scalable

storage, filtering and compression schemes are essential for efficient data processing [1]. If all data is dumped into the storage space, it will cause “data swamp” [2]. Liu Zilong and others explained a big data storage platform called “data Lake”. Its main idea is to uniformly store different types of original data in different fields, including structured data, semi-structured data and binary data, so as to form a centralized data storage set containing all forms of data [3].

Edge computing, which is on the side near the source of the object or data source, adopts an open platform integrating network, computing, storage and application core capabilities, which can provide services nearby [4]. For the Internet of things, multiple computing nodes distributed on the network can unload the computing pressure from the centralized data center, and can significantly decrease the waiting time in message exchange [5]. Each traffic image usually contains multiple vehicle targets. Target detection based on deep learning is mainly divided into target detection algorithm based on candidate region and target detection algorithm based on regression [6]. In 2014, Girshick proposed region CNN [7] target detection algorithm. In 2015, Girshick proposed Fast R-CNN [8] and Faster R-CNN [9]. In 2017, He Kaiming proposed Mask R-CNN [10] target detection algorithm based on Faster R-CNN framework. In 2018, the YOLO-V3 [11] algorithm improved the problem of poor detection accuracy of small targets detection through multi-level prediction. The data transmission process between devices uses the network for communication. In the scenario of industrial Internet, the realization of high-efficiency automation needs to complete real-time operation control. If some steps are delayed due to not receiving instructions in time, the service quality will be reduced and even the system will crash. Therefore, higher requirements are put forward for the delay, which needs to be between 1 and 10 ms [12–14]. Petri net model is used to simulate the branches of interaction in the system. It has rich system description means and system behavior analysis technology. The concept of net was first proposed in the dissertation of Dr. Petri [15, 16], which is the cornerstone of the development of Petri net theory.

Distributed data collection system for traffic images method is the basic requirement of improving data storage, data transmission and making full use of the computing power of edge nodes. This paper proposed a distributed data collection system for traffic images. The features of vehicle structure relationship are extracted by intelligent traffic checkpoint and are expressed as lossy compression. This method realizes the vehicle model retrieval under the specific scene-traffic image. It also realizes efficient the transmission of relevant data to all levels of communication information center storage. Finally, the rationality of traffic image distributed data collection method and the functionality of the system are verified by experiments.

2 The Framework of Traffic Images Collection System Based on Edge Computing

To reduce the load pressure of storage, transmission and computing brought by massive traffic data, a traffic image collection system based on edge computing was designed. By using Internet and intelligent devices deployed in traffic junctions to finish images

collection, edge computing and data transmission functions, and further achieve typical applications like vehicle model retrieval based on traffic images.

2.1 The Design of System Structure

The edge computing based on distributed data collection system for traffic images consists of image collection point, traffic communication center, data processing server and storage server, as shown in Fig. 1.

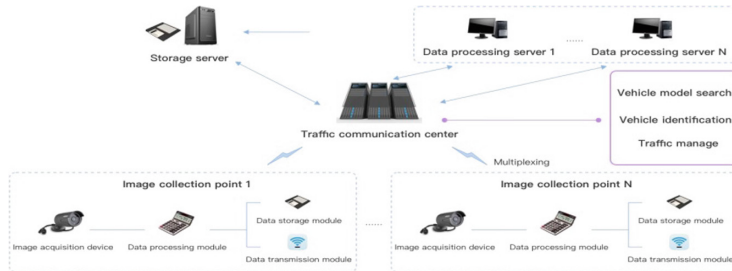


Fig. 1. Edge computing based on traffic images collection system

The deep learning neural network is embedded into the distributed image collection devices to improve the learning ability and reduce network traffic. The image collection point is the resource of traffic images, including data processing module, data storage module and data transmission module. Firstly, the HD camera can collect original traffic images, then use data processing module to achieve efficient object extraction and detection. The data processing module can transform the structural feature information into a lossy compressed representation text. Data transmission module uses network technologies like 5G and Ethernet to transport compressed representation text to network transmission data center in multiplex transmission. At the same time, the data storage module completed the storage function of text and images, and transmitted traffic images to the network transmission center for storage at idle time.

The platform of data transmission center has massive data computing servers and large data storage space. Data processing servers in network transmission center are used to compute, optimize and analyze the lossy compressed representation text; Data storage servers are used to storage traffic images and text information. By this platform, the recognition and retrieval of vehicle model can achieved, traffic scheduling and other typical applications.

2.2 System Features

The compressed representation method based on traffic images enabled the system to store more traffic images information in a same data storage size. With the emergence of the compressed representation method, the information transmitted can be greatly increased when the data transmission traffic is the same, and also greatly improved the

real-time transmission. The data collection of edge nodes is also based on the compressed representation method. Data is computed on edge nodes and transferred the processed data to the traffic communication center. Compare transferred original data to the cloud computing center and centralized processing, this method greatly saved network bandwidth and made sure edge computing capabilities are fully utilized.

The system is based on a hierarchical network structure, and data is transferred from the distributed storage nodes to the upper layer according to the tree structure to ensure the correctness of the data and improve the storage efficiency, as shown in Fig. 2.

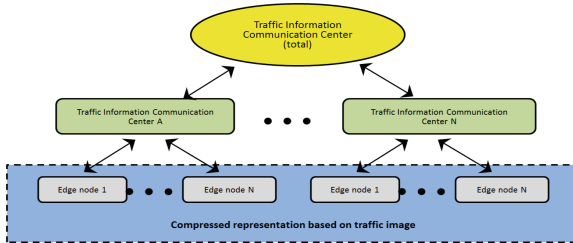


Fig. 2. The hierarchical network structure of system

The system has the distributed feature in both data collection and storage process. When the network bandwidth is poor, the edge nodes can still collect data and store in its data storage space to reduce the time wasted in data transmission process.

3 Compressed Representation of Traffic Images

The compressed representation of traffic images firstly extracts multiple vehicles from the original traffic images according to the edge node target. Then extract the effective structure information of multiple components from the target vehicle. Finally, it is represented as a text with vehicle structure information.

3.1 Data Format

The original traffic data collected by the edge node is a “.png” image with a size of about 2 M. After edge calculation, the target vehicle is a “.png” image with a size of about 500 KB. Finally, the image is represented as “.txt” text with size of about 200 bytes by traffic image compression representation.

3.2 Image Sub-target Extraction

Deep learning is applicable to edge computing environment and intelligent transportation [17]. Yolo-v3 neural network algorithm has the advantages of high precision and fast speed for small target detection, which is used as the function of target extraction in the traffic images in this paper.

Due to the complex background of the image taken by the intelligent traffic junctions, it may contain many kinds of objects. In order to extract the structural vehicle features to get the lossy compressed representation text, the single vehicle in the first step should be extracted. Firstly, use the original traffic images to train the YOLO-V3 neural network model to detect and extract vehicles quickly. As shown in Fig. 3, the target vehicle image extracted by the YOLO-V3 model throws away complex backgrounds and duplicate targets, reducing the storage space by about 75%.



Note: the license plate information is hidden

Fig. 3. Vehicle target extraction from original traffic image

Then extract the structural features of the vehicle images. After the edge calculation, the single vehicle target images realize the multi-component target detection by the YOLO-V3 neural network model, extracts the component structure information, and represents the traffic images information as text information, as shown in Fig. 4.

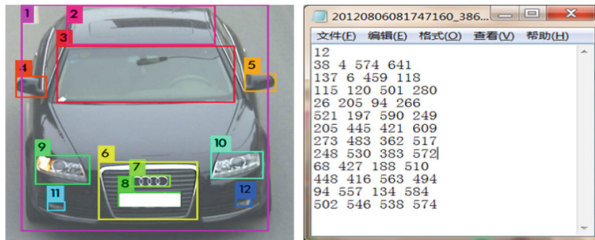


Fig. 4. Compressed representation of multi-part target extraction

Compressed representation text occupies about 200 bytes of storage space. Compared with the original images, the compressed representation of the image greatly reduces the storage space, providing new possibilities for data storage mode and fast data transmission in the future.

3.3 Deployment Requirements for Extraction Methods

Put forward the deployment requirements of validity and accuracy for the extraction method, so carry out validation experiments on the typical scenario of vehicle model retrieval. First of all, using the component pixels in the text to construct the structural

features of vehicle components, establish a vehicle structural feature model. Then, in order to improve the computational efficiency, filter out the invalid features by voting, and optimize the vehicle structural feature model. Finally, analyze the weight of the remaining features, establish the vehicle structure weighted feature model. The vehicle retrieval experiment results are shown in Fig. 5.

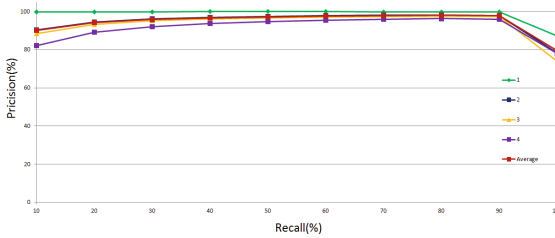


Fig. 5. Vehicle type retrieve P-R diagram

The 4 types of vehicle samples for vehicle type were used retrieve experiments. Among the several types of vehicles, the best results are the first type of vehicles, achieving an optimal precision rate of 99.83% when the recall rate is 90%. The fourth type of vehicle achieved an optimal precision rate of 95.89% when the recall rate was 90%. The average precision of the sample of the four types of vehicles is up to 97.78%. The experiment fully proves the validity and accuracy of the method.

4 Deployment of Traffic Images Compression Method

Based on big data and edge computing, our distributed data collection method for traffic images embedded deep learning neural networks in distributed collection image intelligent devices to improve learning performance and reduce network flow. With the migration of data in the system, the data transmission center is also changing. Therefore, a deployment way based on the traffic images compression method was established, as shown in Fig. 6.

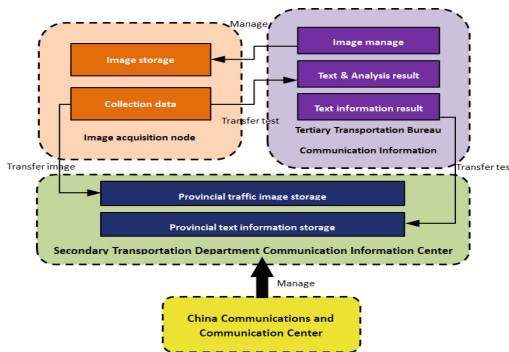


Fig. 6. Deployment way based on traffic images compression method

Firstly, extract the target images from the original traffic images obtained from the image collection node. Then, calculate the text data and transmitted the text data to the Tertiary Transportation Bureau Communication Information Center for calculation and storage. As well as the text data and analysis results were transferred to the Secondary Transportation Department Communication Information Center for preservation. After that, the target image data was transmitted directly from the edge node to the secondary unit. Finally, China Communications and Communication Center (level 1) can call all secondary storage. In this process, the tertiary traffic units do not save the image data, and the image data can be directly called from the collection point storage module, which will save the storage load pressure of the three-level unit.

5 System Simulation Verification Based on Colored Petri-Net

In order to verify the rationality and functionality of the distributed data collection method for traffic images, a colored Petri-net model for the whole system based on the data storage and transmission was established.

5.1 Petri-Net

Petri-net is suitable for describing asynchronous and concurrent computer system models. Petri nets have both strict mathematical expressions and intuitive graphical expressions. It has rich system description methods and system behavior analysis techniques [18, 19]. The definition of the Oriented Net in it is defined as 1.

Definition 1. Oriented Net.

$N = (S, T, F)$ is called oriented net, if and only if:

- (1) $S \cup T \neq \emptyset, S \cap T = \emptyset$;
- (2) $F \cap (S \times T) \cup (T \times S)$;
- (3) $\text{dom}(F) \cup \text{cod}(F) = S \cup T$, where, $\text{dom}(F) = \{x | \exists y : (x, y) \in F\}$, $\text{cod}(F) = \{y | \exists x : (x, y) \in F\}$ are the domain and value range of F respectively.

S is place set of N , T is transition set of N , F is flow relationship.

5.2 System Modeling Based on Colored Petri-Nets

In the model of distributed data collection, data transmission analysis needs to consider various factors. For example, image information and text information have different transmission timeliness. As well as, there are differences in the data storage space of information communication centers at all levels. Therefore there are differences in the types of storage data and the timeliness of calling storage data at different levels of information and communication centers.

The colored network system is a type of advanced Petri net that defines the token color to distinguish the types of resources which enhances its ability to describe the system [19, 20]. In the system, the storage nodes are mapped to places and the related parameters are mapped to places tokens in place. The different information

communication centers correspond to the different colors of tokens and the parameter information corresponds to the value of token, which are both important elements in traffic images based distributed data collection system.

The corresponding relationship of elements is shown in Table 1.

Table 1. The corresponding relationship of elements

Service value chain element	Petri-net element
Data transmission	Transition
Storage node in the system	Place
Related parameters	Token
Transmission control	Connection
Information and communication center	Token color
Parameter information	Token value

On the basis of the colored Petri-net, the control unit is added to represent the data storage, transmission control, information communication center scheduling, etc. The distributed data collection net system for traffic images is defined as 2.

Definition 2. Traffic images based distributed data collection system.

The necessary and sufficient condition for $\Pi = (P, T; F, C, K, D,)$ to be called a distributed data collection net system is:

- (1) $\sum = (P, T; F, C,)$ is colored network system
- (2) $t \in C, D(t)$ is the control function of Transition t
- (3) $p \in P, K(p)$ is the resource limit function of the Place p .

5.3 Construction of System Petri-Net Model

First, use CPN-tools to build the traditional traffic data collection system model, as shown in Fig. 7. The original image is usually transmitted by using the traditional model. Data are kept in traffic information centers at all levels. Although access time is not required, the transmission time is greatly increased.

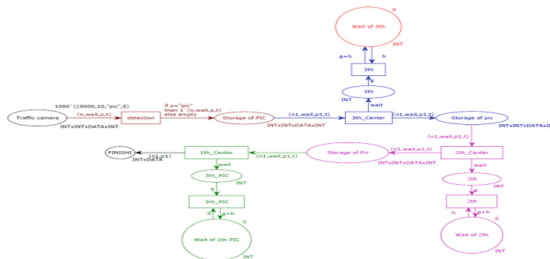


Fig. 7. Petri-net model of the traditional traffic data collection network system

The traffic cameras capture the original images and save them in the data storage node. Then, transfer the original data to the Tertiary traffic information and communication center for preservation and processing. After that, the data and results are transmitted to the Secondary traffic information and communication center for storage and use. If the primary center wants to use the data, data transmission will be required again. This method transmission not only wastes the data storage space and computing power of the intelligent traffic junctions, but also increases the data transmission duration and load, which causes the unnecessary expenses of establishing and maintaining data space of the traffic communication centers.

The storage and scheduling of data has been mentioned in the previous chapter. The Petri-net model of the distributed data collection system for traffic images Petri-net model of is shown in Fig. 8.

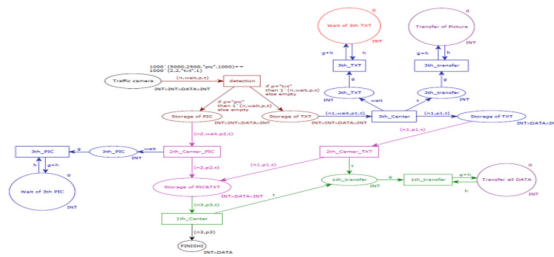


Fig. 8. The Petri-net model of the distributed data collection system for traffic images

The Petri-net model of the distributed data collection system for traffic images solves the problem of information island between multi-level traffic communication centers reduces the maintenance cost of the large-capacity data space in transportation units, and avoids the repeated establishment of storage space. As well as, the method solves the wastage of computing resources in the edge nodes and ensures that the centers at all levels make full use of the optimal data space to complete the tasks of upstream and downstream collaboration.

5.4 Experimental Environment and Parameter Settings

The experiment simulates the runtime system model on CPN Tools 4. 0. 1. CPN Tools support the standard ML language and provide basic data type definitions, data operation descriptions, etc., so as to build a concise parametric mathematical model. In the experiment, defined the range of values of data, detected the duration of the transmission and call of each Token record, and verified the effectiveness of the distributed data collection method for traffic images. The descriptions, types and abbreviations of the main parameters defined in this paper are shown in Table 2.

Table 2. Descriptions of the main parameters

Description	Type	Abbreviation
data size	int	n
data transmission duration	int	wait
data type	string	p
data call duration	int	t
traffic communication center time	int	g
iteration time	int	h
data file type	string	pic,txt

5.5 Experimental Data

The traditional model of traffic data collection net system and our model of the distributed traffic data collection net system are tested in the 20 M Ethernet network environment. Experiment tested 1000 original traffic images data with a size of 2 MB by using the traditional system model, and obtained the results of transmission duration and storage space. As a contrast, 1000 targets extraction vehicle images with a size of 450 KB and 1000 compressed representation texts of images with a size of 200 bytes were tested, and obtained the experimental results of transmission duration, scheduling time and the size of storage space.

5.6 Result Analysis

In the experiment of verifying the rationality of the traffic images distributed data collection method and the function of the system, implemented node functions through different methods of data transmission, storage and scheduling. Expected results are mainly in three aspects as follows. From the perspective of data storage, the data collection methods proposed can greatly reduce storage space and waste of resources. From the perspective of the total time of traffic communication center, the traditional method data scheduling transmission takes much longer than the method designed. From the perspective of cost, the data collection methods proposed can save a lot of cost in data space establishment and maintenance. The results are shown in Fig. 9 below.

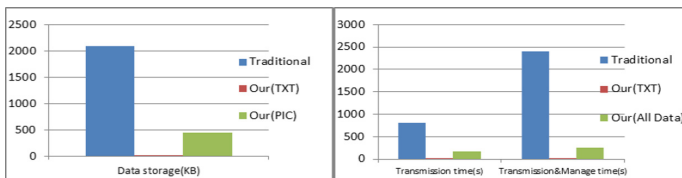


Fig. 9. Comparison of experimental results

Experiment took 1000 images from the camera in the intelligent transportation checkpoint, and transmitted and dispatched them in the 20 M Ethernet network environment. There are some main network parameter settings. Because there is no decimal definition in CPN-Tools, set the parameter n_1 representing the original data size to 20970, the parameter n_2 representing the storage size of the target extraction vehicle image is 4500, and the parameter n_3 representing the size of the compressed description of traffic image is 2. Again, set wait: $wait_1 = 800$, $wait_2 = 175$, $wait_3 = 78$. And set t : $t_1 = 0$, $t_2 = 87$, $t_3 = 39$. It should be noted that $wait_3$ and t_3 are both in microseconds, and the other parameters are in milliseconds.

Compared with the traditional method, this method proposed reduces the storage space of the original image by 10485 times and the storage space of the target extracted by the vehicle image by 2250 times. The node transmits compressed text about 78 ms long, which is 10256 times shorter than the original image transmission time. And compared with the total time of three-level traffic communication center is 2400S in the traditional method, the total time of single vehicle image transmission and data scheduling is about 262.2 s in our method, which is about 9.15 times shorter. Compared with the traditional method, the distributed data collection method for traffic image greatly decreases the size of data storage space, reduces the transmission time of data scheduling and the pressure of communication load, and saves the cost of establishing and maintaining the data space. The rationality of the distributed data collection method and the functionality of the system are proved by simulation experiments.

6 Conclusions and Prospects

This paper verified the rationality of the distributed data collection method and the functionality of the system from the perspective of data form, storage and transmission, designed the data storage and transmission collaboration scheme of traffic communication center, optimized the traffic data collection method. And we simulated the process of data storage and transmission, and then analyzed the experimental results. The experimental results show that collection method for traffic images greatly save the data communication bandwidth, and the computing power of the edge node is fully utilized. Moreover, the size of data storage space is greatly reduced while we can effectively retrieve the vehicle models. And the data transmission duration and the communication load pressure are also reduced. Based on this method, in the future this method can be used for the detection of image structure similarity, image recognition and retrieve, urban planning, smart transportation and other big data storage and application from Internet of Things in distributed scenarios. However, there are still some shortcomings that need to be further improved. For example, there are few types of vehicle retrieval in data sets, and few network parameters designed in the system. The multi-classes vehicle retrieval and network parameter expansion is the next research direction of this paper.

Acknowledgment. This paper is supported by the Natural Science Foundation of China (61672508, U1636213). The authors also would like to express appreciation to the anonymous reviewers for their helpful comments on improving the paper.

References

1. Cai, H., Xu, B., Jiang, L., et al.: IoT-based big data storage systems in cloud computing: perspectives and challenges. *IEEE Internet of Things J.* **4**(1), 75–87 (2016)
2. Hai, R., Geisler, S., Quix, C.: Constance: an intelligent data lake system. In: *Proceedings of the 2016 International Conference on Management of Data*, pp. 2097–2100. ACM (2016)
3. Miloslavskaya, N., Tolstoy, A.: Big data, fast data and data lake concepts. *Procedia Comput. Sci.* **88**, 300–305 (2016)
4. Zhang, K.Y., Gui, X.L., Ren, D.W., Li, J., Wu, J., Ren, D.S.: Survey on computation offloading and content caching in mobile edge networks. *Ruan Jian Xue Bao/J. Software* **30**(8), 2491–2516 (2019). (in Chinese). <http://www.jos.org.cn/1000-9825/5861.htm>
5. Ji Rui, L.I., Xiao Yong, L.I., Gao, Y.L., et al. Review on data forwarding model in Internet of Things. *J. Software* 2018
6. Pei, W., Xu, Y.M., Zhu, Y.Y., Wang, P.Q., Lu, M.Y., Li, F.: The target detection method of aerial photography images with improved SSD. *Ruan Jian Xue Bao/J. Software* **30**(3), 738–758 (2019). (in Chinese). <http://www.jos.org.cn/1000-9825/5695.htm>
7. Girshick, R., Donahue, J., Darrell, T., Malik, J.: Rich feature hierarchies for accurate object detection and semantic segmentation. In: O’Conner, L., (ed.) *Proceedings of the 2014 IEEE Conference on Computer Vision and Pattern Recognition*, pp. 580–587. IEEE Computer Society, Columbus (2014)
8. Girshick, R.: Fast R-CNN. In: O’Conner, L. (ed.) *Proceedings of the 2015 IEEE International Conference on Computer Vision*, pp. 1440–1448. IEEE Computer Society, Santiago (2015)
9. Ren, S.Q., He, K.M., Girshick, R., Sun, J.: Faster R-CNN: towards real-time object detection with region proposal networks. *IEEE Trans. Pattern Anal. Mach. Intell.* **39**(6), 1137–1149 (2017)
10. He, K.M., Gkioxari, G., Dollár, P., Girshick, R.: Mask R-CNN. In: O’Conner, L., (ed.) *Proceedings of the 2017 IEEE International Conference on Computer Vision*, pp. 2980–2988. IEEE Computer Society, Venice (2018)
11. Redmon, J., Farhadi, A.: YOLOv3: an incremental improvement. <https://arxiv.org/abs/1804.02767>
12. Fettweis, G., Boche, H., Wiegand, T., et al.: *The Tactile Internet-ITU-T Technology Watch Report*. ITU, Geneva (2014)
13. Wang, B., Zhang, X., Wang, G., et al.: Anatomy of a personalized livestreaming system. In: *The 2016 Internet Measurement Conference*, pp. 485–498. ACM (2016)
14. Liang, G., Liang, B.: Balancing interruption frequency and buffering penalties in VBR video streaming. In: *IEEE International Conference on Computer Communications*, pp. 1406–1414. IEEE (2007)
15. Du, S., Wu, P., Wu, G., Yao, C., Zhang, L.: The collaborative system workflow management of industrial design based on hierarchical colored petri-net. *IEEE Access* **6**, 27 383–27 391 (2018)
16. Zhao, J., Chen, Z., Liu, Z.: Modeling and analysis of colored petri net based on the semi-tensor product of matrices. *Sci. China Inf. Sci.* **61**(1), 01–05 (2018)

17. Zhou, Z., Liao, H., Gu, B., et al.: Robust mobile crowd sensing: when deep learning meets edge computing. *IEEE Network* **32**(4), 54–60 (2018)
18. Mahato, D.P., Singh, R.S.: Load balanced scheduling and reliability modeling of grid transaction processing system using colored petri nets. *ISA Trans.* **84**, 225–236 (2019)
19. Chen, H., Wu, N., Li, Z., Qu, T.: On a maximally permissive deadlock prevention policy for automated manufacturing systems by using resource-oriented petri nets. *ISA Trans.* **89**, 67–76 (2019)
20. Van Der Aalst, W.M.P.: Three good reasons for using a Petri-net-based workflow management system. In: *Proceedings of the Information and Process Integration in Enterprises*, pp. 179–201 (1996)

CyberDI 2019: Cyber and Cyber-Enabled Intelligence



Robot Path Planning in Dynamic Environments Based on Deep Reinforcement Learning

Yu Han, Yu Guo, Zhenqiang Mi^(✉), and Yang Yang

University of Science and Technology Beijing, Beijing, China
g20178660@xs.ustb.edu.cn , mizq@ustb.edu.cn

Abstract. Path planning in dynamic environment has been the hot research direction. This paper considers a new dynamic environment—the obstacles are randomly distributed in the environment, and all of the obstacles will be distributed randomly again after robot's movements. In the new dynamic environment, traditional path planning methods have some shortcomings when facing the dynamic environments. The traditional path planning algorithms need to re-calculate the path once the environments change, which is a very time consuming process. The deep reinforcement learning (DRL) model is a single-step algorithm, so the dynamic environments will not affect its running time consumption, which is superior to the traditional path planning algorithms in terms of running time consumption. However, the DRL model will face the problem of sparse rewards in the path planning problem due to the large state space of the environments. This paper uses DRL to solve the shortcomings of traditional path planning algorithms in dynamic environments and we propose a new framework to solve the problem of sparse reward in robot path planning. The framework uses a new strategy searching algorithm and a new shaped reward function. The improved framework can effectively solve the convergence problem in path planning. According to the simulation results, in the stochastic dynamic environments, the running time consumption of the new framework is less than the traditional path planning algorithm, and the new framework is better the classic DRL model in training results and planning results.

Keywords: Path planning · Deep reinforcement learning · Sparse reward problem

1 Introduction

The path planning of mobile robots is an important part of robot navigation, and it is the basis and premise of various research applications of robotics. The path planning task requires the mobile robots to find a no-collision path from the start point to the goal point in the environments with obstacles, this path must meet the artificially evaluation criteria [1]. With the development of mobile

robots, the application fields of mobile robots are more and more extensive, and different scenarios impose different requirements on the path planning of mobile robots.

With the combination of robot technology and artificial intelligence technology, robots are gradually developing in the direction of artificial intelligent, and the robots are increasingly equipped with the ability to finish the tasks in place of humans in certain specific situations such as high temperature operations [1]. Among the various tasks, the environments in which mobile robots work is most likely the dynamic and complex environments. If traditional path planning algorithms are used, the changing environments greatly increases the running time consumption of the algorithm [2], and we do not want the robot to waste too much time on the running time of the path planning algorithm. Therefore, it is a very good choice to use the deep reinforcement learning(DRL) model to carry out the path planning problem of the robot [3]. The DRL model can plan the path in single-step according to the environmental information, which can reduce the running time consumption of the algorithm. The DRL model processes the environment states as input and outputs the actions that the agent needs to perform. Then the model will evaluates the results so that the model can take the “good” actions and avoid the “bad” actions in the next planning [4].

There are some challenges need to be tackled in order to apply deep reinforcement learning to path planning.

- (1) Although the DRL model can guide the agent to complete the artificially task, in the path planning problem, how to extract the coordinate information of each obstacle from the input information is the problem should to be solved.
- (2) In the new dynamic environments proposed in this paper, the state space that the model needs to process is extremely huge. This can result in the agent not being able to find the “effective” experience during the training process. This is the reward sparse problem that needs to be solved in deep reinforcement learning.

In this paper, we use convolutional neural networks to preprocess environmental information. The convolutional neural networks are widely used in computer vision and have powerful ability to process pictures. Then, we propose three measures to solve the sparse reward problem, including improved exploration-exploitation algorithms, shaped reward function and new model combined with hindsight experience replay idea [5].

The main contributions of our work can be summarized as follows:

- (1) Solve the problem that the traditional path planning algorithms waste too much time on computation in the new dynamic environment proposed in this paper. We use a new DRL model to do the path planning in the stochastic dynamic environments, which take less computing time than the traditional methods.
- (2) Improve the DRL model based on path planning. Solve the problem of sparse rewards generated by the DRL model in the path planning problem, so that

deep reinforcement learning can effectively carry out path planning in the dynamic environments. Compared with the traditional deep reinforcement learning algorithm, the proposed model has obvious improvement in convergence speed and planning results.

The rest of this paper is organized as follows. The related work is introduced in Sect. 2, Sect. 3 introduces the formulation of path planning problem and the network model. Our improved algorithm is detailed in Sect. 4. Experimental results are included in Sect. 5. Finally, Sect. 6 concludes the experiment.

2 Related Work

Path planning is a very common research direction in computer science. Both A* algorithm and Dijkstra algorithm are classic path planning algorithms, and there are many improved algorithms based on them. In 2002, Shan Lan proposed an A* algorithm with a smart heuristics. Researchers calibrate A* algorithm based on many large path planning data set [6]. Because the traditional A* algorithm do not use any good heuristics, they spend much time to calculate. And researchers ascertain superiority of the proposed algorithm to the classic A* and Dijkstra algorithms by two kinds of extremely different path planning data sets. In the field of dynamic path planning, Kitamura Y proposes an simple method for finding a no-collision path for robot in dynamic environments. The new algorithm uses an octree for representing objects, so it can easily be accelerated by using parallelization techniques [7]. The experimental results prove that this simple method is time-saving and effective.

Reinforcement learning was proposed a long time ago. Scientists have been studying how to apply it to various fields. Volodymyr Mnih and Koray Kavukcuoglu proposed a new deep reinforcement learning model in 2013, using reinforcement learning to successfully learn strategy control in high-dimensional input space [8]. In the past, researchers often used expertly feature functions and strategies to achieve convergence of the reinforcement learning algorithm. Obviously, the traditional reinforcement learning system relies heavily on the expert's feature signature, which leads to reinforcement learning that cannot be widely applied. The model uses the deep convolutional neural networks as deep learning network and uses Q-Learning for policy training [9]. The researchers deployed the model in seven different Atari 2600 games and got better performance than all traditional methods. The DRL model performed very well and even surpassed human expert players in three games.

Deep reinforcement learning in the combination of reinforcement learning and deep learning, and sparse reward problem is a important part of deep reinforcement learning model. In 2017, Deepak Pathak and Pulkit Agrawal proposed a method of using curiosity-driven network to encourage agents to explore the environments [10]. Through the process of exploring the environments in the agent, the network gives the agent a certain degree of reward when the agent discovers new things. The researchers used the prediction error of the forward model in

the new environment as an additional feedback signal in addition to the sparse reward. This feedback signal can be used to encourage the agent to explore the area of the state space location. In 2018, Max Jaderbeg and Volodymyr Mnih proposed a method of setting some auxiliary tasks to help train agents [11]. Researchers combined reinforcement learning with unsupervised auxiliary tasks which significantly improved the learning efficiency of agents. The researchers built a 3D maze that allowed the agent to find the target in the maze. Instead of using these sparse rewards, the researchers used three additional reward signals to speed up the entire training process. The three reward signals are: pixel control, reward prediction, and evaluation function playback. Experiments prove that the setting of these three auxiliary tasks can effectively accelerate the training process of the agent.

There are some researches try to solve the dynamic path planning through DRL model too. In 2018, Panov and Aleksadr apply deep reinforcement learning on grid path planning. Their experiments proof that agent using neural q-learning algorithm robustly learns to achieve the goal in the small map [12]. And in 2018, Lei Xiaoyun apply the DRL model to the dynamic path planning. The researchers set some moving obstacles as the dynamic environment and use the double q-network as the training model. The experimental results show that the DQN can find the right path in this dynamic environments [13].

At present, some researcher have applied deep reinforcement learning to dynamic path planning. However, their dynamic environment space is not particularly large, so there is not much advantage compared to the traditional methods. In this paper, The dynamic environment that the obstacle distribute randomly is a larger state space than the environments above. We will improve the classic DRL model and compare to the traditional methods and classic DQN in the stochastic dynamic environments. Besides, we will improve the efficiency of path planning by using DRL model and solve the problem of sparse reward that appear in the planning process. Specifically, we hope the improved DRL model can reduce the computation time and improve the efficiency in the stochastic dynamic environments.

3 Problem Formulation and System Model

In this section, we will first briefly introduce the problem that will be solved in this paper and the system models of the path planning problem.

3.1 Problem Formulation of Robot Path Planning

This paper discusses the path planning problem of mobile robots in a new dynamic environment. In this dynamic environments, the environment states change randomly after each movement of the mobile robot. Therefore, the traditional path planning algorithms need to recalculate after the environments change, which will take too much time on calculations. The DRL model can output the next action in the face of the dynamic environments due to the Markov

property of the model which takes less time on calculations [14]. However, in the dynamic environments, because the obstacles are randomly changing, the experimental environments are a very high-dimensional state space, so the sparse reward problem of reinforcement learning model is very serious [15, 16]. What we need to solve is the problem of sparse reward generated by mobile robot's path planning in the dynamic environments. The primary models' notations are shown in Table 1.

Table 1. Formulation notations of path planning model

Symbol	Description
s	The environment state at current time
a	Action the agent will perform
r	Feedback after the action is performed
$V(s)$	Value-state function
$Q(s,a)$	Value-state-action function
π	The strategy that agent take
λ	Discount factor

Reinforcement learning model is based on Markov decision process. The Markov process means that the model's next state only depends on the current state and the current action [17]. In this section, this paper will introduce the basic network structure of the deep reinforcement model. Then, the improved algorithm which can solve the sparse reward problem will be described. We use the value function to describe the value of each state in the process. The value of the current state is related to the value of the next state and the feedback of the current action. We use Bellman equation to estimate the value function, and the function is shown as follows.

$$V(s) = E[R_{t+1} + \lambda v(S_{t+1}) | S_t = s] \quad (1)$$

Considering that each state has different actions to choose to execute, we will pay more attention to the action which agent take in the last state. So our value-action function is defined as follows:

$$Q^\pi(s, a) = E[r + \lambda Q^\pi(s', a') | s, a] \quad (2)$$

But the problem we have to solve is a model-free question, we can't calculate the values of next states through state transition probability matrix. So we use the time-difference method to solve the path planning problem, and we use the time-difference error to update our value-action function. The update formula is shown below:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha(R_{t+1} + \lambda \max Q(s_{t+1}, a) - Q(s_t, a_t)) \quad (3)$$

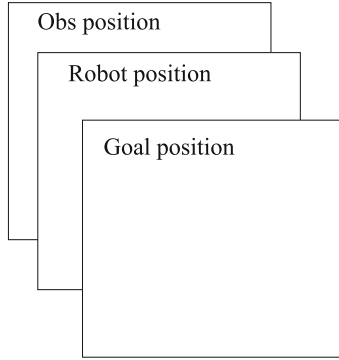


Fig. 1. The layer structure of map

We should make the deep reinforcement learning network constantly update the parameters of the function until the value-action function eventually converges. According to this function, we can get the optimal action that the agent needs to perform in current state.

3.2 The Network Structure of Deep Learning Model

(1) The Dueling Deep Network Structure

The basic network model used in this paper is the deep q-learning network with deuling ideas. deuling-based deep q-learning network can greatly improve learning efficiency and speed up convergence [18]. We select the convolutional neural network to handle the input images. The map we use can be represented by a matrix of $12 \times 12 \times 3$ units, where the first layer represents the location information of obstacles, the second layer represents location information of the agent, and the third layer represents the destination of the path planning [19, 20]. Each unit is expanded to a 7×7 pixel color block so that our input image size is $84 \times 84 \times 3$ pixels. The map information is shown in Fig. 1.

The input information of our deuling deep q-learning network includes: location information of obstacles on the map, location information of the robot, and location information of the destination. The input image sized as $84 \times 84 \times 3$ is outputted through the four-layer convolutional neural network and outputs a vector sized as $1 \times 1 \times 512$. Then the output data will be split into the advantage head and the value head in a 2:3 ratio in the fully connected layer. The value of the original output represents the Q value of each action. We divide the Q value into the following two parts:

$$Q(s, a; \theta, \alpha, \beta) = V(s; \theta, \beta) + A(s, a; \theta, \alpha) \quad (4)$$

We artificially divide the output value into two partial outputs, and then input the two parts into different fully connected layers, each with its own weight and bias. The network structure is shown is Fig. 2.

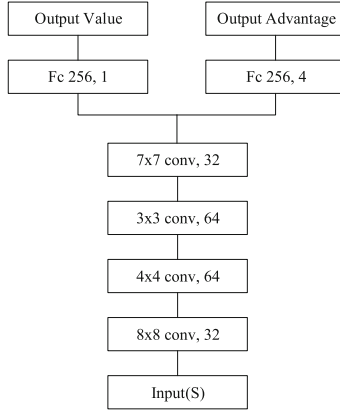


Fig. 2. The structure of network

(2) The Double Deep Q-Learning Network Structure

This paper chooses the double deep q-learning network as the primary algorithm of path planning. Because the deep q-learning network is based on the q-learning algorithm, the Q value calculated by the q-learning algorithm will have an issue of overestimation, and the double deep q-learning network can solve this problem [9]. Double DQN and DQN have the same network structure. These two algorithms are different in the way of calculating target Q. The update formula of Double DQN is as follows:

$$Y_t^{DoubleDQN} = R_{t+1} + \gamma Q(S_{t+1}, \operatorname{argmax} Q(S_{t+1}, a; \theta_t), \theta_t^-) \quad (5)$$

The training process of the network is shown in the Fig. 3.

4 Improvement of New Double Deep Q-Learning Network

In the training process of deep reinforcement learning, there is a widespread problem—sparse reward problem. Reward is a very important part of the DRL model. The training of DRL model, adjustments of parameters and so on all require reward values as input parameter [3]. Our agent takes random actions to explore the experimental environments during the training process. If the agent takes the correct action which can accomplish the task, then we will give the agent a certain reward value. This reward value will be used to update the Q value in q-Learning. However, in real life, the tasks we set often tend to be like this: the intelligent agent explores the experimental environments very hard, but no matter how much time the agent takes, the intelligent agent can't find the correct actions. In other words, if we don't interfere the process of training, the agent will never get a positive reward, which is the problem of sparse rewards.

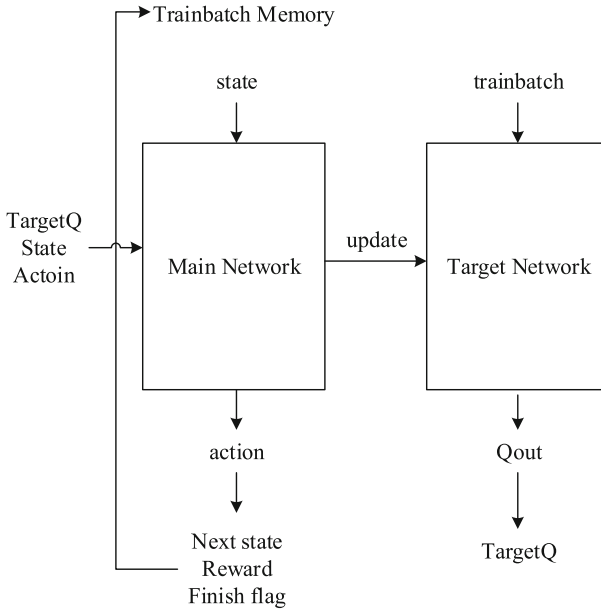


Fig. 3. The structure of double DQN

The sparse reward problem affects the training efficiency and training results of the DRL model. When the reward is severely sparse, the training results of the DRL model are wrong decision.

There are sparse reward problem in the experiments in this paper too. Our map is a 20×20 grid map with start point, goal point and 30 obstacles randomly distributed in the map. The state space size of this environment is $C_{20 \times 20}^{30}$. If we use the classic double deul deep q-learning network, the rewards will become very sparse and we will not get the desired results. In order to solve the sparse reward problem caused by DRL model in robot path planning, This paper adopts the following three measures:

- New exploration-exploitation strategy search algorithms based on weight sorting.
- Shaped reward function for path planning.
- Improved algorithm model with Hindsight Experience Replay idea.

4.1 Exploration-Exploitation Strategy Search Algorithm

The training of reinforcement learning includes the exploration phase and the exploitation phase. The exploitation means that the agent makes the best choices through the network model according to the input information; The exploration phase means that the agent makes other random decisions based on the search strategy to gather more experiences. These two phases are important factors

influencing the performance of the reinforcement learning algorithm. We need to balance the relationship between exploration and exploitation. Too much exploration creates redundant useless experience, which leads the agent to learn “wrong knowledge”; Excessive exploitation will make the training results of the agent fall into local optimum. The most commonly used search strategies are greedy strategy, ε -greedy strategy and bolzmann search strategy.

(1) The ε -greedy strategy

The ε -greedy search strategy is a very classic and commonly used strategy. It is improved from the greedy search strategy and is currently widely used in DRL model. The ε -greedy strategy determines the current choice by comparing a random number with ε , in this way, although the agent maybe can not choose the right action, “exploratory” can gather some new experiences for the experience pool [14]. The specific algorithm is shown in Algorithm 1.

Algorithm 1. ε -greedy Strategy

```

1: Randomly generate probability  $p$ , where  $0 < p < 1$ ;
2: if  $p < \varepsilon$  then
3:   Randomly generate an action  $a$ ;
4: else
5:    $a = \operatorname{argmax}(Q(s, a))$ 
6: end if

```

The ε -greedy search strategy algorithm is simple and practical, but it only considers whether the current action is the most beneficial and is easy to fall into local optimum. In addition, in the path planning environments of this paper, due to the huge state space, the ε -greedy search strategy search efficiency is very low, which resulting in slower training rate and bad training results.

(2) The improved search strategy

In this paper, we propose an improved search strategy in order to overcome above problem. The strategy mainly improves the algorithm from two aspects, one is the choice of actions in the algorithm, and the other is the sample selection from the experience pool.

The agent actually has uncertainty about its own actions selection during the training process. In the model of reinforcement learning, the distribution of weight values affects the distribution of actions selected. In general, we use the Bayesian Probability Network to calculate the action to be taken, but if we use the probability network with dropout, we obtain the approximate task of simulating Bayesian sampling when we obtain the experience. The improved search strategy algorithm is shown in Algorithm 2.

With the support of the search strategy, the agent makes action a in the current state s , and then can get the next state s_1 , feedback r and completion

Algorithm 2. The Improved Search Strategy Algorithm

```

1: Randomly generate probability  $p$ , where  $0 < p < 1$ ;
2: if  $p < \varepsilon$  then
3:   Randomly generate an action  $a$ ;
4: else
5:    $a = \text{tf.nn.softmax}[\text{argmax}(Q(s, a))]$  with dropout
6: end if
7: Put  $\{s, a, s_1, r, d\}$  into the experience pool

```

flag d , we call $\{s, a, s_1, r, d\}$ as an experience, This experience will be stored in the experience pool. In the experience replay, a certain number of experience is randomly selected from the experience pool for network training. In the path planning environments of this experiment, because of the huge state space, there will be a lot of experience with a reward of 0. If you randomly extract experience to form a training batch, the network may get a lot of “useless experience” with zero reward. To solve this problem, we assign weights to each experience and perform “pseudo-random extraction” based on weights. The size of the weights is related to the influence of each experience on network training. However, the sorting algorithm will consume some time, so we can’t choose experience based on weights all the time. We only need to let the agent quickly find the “influential” experience in the early stage of training. Therefore, the improved algorithm combines the idea of ε -greedy, and only uses the weight sorting to select the experience when the random number is less than ε . The value of ε will gradually increase with the training process, and finally approach to 0.999, which ensures that the selection of experience is independent. The improved experience sampling algorithm is shown in Algorithm 3.

Algorithm 3. The Improved Experience Sampling Algorithm

```

1: Randomly generate probability  $p$ , where  $0 < p < 1$ ;
2: if  $p < \varepsilon$  then
3:   Sort experience by absolute value of reward
4:   Calculating the baseline probability,  $Prob = \eta^i$ ,  $\eta$  is unusual sample factor
5:    $p = Prob / \text{sum}(Prob)$ 
6:   Select samples according to the probability distribution of  $p$ 
7: else
8:   Select samples randomly
9: end if

```

4.2 Shaped Reward Function Based on Path Planning

The reward function is one of the most important factors affecting the effect of reinforcement learning. The artificially reward function will directly affect the model’s training results. Some inappropriate reward functions not only make

the DRL model training converge slowly, but even can not converge to the optimal value; and the excellent reward function will be different according to the environments and experimental requirements. Traditional reinforcement learning, such as q-learning, generally gives a larger positive reward to the action that reaches the target state; unreasonable states such as hitting an obstacle or out of bounds will have a negative value, and in other irrelevant states the bonus value will be set to zero. In the path planning environments, according to the traditional q-learning reward function, our reward function is expressed as follows:

$$reward = \begin{cases} +1 & \text{if agent arrives the goal point} \\ -1 & \text{if agent reaches the obstacles} \\ 0 & \text{other situation} \end{cases} \quad (6)$$

In robot path planning problem, there are too many states in the state space. During the training, the agent will take a lot of “useless actions” with a reward of 0. So it is very difficult for the agent to reach the target point. We believe that the traditional q-learning reward function does not motivate the agent to move towards the destination in the path planning problem, or in other words the traditional reward function setting is not instructive.

We should design a suitable and inspiring reward function. This paper use state potential values to represent the agent’s “attitude” to a state (indicating whether the agent wants to tend or stay away from a certain point). The state potential value is obtained from the output value in the duel network. We first find the state potential of each point in the fixed map (the starting point in the map and the obstacles will not change), the map is a grid map with concave obstacles which is shown in Fig. 4.

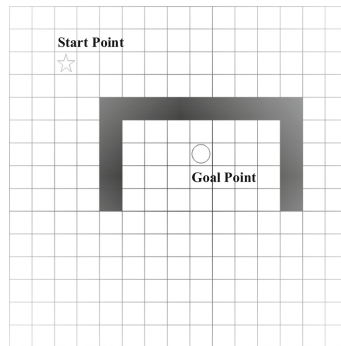


Fig. 4. The gridmap

After model training, the agent can find a stable path from the start point to the target point. We can also find the points’ state potential in the map. We can find that the state potential near the target point is also higher than other places,

and the area where the obstacle is located is the area with lower state potential. It can be known from the above experiment that the agent tends to approach the target point and away from the obstacle area. And the closer to the target point, the larger the state potential value is. Also the closer to the obstacle state, the smaller the potential value is. The state potential value represents the value of the state of the model output. The experiment provides us with evidence that the agent does respond to the environments as we intuitively expect. So we set the reward function as follows:

$$Reward = \alpha e^{\frac{D}{d_1}} + \beta e^{\frac{D}{d_2}} \quad (7)$$

In the above formula, d_1 is the distance between the agent and the target point. d_2 is the distance between the agent and the nearest obstacle. And D is the diagonal length of the map. α and β are discount factors. In addition, in order to make the agent arrive the destination faster, we will give each step a reward of -0.1 , which will avoid the agent not moving forward.

4.3 Hindsight Experience Replay for Path Planning

Hindsight Experience Replay (HER) is to solve the problem that the deep reinforcement learning does not converge when the model deals with the sparse environments. HER is based on the idea of universal value function approximators [5]. When we started an episode training, we were able to know the goal that the current episode needs to complete, that is, our input information has more than the status s , and there is also a target g to be completed. Thus our strategy is expressed as an action selected based on state s and target g : $\pi(a|s, g)$. Since the target g is added to the input, the bonus function also needs to be rewritten as $r(s, a, g)$. Therefore, our reinforcement learning becomes multi-objective reinforcement learning. When we want to complete multi-target training, the model will sample each trajectory of the agent, and then select different targets to make the reward becomes positive. Therefore, the trajectory with a reward of 1 in HER's experience replay buffer is increased, so that our agent can train more effectively in the environments of sparse rewards.

The HER idea is as follows: The agent interacts with the experimental environments under the guidance of the current policy to obtain the track t , and then stores the track $t\{s, a, r(a, s, g), s_1, g\}$ in the experience replay buffer. Then select another goal that can make the track's reward improved. The new track is stored in the experience replay buffer, then the buffer will be sampled and trained. The specific algorithm combining the HER idea is shown in Algorithm 4:

The HER algorithm is a time-consuming algorithm. Our goal is to make the agent find the useful experience quickly, so we only let the HER intervene in the early stage of training to help the agent find the right samples faster. This function is controlled by the HER flag.

Algorithm 4. improved DQN with HER

```

1: Initialize experience buffer R and HER flag  $f$ 
2: for  $epoch \in [1, E]$  do
3:   for  $cycle \in [1, C]$  do
4:     for  $episode \in [1, N]$  do
5:       Initial and process goal  $g$  and an initial state  $s$ 
6:       Initial episode buffer  $B$ 
7:       Use strategy search algorithm pre-train model
8:       for each  $t \in [0, T]$  do
9:         if  $f < \varepsilon$  then
10:          Get  $\{s, a, r, s_1, g\}$  from episode buffer  $B$ 
11:          Concatenate  $s, s_1$  and  $g$  get new input  $[s, g]$  and  $[s_1, g]$ 
12:          Add trajectory  $t \{[s, g], a, r, [s_1, g]\}$ 
13:          for each  $k \in [0, K]$  do
14:            Get  $g_1$  from episode buffer
15:             $r_1 = r(s, a, g_1)$ 
16:            Add trajectory  $t \{[s, g_1], a, r_1, [s_1, g_1]\}$ 
17:          end for
18:        end if
19:      end for
20:    end for
21:    for each  $t \in [0, N]$  do
22:      sample training batch from experience buffer
23:      train the deep Q-learning network
24:    end for
25:  end for
26: end for

```

5 Experimental Simulations

5.1 Experimental Environments

In the research of mobile robot path planning problem, there are two main ways to represent the environments of the state space: geometric mode and topological mode [1]. In this paper, we use geometric patterns to represent the path planning environment. The geometric patterns represent the map in the form of a grid. The map sample is shown in Fig. 5.

A total of 62 unit points with 60 obstacles, start point and target point were randomly distributed in a 20×20 grid, for a total of C_{400}^{62} different map environments. In the dynamic environments, the map environments change randomly after each step of the agent's actions, which means that after each movement, the traditional path planning algorithm needs to recalculate the path.

5.2 Parameter Setting

The network parameters are set as Table 2:

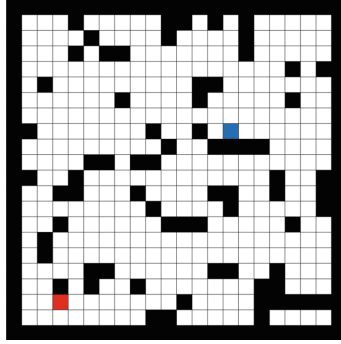


Fig. 5. The map environment

Table 2. Parameter setting of network

Convolution layers	Output size	Kernel size	Stride	Padding
The 1st layer	32	[8, 8]	[4, 4]	VALID
The 2nd layer	64	[4, 4]	[2, 2]	VALID
The 3rd layer	64	[3, 3]	[1, 1]	VALID
The 4th layer	512	[7, 7]	[1, 1]	VALID

5.3 Experimental Results

In order to verify that the improved DRL model proposed in this paper is more efficient than traditional models. We conducted three experiments to prove:

- The efficiency comparison between the improved DRL model and the traditional path planning algorithm.
- The efficiency comparison between the improved DRL model and the traditional DQN.
- The ability of dealing with sparse state space comparison between the improved DRL model and the traditional DQN.

(1) Efficiency Comparison between Improved Model and Traditional Algorithm

The A* algorithm is a very common heuristic algorithm in path planning algorithms [6]. A* algorithm can be used to search for the shortest path or to guide itself with heuristic functions. The A* algorithm searches for the shortest path by weighing the heuristic evaluation cost. Because the A* algorithm balances the relationship between computation and precision, it is widely used in path planning in games path planning and so on [2].

In this experiment, the experimental environment is a 20×20 grid map with 30 obstacles, start point and target point randomly distributed. In the static environments, the map will not change from the agent leaves the start point until the agent reaches the target point. In the dynamic environments, the obstacle

distribution will change randomly after each movement of the agent. In the above experimental environments, we used the A* algorithm to perform 2000 path planning experiments, and the average calculation time will be counted. Similarly, we also will use the improved deep reinforcement learning do the same experience, than we will count the calculation time. Among them, we need to pay attention to the fact that in the dynamic environments, each movement of the agent will lead to changes of the map. However the A* algorithm can only plan the entire path and cannot perform single-step planning. So we can only do the entire path planning, then select the next action for the agent to execute. The improved DRL model can do single-step path planning based on the input information, which saves much time compared to the A* algorithm. The specific experimental results are shown in the Tables 3 and 4:

Table 3. Time consumption of improved DRL model and A* algorithm in static environment

	Time Consumption in Static Environment	
	Time consumption for one step	Time consumption for the entire path planning
A* algorithm	0.014 s	0.014 s
Improved DRL model	0.091 s	0.091 s

Table 4. Time consumption of improved DRL model and A* algorithm in dynamic environment

	Time Consumption in Dynamic Environment	
	Time consumption for one step	Time consumption for the entire path planning
A* algorithm	0.014 s	0.21 s
Improved DRL model	0.0065 s	0.0975

It can be seen from the experimental results that the improved DRL network model computing speed is not as good as the A* algorithm in the static environment, the difference of time consumption is 0.077 s. In the dynamic environments, the improved DRL network model computing speed is better than the A* algorithm, the difference of time consumption for single-step planning is 0.0075 s, and it takes an average of 15 steps from the starting point to the target point. So the path planning time consumption difference of this two model is 0.113 s. In summary, the improved DRL model is slower than the A* algorithm in the static environments, however in the dynamic environments the computing speed is significantly better than the A* algorithm.

(2) The Efficiency Comparison between The Improved DRL Model and The Traditional DQN

The improved model and the traditional DRL model were trained on a small map which the size is 5×5 with two obstacles. The training results are shown in the Fig. 6:

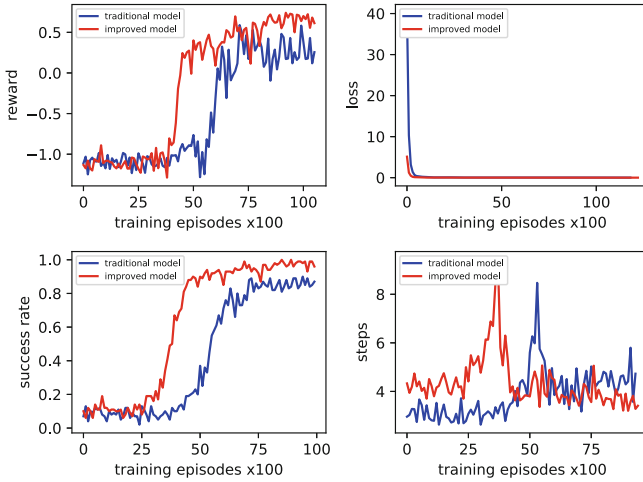


Fig. 6. The result of efficiency comparison

The four experimental results show these two models' difference in the reward value, loss value, success rate, and planned path length. The blue line represents the traditional DRL model, and the red line represents the improved model in this paper.

The reward value directly reflects the completion degree of the agent's task, and the high reward means that the agent can achieve satisfactory results in every experiment. As can be seen from the figure, the improved model can converge to higher reward values more quickly than the traditional model, and the final peak is also higher than the traditional model. The results show that the improved model is superior to the traditional model in the training speed.

The loss value indicates the difference between the training result and the target result during the model training. The figure shows that both models can successfully converge to a stable value. However, the improved model's initial loss value in training is significantly smaller than the traditional model, indicating that the improved model can help the agent quickly find the training direction at the beginning of training.

The success rate indicates whether the agent successfully reaches its destination. From the figure we can see that the improved model can reach the convergence state faster, and the success rate after convergence is higher than the traditional model.

The number of moving steps represents the number of steps that the agent moves in one training, which is a standard for measuring the effect of robot path planning. From the figure we can find that the improved model converges faster than the traditional model, and the number of steps after convergence is also smaller than the traditional model.

The above experiments prove that our improvement measures are more effective compared with the traditional DQN.

(3) The Ability of Dealing with the Sparse Reward Problem

The problem of sparse reward is the key problem that DRL model must solve. When the map size is 20×20 and the number of obstacles is 60, the problem of sparse reward becomes very prominent. The training results of the two models are shown in the Fig. 7:

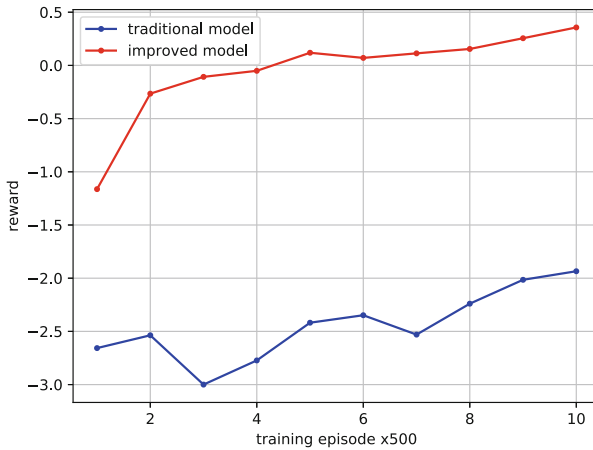


Fig. 7. The ability of dealing with the sparse reward problem (Color figure online)

The blue line is the training result of the traditional DQN model, and the red line is the training result of the improved model in this paper. As can be seen from the figure, the traditional DQN model cannot learn any “knowledge” in the sparse environments. The reward value is oscillating in the area of -3 to -2 . Therefore, it can be judged that the traditional model cannot get effective results in this experimental environment.

From the improved model, we can find that the reward value has been significantly improved compared to the traditional model, and finally converges to around $+0.5$. Positive rewards indicate that improved models can choose the right actions. We further measured the model’s success rate and moving steps, the results are shown in the Fig. 8.

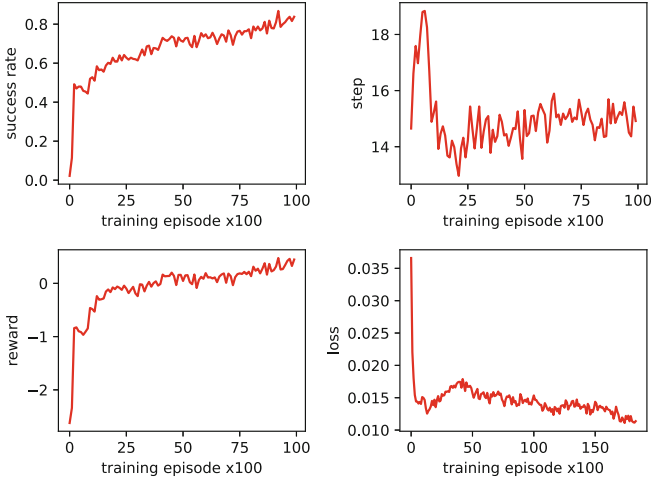


Fig. 8. The training result of improved model

We can see that the success rate of the final model is around 80%, and the number of moving steps is around 15 steps. The experimental results show that the improved model does solve the reward sparse problem that appears the path planning of mobile robots.

6 Conclusion

In the new dynamic environments that the obstacles distribute randomly, the traditional algorithm must do the recalculation when the environment changes, which will waste too much time on calculation. We proposed an efficient DRL model to do the path planning in dynamic environment. According to the Experimental Results, the DRL model takes less time on computation than the traditional algorithm. Beside, this paper proposes the weight-based exploration-exploitation strategy search algorithm, shaped reward function for path planning and new model with hindsight experience replay idea totals three measures to solve the sparse reward problem. The experimental results show that the improved model is not only better than the traditional algorithm in dynamic environments, but also more effectively than the classic DQN model.

Acknowledgments. This work has been supported by the National Natural Science Foundation of China under Grant No. 61772068, Grant 61472033 and Grant 61672178, and Fundamental Research Funds for the Central Universities under Grant No. FRF-GF-17-B28.

References

1. Kulushev, F.A., Bogdanov, A.A.: Multi-agent optimal path planning for mobile robots in environment with obstacles. In: Bjørner, D., Broy, M., Zamulin, A.V. (eds.) PSI 1999. LNCS, vol. 1755, pp. 503–510. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-46562-6_45
2. Yao, J., Lin, C., Xie, X., Wang, A.J.A., Hung, C.: Path planning for virtual human motion using improved A* star algorithm, pp. 1154–1158 (2010)
3. Sutton, R.S., Barto, A.G.: Introduction to reinforcement learning. *Mach. Learn.* **16**(1), 285–286 (2005)
4. Qiao, J., Wang, G., Li, W., Chen, M.: An adaptive deep Q-learning strategy for handwritten digit recognition. *Neural Netw. Off. J. Int. Neural Netw. Soc.* S0893608018300492 (2018)
5. Andrychowicz, M., et al.: Hindsight experience replay. In: *Neural Information Processing Systems*, pp. 5048–5058 (2017)
6. Chabini, I., Shan, L.: Adaptations of the A* algorithm for the computation of fastest paths in deterministic discrete-time dynamic networks. *IEEE Trans. Intell. Transp. Syst.* **3**(1), 60–74 (2002)
7. Kitamura, Y., Tanaka, T., Kishino, F., Yachida, M.: 3-D path planning in a dynamic environment using an octree and an artificial potential field. In: *International Conference on Intelligent Robots and Systems* (1995)
8. Mnih, V., Kavukcuoglu, K., Silver, D.: Human-level control through deep reinforcement learning. *Nature* **518**(7540), 529 (2015)
9. Schmidhuber, J.: Deep learning in neural networks: an overview. *Neural Netw.* **61**, 85–117 (2015)
10. Pathak, D., Agrawal, P., Efros, A.A., Darrell, T.: Curiosity-driven exploration by self-supervised prediction. In: *IEEE Conference on Computer Vision and Pattern Recognition Workshops* (2017)
11. Papoudakis, G., Chatzidimitriou, K.C., Mitkas, P.A.: Deep reinforcement learning for doom using unsupervised auxiliary tasks (2018)
12. Panov, A.I., Yakovlev, K.S., Suvorov, R.: Grid path planning with deep reinforcement learning: preliminary results. *Proc. Comput. Sci.* **123**, 347–353 (2018)
13. Lei, X., Zhang, Z., Dong, P.: Dynamic path planning of unknown environment based on deep reinforcement learning. *J. Robot.* **2018**(12), 1–10 (2018)
14. Kim, B., Pineau, J.: Socially adaptive path planning in human environments using inverse reinforcement learning. *Int. J. Soc. Robot.* **8**(1), 51–66 (2016)
15. Vecerik, M., et al.: Leveraging demonstrations for deep reinforcement learning on robotics problems with sparse rewards. *arXiv Artificial Intelligence* (2017)
16. Shah, P., Fiser, M., Faust, A., Kew, J.C., Hakkaniatur, D.: FollowNet: robot navigation by following natural language directions with deep reinforcement learning. *arXiv Robotics* (2018)
17. Kaelbling, L.P., Littman, M.L., Moore, A.W.: Reinforcement learning: a survey. *J. Artif. Intell. Res.* **4**(1), 237–285 (1996)
18. Wang, Z., Freitas, N.D., Lanctot, M.: Dueling network architectures for deep reinforcement learning (2015)
19. Gu, S., Lillicrap, T., Sutskever, I., Levine, S.: Continuous deep Q-learning with model-based acceleration. In: *International Conference on International Conference on Machine Learning* (2016)
20. Lei, T., Liu, M.: A robot exploration strategy based on q-learning network. In: *IEEE International Conference on Real-time Computing and Robotics* (2016)



A Way to Understand the Features of Deep Neural Networks by Network Inversion

Hong Wang^{1,2(✉)}, Xianzhong Chen^{1,2}, and Jiangyun Li^{1,2}

¹ School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing 100083, China

wanghong@ustb.edu.cn

² Key Laboratory of Knowledge Automation for Industrial Processes, Ministry of Education, Beijing 100083, China

Abstract. New variants of Deep Neural Networks (DNN) have been proposed continuously in recent years, and have led to impressive performance in a wide range of fields such as computer vision, natural language processing, and recommender systems. However, DNN are often criticized by the lack of interpretability. This paper proposes a network inversion method to understand the features extracted by DNN. DNN can be considered as a kind of transformation. When studying the characteristics and the features of a transformation, the inverse transformation is often involved. By comparing the inverted signal with the original one, better understanding of the features and properties of transformation can be achieved. In this paper, it has been found that the features extracted by a dimension-reduction layer in a DNN are essentially the special solution of the layer's constraint equations, and the linear combination of the general solutions is neglected by the layer. This find-out should help to understand the structure and function of a DNN. The experiments in this paper showed the importance of this find-out.

Keywords: Network inversion · Feature understanding · DNN

1 Introduction

New variants of Deep Neural Networks (DNN) have been proposed continuously in recent years, and have led to impressive performance in a wide range of fields such as computer vision [1–4], natural language processing [5, 6], and recommender systems [7]. However, DNN are often criticized by the lack of interpretability. The development of DNN is mainly driven by trial-and-error strategies and a considerable amount of intuition, for the absence of theoretical guidance. In this paper, a way to understand the features of DNN by network inversion is proposed. Based on the network inversion, the abstract features extracted by the intermediary layers can be visualized in the inverted signal or image, which can help to understand the features and the structure of the network. This paper mainly discusses the network inversion and feature understanding of the forward full-connection networks and convolution networks. However, the proposed method can also be applied to other structure DNN.

DNN are often considered as “black-box”, since these models cannot provide meaningful explanations on how a certain prediction (decision) is made, and why these models perform so well, or how they can be improved [8, 9]. DNN can be considered as a kind of transformation. When studying the characteristics and the features of a transformation, the inverse transformation is often involved. By comparing the inverted signal with the original one, better understanding of the features and properties of transformation can be achieved.

Inverting a neural network is to recover an input signal from the network output. In many applications, neural networks are usually dimension-reduction networks. When the network is inverted, it will result in a one-to-many mapping between the output and inputs. Therefore, there is no close-formed expression for the inverse mapping of such neural networks [10].

The forward full-connection neural networks are the earliest proposed DNN. Network reversion was first introduced by Williams [11] and then rediscovered by Linden and Kindermann [12]. It is an iterative algorithm for inverting forward neural networks. The inverse problem is formulated as an unconstrained optimization problem and solved by a gradient descent method similar to the back-propagation algorithm. Jordan and Rumelhart [13] proposed an approach to invert forward neural networks in order to solve the inverse kinematics problems for redundant manipulators. Lee and Kil [14] presented a method for computing the inverse mapping of a continuous function approximated by a forward neural network. Lu [15] tried to deal with the inverse problem using mathematical programming techniques, and the method is also applied to examine and improve the generalization performance of trained networks. However, Lu did not discuss what features the network has extracted. Saad [16] studied a new explanation algorithm that relies on network inversion, which is a pedagogical algorithm, and can extract rules from neural networks in the form of hyperplanes. This method has been applied to synthetic problems and to a real aerospace problem. Results have been compared with similar algorithms on benchmark problems. Bondarenko [17] provided an overview of extracting knowledge from a trained multi-layered fully connected sigmoidal neural network, and described a Neural Network Knowledge eXtraction (NNKX) system which was successfully applied to better understand and validate ANN models.

Convolutional Neural Networks (CNN) was introduced by LeCun [18] in the early 1990’s, and recently the large CNN models have demonstrated a significant classification performance on the ImageNet benchmark Krizhevsky [19]. As the CNN increase in depth and complexity, interpretation of CNN attracts an increasing attention.

Mahendran [20] proposed an optimization method to invert shallow and deep representations based on optimizing an objective function with gradient descent. The visualizations shed light on the information represented at each layer. Zeiler [21–23] introduced a deconvolutional network, to provide a visualization technique that gives insight into the function of intermediate feature layers and the operation of the classifier, which makes it possible to learn multiple layers of representation. Zhou [24] proposed a simple modification of the global average pooling layer and a class activation mapping (CAM) technique, which can localize class-specific image regions in a single forward-pass. Zhang [25] proposed a method to modify traditional convolutional neural networks (CNNs) into interpretable CNNs. In an interpretable CNN, each filter

in a high conv-layer represents a certain object part. The clear knowledge representation in an interpretable CNN can help people understand the logics inside a CNN, i.e., based on which patterns the CNN makes the decision. Singh [26] presented a stability-based approach for filter-level pruning of CNNs, and demonstrated its generalizability through experiments. Moreover, their compressed models can be used at run-time without requiring any special libraries or hardware, significantly outperforming other state-of-the-art filter pruning methods.

The aforementioned works provide interpretation and visualizing techniques to understand the features extracted by DNN. However, there is still a lack of effective theoretical guidance on network structure, level depth and parameter setting. In this paper, we propose a novel network inversion method to understand the features extracted by DNN, and then discuss the relation of the features and the structures of DNN based on the inversion.

The contributions of this paper are as follows: (1) we propose a novel way to understand the features of DNN by network inversion; (2) we demonstrate the effectiveness of this method by experiments; (3) we maybe the first to point out that the features extracted by a dimension-reduction layer in a DNN are essentially the special solution of the layer's constraint equations, and the linear combination of the general solutions is neglected by the layer. The experiments in this paper showed the importance of this find-out.

The remainder of this paper is organized as follows: In Sect. 2, we propose the network inversion method which is based on the iteration of solving linear equations. In Sect. 3, we provide the experiments of the network inversion and then discuss what features are extracted by the DNN. Finally, in Sect. 4 we conclude the paper and suggest some research directions for future work.

2 Network Inversion

2.1 Inversion of the Forward Full-Connection Network

Forward full-connection network is one of the basic structures of DNN. It is also the earliest DNN in research and application. We note the i th layer with L_i , the neurons of the layer are N_i , input of the layer is X_{i-1} (dimension is m_{i-1}), output of the layer is X_i (dimension is $m_i = N_i$). The equation of the input-output can be depicted as Eq. 1:

$$X_i = \delta(w_i \cdot X_{i-1} + b_i), \quad \delta(\cdot) \text{ is the activation function} \quad (1)$$

The inversion of Layer L_i means to solve the equation of Eq. (1), by given the layer L_i output X_i , and the parameters w_i and b_i of the layer. The solving of Eq. 1 to get X_{i-1} can be decomposed into two processes:

- (1) the inverting of the activation function $\delta(\cdot)$ to get Z_i , by Eq. 2:

$$Z_i = \delta^{-1}(X_i) \quad (2)$$

(2) the solution of linear equation of Eq. 3 to get X_{i-1} :

$$Z_i = w_i \cdot X_{i-1} + b_i \tag{3}$$

There are many choices of activation function in the above process (1), such as: sigmoid function, relu function, and tanh function etc. If it is a monotone reversible function, its inversion process is relatively simple; If it is a non-monotone reversible function, such as relu function, it is strictly irreversible. When there exist many reversible results, the process of finding one of them is called “pseudo-inversion”. In the above process (2), there are two conditions with the values of Z_i (dimension is $m_i = N_i$) and X_{i-1} (dimension is m_{i-1}): (a) if $m_i \geq m_{i-1}$, the dimension of Z_i (also X_i) is greater than or equal to the dimension of X_{i-1} , the layer can be abbreviated as “dimension-raising layer”. There may be a unique solution or no solution in this case; (b) if $m_i < m_{i-1}$, the layer can be abbreviated as “dimension-reduction layer”. there may be infinite sets of solutions or no solutions in this case. If neglect the no solution case in practical network applications, there will be a unique inverting solution in condition (a); in condition (b), the inversion may have infinite sets of solutions. The infinite sets of solutions corresponding to condition (b) is the key consideration in the inversion problem. This inversion problem has been detailly discussed in literatures [11, 12, 14, 15].

From the last layer of the network, inverting the layers one by one, the whole network can be inverted.

2.2 Inversion of the Dimension-Reduction Layer

For the “dimension-reduction layer”, there may be infinite sets of solutions of the input inverted from output. The inverted solutions can be expressed as:

$$X_{i-1} = K_i \cdot X_{n(i-1)} + X_{s(i-1)} \tag{4}$$

$$X_{n(i-1)} = null(w_i, 'r') \tag{5}$$

$$X_{s(i-1)} = w_i \setminus X_{c(i-1)} \tag{6}$$

In Eq. 4 $X_{n(i-1)}$ is the general solution of $w_i \cdot X_{i-1} = 0$, namely zero space solution. In Eq. 5, $X_{s(i-1)}$ is the special solution of $X_{c(i-1)} = Z_i - b_i = w_i \cdot X_{i-1}$, and K_i is a set of arbitrary undetermined constants.

For multi-layer forward full-connection networks, the output X_{i-1} of layer L_{i-1} is the input of layer L_i , if layer L_i is a dimension-reduction layer, the output-input relation is:

$$\begin{aligned} X_i &= \delta(w_i \cdot X_{i-1} + b_i) = \delta(w_i \cdot (K_i \cdot X_{n(i-1)} + X_{s(i-1)}) + b_i) \\ &= \delta(w_i \cdot X_{s(i-1)} + b_i) \end{aligned} \tag{7}$$

From Eq. 7 it can be observed that the layer L_i actually decomposes the output X_{i-1} of layer L_{i-1} into two parts, the linear combination of general solutions $K_i \cdot X_{n(i-1)}$ is

ignored in transmission to the next layer, and the special solution $X_{s(i-1)}$ is the real feature extracted by layer L_i , and then it is converted by the activation function as the output X_i of layer L_i .

This conclusion is obvious, but strangely, previous researchers did not pay attention to the importance of this conclusion. In the Sect. 3 of this paper, the importance of this find-out was shown by experiments.

2.3 Problems Often Concerned in Network Inversion

In the inversion of dimension-reduction layer, the inversion of X_i to X_{i-1} can get infinite results, among them, the special solution $X_{s(i-1)}$ is the most representative feature. However, the special solution $X_{s(i-1)}$ may not satisfy the constraints of requirements in specific applications (for example, the sigmoid activation function requires X_{i-1} in range of $[0, 1]$ constraints), by selecting suitable $K_i \cdot X_{n(i-1)}$, X_{i-1} can be suitable for the constraints.

In image processing and image classification applications, the network inversion problems usually involve forward full-connection networks are as follows:

- (1) If given an input image X_i , after passing through the network, the output is Y_i . Whether there are any other input images X'_i , and the output is also Y_i ?
- (2) When adding some disturbances on Y_i to get \tilde{Y}_i , what is the corresponding input image \tilde{X}_i ?
- (3) If the inputs are X_i and X_j , and the outputs are Y_i and Y_j . Whether we can add some disturbances on X_i to get \hat{X}_i , but the output of \hat{X}_i resembles Y_j as much as possible?

If dimension-reduction layers exist in the forward full-connection network, for the above problem (1) there should be multiple possible inverted X'_i , which have the same output Y_i as the input X_i . As to problem (2), if exists infinite results \tilde{X}_i corresponding to the output \tilde{Y}_i , the solutions that satisfy certain constraints should be founded. Then to problem (3), this problem is similar to using GAN (Generative Adversarial Networks) to generate adversarial samples, similar results can also be achieved by using the special solutions $X_{s(i-1)}$ and linear combination of general solutions $K_i \cdot X_{n(i-1)}$.

2.4 Inversion of Image Convolution Operation

Image convolution network is also one of the basic structures of DNN, and it is the most widely used DNN in the field of image processing and classification.

In image convolution operation, the size of convolution kernel, image edge filling (padding) and convolution stride are the parameters to be considered and selected. The input and output relation of convolution operation can be depicted the same as Eq. 1.

In many CNN (Convolutional Neural Networks) networks, convolution layer is often combined with a pooling process. The input and output relation can be considered as the following three processes: (1) the linear constraint process of image convolution; (2) the conversion process of activation function; (3) the pooling subsampling process (Fig. 1).

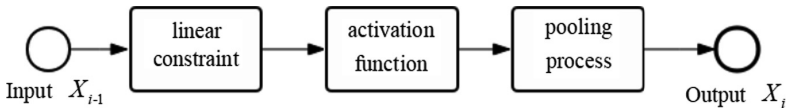


Fig. 1. Three process for convolution and pooling layer

The above processes (1) and (2) are similar to those of full-connection networks, and the pooling of process (3) includes Max pooling, Average pooling, random pooling, empty pyramid pooling, etc. Generally speaking, the pooling process is non-linear. There are many possible results in its inversion (also known as unpooling). Choosing different results will have different impacts on the final inversion results, which will not be discussed in detail here. Reference can be made to the literatures [20–25].

The inversion problem of CNN network is not as much concerned as that of fully connected network. The output of a convolution layer is a sets of feature-maps, such feature-maps can be visualized and better understood, while the output of fully connected layer is abstracted features. However, Zeiler [23] performed a sensitivity analysis of the classifier output by occluding portions of the input image (also called hot-map), revealing which parts of the scene are important for classification by using network inversion of the CNN network. This research has attracted extensive attention of researchers.

In the CNN, convolution layer is often a dimension-raising process, usually increases the input dimension to a very high dimension. When inverting the convolution layer, theoretically there exists only one inverting result. But if inverting one of the feature map in the convolution layer, it's usually a dimension-reduction process, the special solution corresponding to each feature map can be obtained. If the network structure need to be pruned for computation reduction, the convolution filters with similar special solution can be removed from the convolution layer, this way is applicable to situation mentioned in paper [26].

2.5 Inversion by AutoEncoder and Decoder

The inversion of the network can also be carried out by using AutoEncoder and Decoder in the form of structural symmetry. The deconvolution structure of CNN network is actually an AutoEncoder structure.

For the “dimension-raising layer”, its input to output are “one-to-one mapping”. AutoEncoder can be trained to obtain good and unique inversion results. But for the “dimension-reduction layer”, its input to output are “many-to-one mapping”. Using AutoEncoder method, only one of the many inversion results can be obtained. In practice, the ideal inversion results are often not obtained.

3 Experimental Results and Analysis

In this section experiments are provided to demonstrate the effectiveness of using network inversion to understand the features of DNN. The features extracted by a dimension-reduction layer in a DNN are essentially the special solution of the layer's

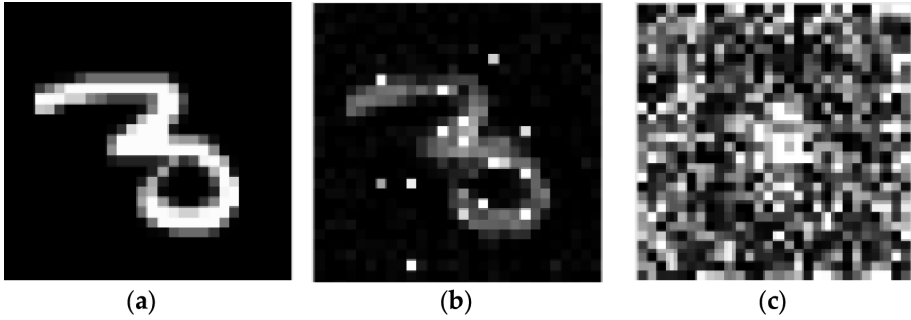


Fig. 2. Results of Experiment 1. The images are: (a) Original input image X_0 ; (b) Inverted image X'_0 ; (c) Inverted image X''_0 . By the output X_2 of the input X_0 , two different inverted images X'_0 and X''_0 can be obtained.

constraint equations, and the linear combination of the general solutions is neglected by the layer. The experiments showed the importance of this find-out.

Experiment 1: With the MNIST data set, a simple full-connection forward network of [784, 30, 10] is trained. [784, 30, 10] means: the input image X_0 with $28 \times 28 = 784$ pixels, the first layer with 30 neurons and the output is X_1 , the second layer with 10 neurons and the output is X_2 . The classification accuracy of this network is 96.4%, which is sufficient to our experiment.

If input image is X_0 as shown in Fig. 2(a), the network output is X_2 . Then, X_2 is inverted to get X'_1 and X'_0 . Figure 2(b) shows an inverted X'_0 from multiply inverting results, which is resembling to the original input image X_0 . But another image X''_0 can be inverted from X_2 , as shown in Fig. 2(c) which is very different from the original input image X_0 . However, while input all those images X_0 , X'_0 and X''_0 to the network, the outputs are the same as X_2 .

Experiment 2: Using the same data and network of Experiment 1, an image X_0^* is to be inverted, with constraints: (1) X_0^* resembles the input image X_0 with only a few different pixels, and (2) network output of image X_0^* is the same with image X_0 .

With input X_0 to the network, the layer L_1 output X_1 can be calculated (also with the intermediary parameters K_1 , X_{n_0} , X_{s_0} and $X_1 = K_1 \cdot X_{n_0} + X_{s_0}$), and then the layer L_2 output X_2 can be calculated. To reduce the invert iterations, a man-made modified image X'_0 with a few different pixels to the original input was used. With input X'_0 to the network, the layer L_1 output X'_1 can be calculated (also with K'_1 , X'_{n_0} , X'_{s_0} and $X'_1 = K'_1 \cdot X'_{n_0} + X'_{s_0}$), and the layer L_2 output X'_2 . Note that X_0 and X'_0 are different, the corresponding outputs X_2 and X'_2 are also different. Then, keep the X_{n_0} , X_{s_0} , X_2 as fixed, but use K'_1 as an initial value to invert image X_0 . By using iterations to meet the limitations of the activation function, X_0^* can be get. The inverted image X_0^* is much resemble to X'_0 with only a few different pixels, but has the same output X_2 with the input X_0 . Figure 3 shows the result images of the Experiment 2.

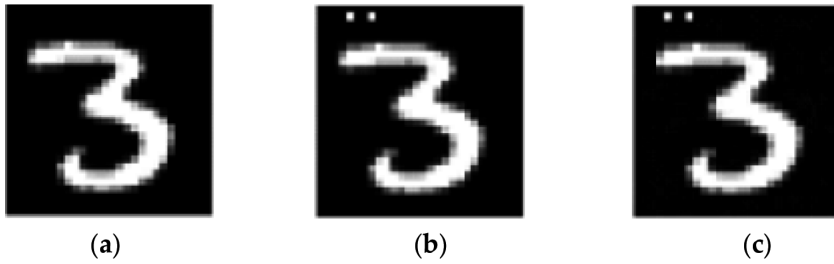


Fig. 3. Results of Experiment 2. The images are: (a) Original input image X_0 ; (b) Man-made a few modifications on the original input image to get X'_0 ; (c) Inverted image X_0^* with only a few different pixels to image X_0 , but has the same output X_2 with the input X_0 .

Experiment 3: Using the same data and network of Experiment 1. With X_0^i is the original input image with category C_i , disturbances from image X_0^j (with category C_j) are taken out and added to X_0^i . A new image $X_0^{i_i}$ can be get, which resembles X_0^i (with category C_i) but the network will classify $X_0^{i_i}$ to a wrong category C_j .

As mentioned in Sect. 2.2, that a dimension-reduction layer extracts the special solution as the feature, and omits the linear combination of general solutions. Keep the X_{n0}^i, X_{s0}^j (in place of X_{s0}^i), X_2^j (in place of X_2^i) as fixed, but use K_1^i as an initial value to iteratively invert an image X_0^i . The image $X_0^{i_i}$ resembles X_0^i (with category C_i), but with the same network output X_2^j as the input of X_0^j (with category C_j). Figure 4 shows the result.

This example has some relation to the adversarial sample, but the adversarial sample comes from network inversion rather than generated by a GAN network.

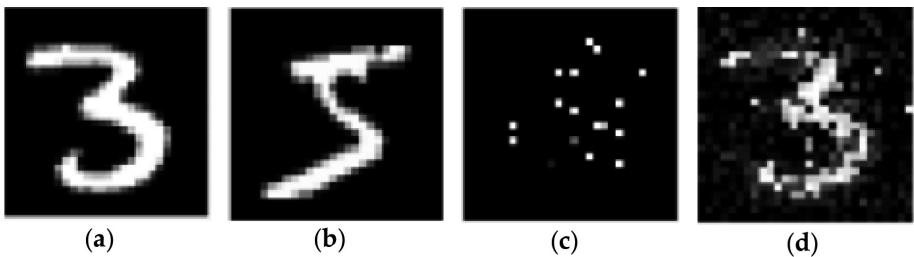


Fig. 4. Results of Experiment 3. The images are: (a) Original input image X_0^i with right category “3”; (b) image X_0^j with right category “5”; (c) the special solution X_{s0}^j as a disturbances; (d) inverted image $X_0^{i_i}$ resembles X_0^i , but with category “5”.

Experiment 4: Using the MNIST data set. This experiment is to deal with the network structure of depth and width. If the requirements are classification accuracy higher than 95% and the network parameters as fewer as possible, the problem is to find out how

many layers and how many neurons of each layer are needed for a full-connection network. This paper can not provide the optimal solution, but propose a network inversion method to this problem.

With a trained network of [784, 100, 30, 10] with classification accuracy 96.6%, the following inverted images in Fig. 5 can be obtained.

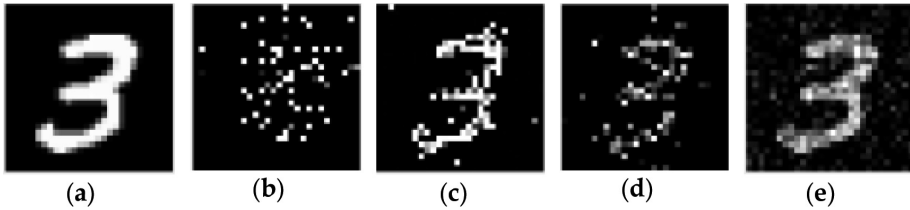


Fig. 5. Results of Experiment 4 network of [784, 100, 30, 10]. The images are: (a) Original input image X_0 ; (b) image X_{s0} corresponding to the original input image (with only 100 non-zero values); (c) Image inverted by X_{s1} (select the 100 largest values, other values are set to zero.); (d) Image inverted by X_{s2} (select the 100 largest values, other values are set to zero.); (e) Image inverted by X_3 .

And then, a trained network of [784, 300, 100, 30, 10] with classification accuracy 96.8%, the following images in Fig. 6 can be obtained.

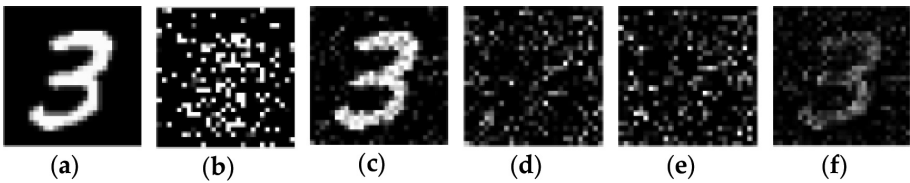


Fig. 6. Results of Experiment 4 network of [784, 300, 100, 30, 10]. The images are: (a) Original input image X_0 ; (b) image X_{s0} corresponding to the original input image (with only 300 non-zero values); (c) Image inverted by X_{s1} (select the 300 largest values, other values are set to zero.); (d) Image inverted by X_{s2} (select the 300 largest values, other values are set to zero.); (e) Image inverted by X_{s3} (select the 300 largest values, other values are set to zero.); (f) Image inverted by X_4 .

Then, the networks with the same number of layers, but different neurons on the first layer, are compared. All of the networks with classification accuracy higher than 95%, accuracy difference is lower than 1%. In the Fig. 7, the first row is network [784, 200, 50, 10], the second row is network [784, 250, 50, 10], the third row is network [784, 150, 50, 10].

From the three networks above, it seems that 150 neurons in the first layer maybe a good choice.

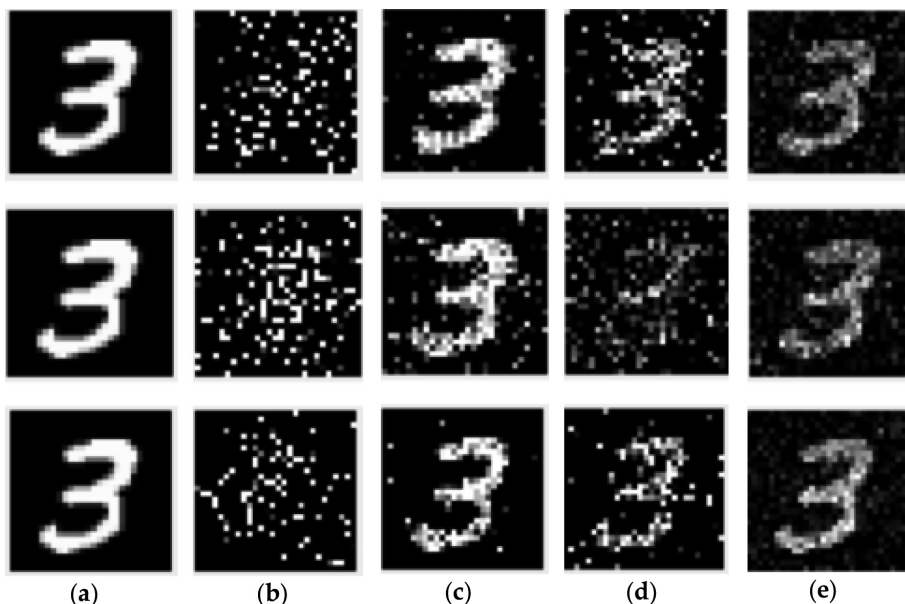


Fig. 7. Results of Experiment 4, the first row is network [784, 200, 50, 10], the second row is network [784, 250, 50, 10], the third row is network [784, 150, 50, 10]. The images are: (a) Original input image X_0 ; (b) image X_{s0} corresponding to the original input image; (c) Image inverted by X_{s1} ; (d) Image inverted by X_{s2} ; (e) Image inverted by X_3 .

From all the examples above, it can be concluded that: (1) For MNIST data set, a two- or three-layer fully-connected neural network (not including the input layer) can achieve results that are desirable enough; (2) Special solution X_{si} of each layer can represent the features extracted by that layer. The number of neurons in each layer can be selected according to the inverted image by using each layer's special solution X_{si} .

4 Conclusions

This paper proposes a network inversion method to understand the features extracted by DNN. In this paper, it has been found that the features extracted by a dimension-reduction layer in a DNN are essentially the special solution of the layer's constraint equations, and the linear combination of the general solutions is neglected by the layer. This find-out should help to understand the structure and function of a DNN. The experiments in this paper showed the importance of this find-out.

Experiment 3 in Sect. 3 shows that the network inversion have some relations with the GAN. How to use features from two or more images to generate new images will be one of the future works. Another research direction could be the improvement on the efficiency of iterative algorithm to implement network inversion with constrain conditions.

References

1. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (2016). <https://doi.org/10.1109/CVPR.2016.90>
2. Krizhevsky, A., Sutskever, I., Hinton, G.E.: Imagenet classification with deep convolutional neural networks. In: Advances in Neural Information Processing Systems (2012). <https://doi.org/10.1016/B978-008046518-0.00119-7>
3. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition (2014). <https://doi.org/10.2146/ajhp170251>
4. Wen, Y., Zhang, K., Li, Z., Qiao, Yu.: A discriminative feature learning approach for deep face recognition. In: Leibe, B., Matas, J., Sebe, N., Welling, M. (eds.) ECCV 2016. LNCS, vol. 9911, pp. 499–515. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-46478-7_31
5. Vaswani, A., et al.: Attention is all you need [transformer]. In: The 31st Conference on Neural Information Processing Systems (NIPS 2017) (2017)
6. Radford, A., Salimans, T.: Improving language understanding by generative pre-training (transformer in real world). OpenAI (2018)
7. Chen, J., Zhang, H., He, X., Nie, L., Liu, W., Chua, T.-S.: Attentive collaborative filtering: multimedia recommendation with item- and component-level attention. In: Proceedings of the 40th International ACM SIGIR Conference on Research and Development in Information Retrieval - SIGIR (2017). <https://doi.org/10.1145/3077136.3080797>
8. Liu, X., Wang, X., Matwin, S.: Interpretable deep convolutional neural networks via meta-learning. In: Proceedings of the International Joint Conference on Neural Networks (2018). <https://doi.org/10.1109/IJCNN.2018.8489172>
9. Du, M., Liu, N., Song, Q., Hu, X.: Towards explanation of DNN-based prediction with guided feature inversion. In: KDD (2018): The 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, London, United Kingdom, 19–23 August 2018, 10 p. ACM, New York (2018). <https://doi.org/10.1145/3219819.3220099>
10. Jensen, C.A., et al.: Inversion of feedforward neural networks: algorithms and applications. Proc. IEEE (1999). <https://doi.org/10.1109/5.784232>
11. Williams, R.J.: Inverting a connectionist network mapping by back-propagation of error. In: Proceedings of 8th Annual Conference of the Cognitive Science Society, pp. 859–865. Lawrence Erlbaum, Hillsdale (1986)
12. Linden, A., Kindermann, J.: Inversion of multilayer nets (2003). <https://doi.org/10.1109/ijcnn.1989.118277>
13. Jordan, M.I., Rumelhart, D.E.: Forward models: supervised learning with a distal teacher. Cogn. Sci. (1992). [https://doi.org/10.1016/0364-0213\(92\)90036-T](https://doi.org/10.1016/0364-0213(92)90036-T)
14. Lee, S., Kil, R.M.: Inverse mapping of continuous functions using local and global information. IEEE Trans. Neural Netw. (1994). <https://doi.org/10.1109/72.286912>
15. Lu, B.L., Kita, H., Nishikawa, Y.: Inverting feedforward neural networks using linear and nonlinear programming. IEEE Trans. Neural Netw. (1999). <https://doi.org/10.1109/72.809074>
16. Saad, E.W., Wunsch, D.C.: Neural network explanation using inversion. Neural Netw. (2007). <https://doi.org/10.1016/j.neunet.2006.07.005>
17. Bondarenko, A., Alekseyeva, L., Jumutc, V., Borisov, A.: Classification tree extraction from trained artificial neural networks. Procedia Comput. Sci. (2016). <https://doi.org/10.1016/j.procs.2017.01.172>

18. LeCun, Y., et al.: Backpropagation applied to handwritten zip code recognition. *Neural Comput.* (2008). <https://doi.org/10.1162/neco.1989.1.4.541>
19. Krizhevsky, A., Sutskever, I., Hinton, G.E.: ImageNet classification with deep convolutional neural networks (2012)
20. Mahendran, A., Vedaldi, A.: Understanding deep image representations by inverting them. In: *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (2015). <https://doi.org/10.1109/CVPR.2015.7299155>
21. Zeiler, M.D., Krishnan, D., Taylor, G.W., Fergus, R.: Deconvolutional networks. In: *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (2010). <https://doi.org/10.1109/CVPR.2010.5539957>
22. Zeiler, M.D., Taylor, G.W., Fergus, R.: Adaptive deconvolutional networks for mid and high level feature learning. In: *Proceedings of the IEEE International Conference on Computer Vision* (2011). <https://doi.org/10.1109/ICCV.2011.6126474>
23. Zeiler, M.D., Fergus, R.: Visualizing and understanding convolutional networks. In: Fleet, D., Pajdla, T., Schiele, B., Tuytelaars, T. (eds.) *ECCV 2014*. LNCS, vol. 8689, pp. 818–833. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10590-1_53
24. Zhou, B., Khosla, A., Lapedriza, A., Oliva, A., Torralba, A.: Learning deep features for discriminative localization. In: *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (2016). <https://doi.org/10.1109/CVPR.2016.319>
25. Zhang, Q., Wu, Y.N., Zhu, S.C.: Interpretable convolutional neural networks. In: *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (2018). <https://doi.org/10.1109/CVPR.2018.00920>
26. Singh, P., Kadi, V.S.R., Verma, N., Nambodiri, V.P.: Stability based filter pruning for accelerating deep CNNs. In: *Proceedings - 2019 IEEE Winter Conference on Applications of Computer Vision, WACV* (2019). <https://doi.org/10.1109/WACV.2019.00129>



Detection of Weak Defects in Weld Joints Based on Poisson Fusion and Deep Learning

Xinli Chen¹, Hongbing Wang¹(✉), Li Li¹, Jingyi Liu¹, Shuqi Wei¹, Haihua Li², and Jinxin Lv²

¹ University of Science and Technology Beijing, Beijing 100083, China
wanghongbing0816@163.com

² XinJiang TianWei Nondestructive Testing, Shanghai 834000, XJ, China

Abstract. There exist crack, bar and round defects in the weld joints of pressure vessels and pipes, which are detected by the X radiographic inspection system. The check and evaluation for defects in the radiographic images are often done manually and the work efficiency is low, the evaluation has artificial subjectivity. The automatic detection method of defects in weld joints based on Poisson fusion and deep learning is proposed. The defects in weld joints are typical industrial weak objects because of their small size, distinct edge erosion, and small SNR in radiographic images. The training images should be augmented for the application of deep learning in the object detection of industrial images. The augmentation method based on Poisson image fusion is given to simulate the edge erosion in radiographic images. The histogram is used to find a suitable position for the Poisson fusion of the object defect and background region. The detection model is obtained in the framework of Faster R-CNN with the pre-trained ResNet50. Feature Pyramid Network is integrated for its strong detection capacity for industrial weak objects. The results show that our Poisson image fusion has a much greater contribution to the detection model than the general data augmentation in geometry transform in terms of AP and Recall.

Keywords: Deep learning · Poisson fusion · Weak defects · Feature Pyramid Network

1 Introduction

1.1 Background

In industrial production, welding is a process of connecting two or more parts at high temperature or high pressure. For example, electric arc welding, argon arc welding, and CO₂ protection welding. It is widely used in aerospace, energy transportation, machinery manufacturing and petrochemical and so on [1]. Inevitably, there will be various welding defects within the device due to welding methods and operation processes. The typical defects are round, crack, bar, lack of penetration, incomplete fusion, slag inclusions, Tungsten inclusions, burn through, undercut and so on, in which round and bar defects are the most frequently found in the weld, and crack is the most harmful defect [2]. These defects will influence the quality of products harmfully. Defects reduce the carrying intercept area of welds and weaken the strength of static

tensile. Defects may create gaps, and gaps can occur with stress concentration and brittleness at the tip of the gap, and penetrate the welds and leak, seriously affecting the density. Therefore, it is very important to carry out NDT (Non-Destructive Testing) of welded components.

X radiographic is commonly used in industry with an equipment inspection. It can show the information about the weld on the film or digital plate detector. Because of its small size, distinct edge erosion and small SNR, it is difficult to detect the defect in radiographic images.

The traditional defect detection is done by manual using strong light to shine the film. Heavy workload, low efficiency, long-term work make eyes injured. On the other hand, results rely on professional knowledge and work experience.

1.2 Related Work

For the traditional image processing methods, Mahmoudi et al. [3] propose a method to extract and classify defects in radiographic images quickly. First, the weld area is extracted by the global threshold on the pre-processed image, and then the weld defect area is extracted by the local threshold. This method does not have an obvious effect on the welding defect of extracting complex shapes. Alaknanda et al. [4] proposed a method to process the radiographic image according to the shape of the weld. The canny operator is used to determine the defect boundary with the appropriate threshold, then the morphological method is used to fine-tune the boundary, and finally, the detected defects are classified. Daum et al. [5] proposed a method of defect segmentation based on background elimination. It is generally effective, but it is difficult to detect small defect areas between 4 and 6 pixels in size. Zou et al. [6] put forward a real-time method to detect screw pipe weld defects based on Kalman filtering. Kalman filtering is used to detect the trajectory continuity of defects in the image sequence to identify the real defects. Yan Jiaxin et al. [7] put forward the preliminary segmentation of the defect with thin of the width of fewer than 3 pixels in the image. A column-by-column adaptive threshold method is used to filter noise. And the improved local Hough transformation is applied to remove a large amount of noise in the preliminary segmentation result, and accurately divides the defect with thin of the width less than 3 pixels in the image.

In the study of machine learning, DaSilva et al. [8] studied the nonlinear pattern classifier implemented by ANN (Artificial Neural Network). Geometric features of defects, such as position, aspect ratio, and roundness, are used as the input of the classifier to train the classification model. However, the model is not robust enough. Kumar et al. [9] computed the texture and geometric features of GLCM (Gray-Level Co-occurrence Matrix) as the input of BP (Back Propagation) neural network to train the classifier and finally obtained a suitable accuracy. Wang et al. [10] used a multi-threshold image feature extraction method and SVM (Support Vector Machine) to classify defect and non-defect features to obtain a rough defect area. Finally, Hough transformation is used to remove the noisy pixels in the rough defect area to locate and segment the defects. The experimental results show that the method is effective for the segmentation and localization of defects in radiographic images of welding seams with noise and low contrast. Boaretto et al. [11] proposed an automatic welding defect

recognition and classification method. Firstly, the position of welding seam was detected and the discontinuous parts were found. These features were used to train a feed-forward MLP (Multilayer Perceptron) in binary classification.

At present, there is research in the field of deep learning convolutional neural network for automatic extraction of image features. Liu et al. [12] recognized the welding seam region by wavelet noise reduction, Sin enhancement, image segmentation, and other methods. The clustering algorithm of OPTICS based on sorting points is used to segment the weld area, which is normalized and fed into the CNN (Convolution Neural Network) for defect identification. In the detection of crack defect video, Chen et al. [13] used the method of sliding window to segment images. The segmented images were input into the CNN (Convolutional Neural Network) for judgment. Then the method of spatial-temporal registration and naive Bayesian data fusion is used to improve the recognition accuracy and recall rate. A method for extracting the weld zone was proposed by Suyama et al. [14]. Radiographic images of welding seams were preprocessed and then combined with masks to divide the images into several small blocks. The weld area was extracted by DNN (Deep Neural Network), and then defects were detected.

From the previous work, it can be found that the traditional image processing method which depends on artificial design features does not have good robustness. Compared with the above methods of extracting the proposal area by segmentation, this paper proposed the detection model in the framework of Faster R-CNN with the pre-trained ResNet50. FPN (Feature Pyramid Network) is integrated for its strong detection capacity for industrial weak objects. Because most of the weld defects are weak objects in industry, it is difficult to obtain a large number of images, especially for radiographic images containing cracks. The training images should be augmented for the application of deep learning in the object detection of industrial images. According to the distribution characteristics of each defect, the Poisson fusion method based on the statistical histogram is proposed to augment the data by simulating the edge erosion effect of X radiographic film. Compared with the traditional data augmentation method, the mAP (Mean Average Precision) for our Poisson fusion method increased by 0.115, and the maximum recall rate of crack, bar and round increased by 0.125, 0.106 and 0.010 respectively.

2 The Proposed Approach

2.1 Data Augmentation

Radiographic film imaging refers to that radiography irradiates the emulsion layer of the film. The silver halide crystals in the emulsion layer react chemically and coalesce with the adjacent silver halide crystals, which are also irradiated by X radiography, and deposit on the film, leaving an image. The brightness of each area on the film is directly proportional to the thickness of the plate, that is, the bigger the thickness is, the higher the attenuation is, and the whiter the image is. The weld zone includes the groove and

root zone, and the HAZ (heat-affected zone) is between metal and weld as shown in Fig. 1.

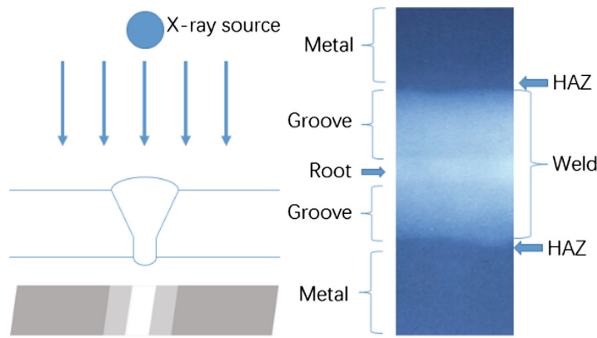


Fig. 1. X radiographic weld joint

The typical weld defects include the crack, bar, and round. According to the generation mechanism of different defects, the defects show in some distribution characteristics. The crack defects, often appearing in welds and heat-affected zones, show as the black wire or black line, around which are tiny serrations and bifurcations. Bar and round defects may appear at any position in the weld zone. Bar and round defects may appear densely or separately [15].

Data Augmentation in Geometry

Due to the small amount of source data, an appropriate augmentation is necessary to learn fully the data characteristics when deep neural network model training is conducted. Geometric transformation is a conventional data augmentation method, which is composed of rotation, flip, distortion, and deformation. Because distortion and deformation fail to conform to the generation mechanism of defects, they are invalid for the data augmentation. The data augmentation and geometric methods are shown in Table 1.

Table 1. Data augmentation and geometric methods

	Geometric methods
Rotation	180°
Flipping	Horizontal
Flipping	Vertical

An example of the data augmentation using geometric methods is shown in Fig. 2.

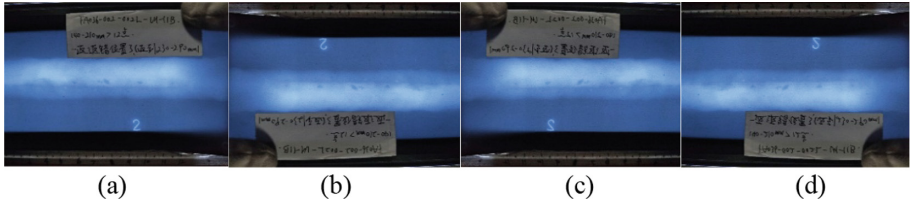


Fig. 2. Geometric Data Augmentation (a) Origin Image (b) Rotation (c) Vertical Flipping (d) Horizontal Flipping

Data Augmentation in Poisson Fusion

For radiographic images with distinct edge erosion and small SNR, there are two methods for industrial object detection. The first is that traditional object detection and noise reduction is used to remove edge erosion and increase SNR. This is difficult because the size of edge erosion cannot be determined accurately and there are many causes for noises in radiographic images. The second is that image fusion is applied to simulate the characteristics and distribution of the original industrial image with distinct edge erosion so as to improve the detection capability of the model.

Image fusion generates a new image by embedding an object or an area in the source image into the target one. In order to make the fused image more natural, which means that the fused image is more similar to the real images including defects, the fusion boundary should be seamless. However, if the original image and the target image have different color, brightness, texture, and surface, the fused image will have distinct boundaries.

Poisson fusion is a method to figure out the optimal value of pixels by constructing the Poisson equation. While the gradient information of the source image is preserved, the background of the source image and the target image can be fused well. According to the specified boundary conditions, this method constructs a Poisson equation to calculate respectively the gradient fields of the two images. After that, the gradient is replaced in corresponding regions, the image divergence is calculated and the Poisson equation to get the optimal pixel value of the fusion region is figured out. Poisson fusion realized the continuity in the gradient domain, and seamless fusion at the boundary. The fusion process is shown in Fig. 3.

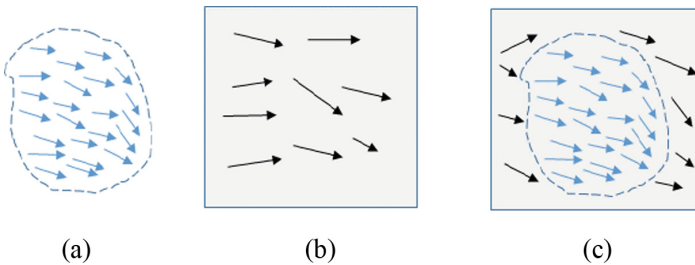


Fig. 3. Poisson Fusion (a) Gradient of Object Image (b) Gradient of Background Image (c) Gradient after Poisson Fusion

The augmentation method based on Poisson image fusion is proposed as shown in Fig. 4. Firstly, images and annotated files are obtained and the location and category of defects by parsing annotated files are found. According to the distribution characteristics of defects, different fusion zones are chosen. If it is a crack defect, because of its frequent appearance in the middle of HAZ and weld area in a threadlike shape, the fusion zone can be selected in the horizontal or vertical direction of the original position according to the size of the short side, and the number is generally set to be from 2 to 3. If it is another defect, such as bar and round, because of its limitless position in the weld area and its small size, the fusion zone can be selected in the weld zones around it and the number can be set to be from 4 to 6. Then according to the judging method, we can decide whether to use the area or to return to the area selecting step.

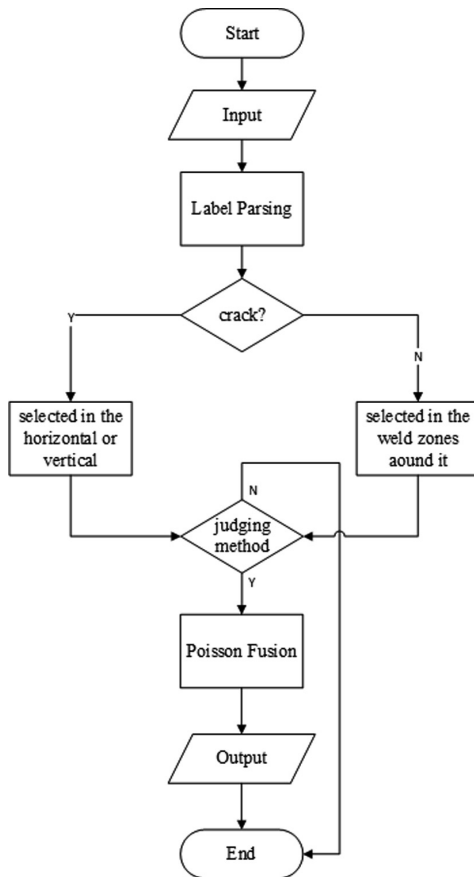


Fig. 4. Data Augmentation using Poisson Fusion

The judgment of whether the fusion region could be taken or not is done by calculating the statistical histogram of the region. The fusion region is taken up if there is no obvious single peak or double peak in the histogram. The original defect area, optional area, non-optional area, and their corresponding statistical histograms are shown in Fig. 5.

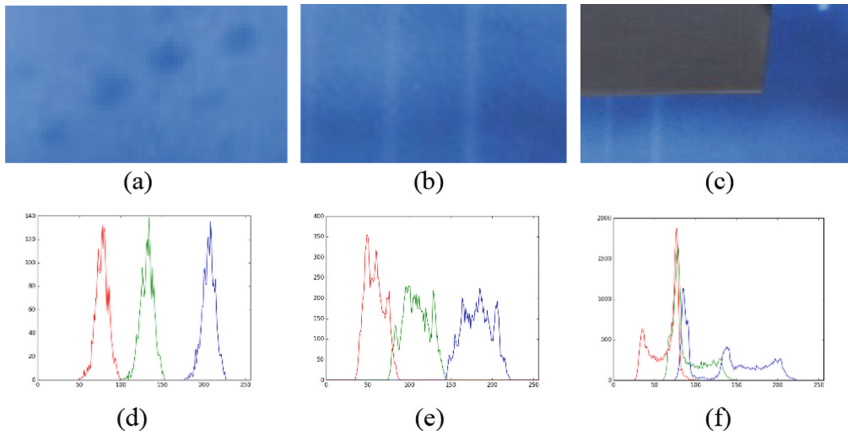


Fig. 5. Statistical Histogram (a) Original Image (b) Applicable Image (c) Invalid Image (d) Histogram of Original Image (e) Histogram of Applicable Image (f) Histogram of Invalid Image

Finally, the results are shown as follows (Figs. 6 and 7).

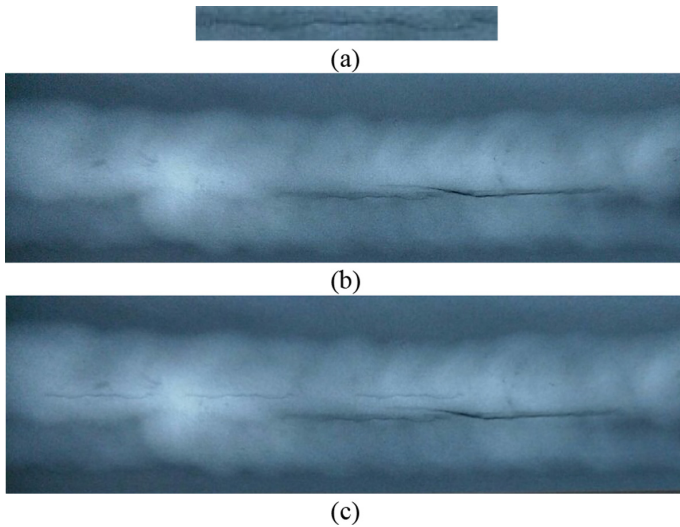


Fig. 6. Generation of Crack Fusion Images (a) Crack Image (b) Original Image (c) Fusion Image

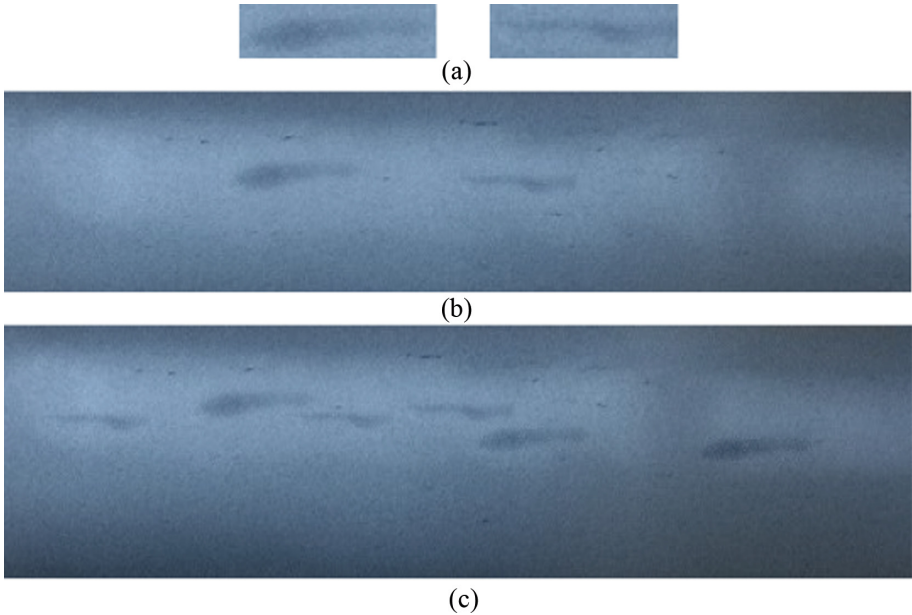


Fig. 7. Generation of Bar Fusion Image (a) Bar Image (b) Original Image (c) Fusion Image

Result of Data Augmentation

Based on the above two methods, the augmented data are shown in Tables 2 and 3.

Table 2. Number of samples

Number	Bar	Crack	Round	Total
Original images	16	12	32	60
Geometry images	48	36	96	180
Fusion images	15	14	32	61
Total	79	62	160	301

Table 3. Number of defects

Number	Bar	Crack	Round	Total
Original images	30	15	174	219
Geometry images	90	45	522	657
Fusion images	77	49	411	537
Total	197	109	1107	1413

2.2 Object Detection Based on Deep Learning

Faster R-CNN

With the continuous development of deep learning, object detection model based on the convolutional neural network has been gradually applied to various fields. So far,

Faster RCNN has been a relatively mature object detection framework that underwent two developmental stages: RCNN and Fast RCNN. RCNN firstly generates 1 k–2 k candidate regions for images, uses a convolution neural network to extract the features of each region and inputs them into the SVM classifier, and finally adopts a regression method to finely correct the position of the candidate frames. Fast RCNN improves the detection speed by mapping the proposal area to the last layer of CNN so that feature extraction is only performed once per image. Using Region Proposal Network (RPN) to calculate candidate regions, and feature sharing mechanism, Faster RCNN enjoys another round of enhancement in speed [18, 19].

Feature Pyramid Network

Although Faster RCNN has the characteristic of high detection stability, it lacks the ability to detect fine-grained and small-size features. Yun et al. [20] used the top-down jumping connection technique to detect small objects in remote sensing images, such as airplanes and ships. Based on the Faster RCNN network and convolution feature extraction process, they obtained better small object detection results.

In this paper, a detection framework combining Faster RCNN and FPN (Feature Pyramid Network) is used. As shown in Fig. 8(a), shows a sketch of Faster RCNN extracting and predicting features, a process that only uses the last layer feature map of the convolutional neural network. However, due to the small size of weld defects studied in this paper, its information will be lost after several convolution and pooling operations. Figure 8(b) shows the structure of FPN, which uses the inherent multi-scale and multi-level structure of deep convolution neural network and adopts a top-down side connection to construct high-level semantic feature maps at all scales, gaining the ability to detect fine-grained features [21].

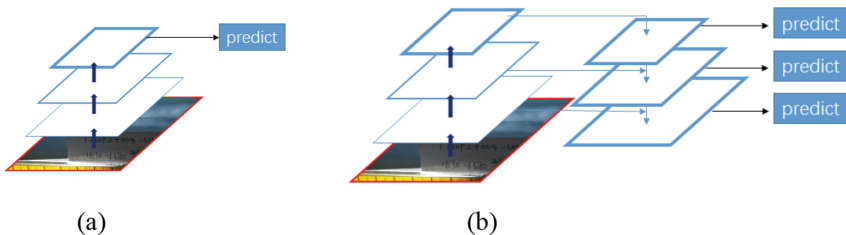


Fig. 8. Different Structure of Feature Map (a) Single Feature Map (b) Feature Pyramid Network

3 Experiments and Results

Experiments are evaluated in the computer with the Ubuntu16.04 system, Intel i7-7700 16 GB CPU, and TITAN Xp 12 GB GPU in this paper. Based on the three groups of data mentioned above, the compared experiments were executed. The test set was from the half random sample from source data, marked as D(T). While the remaining were used as the training set for the first group of experiments, marked as D(S). The training set of the first group and the data of other two groups constitute the second and third

groups of experimental training sets marked as D(S)+D(G) (Geometric images) and D(S)+D(P) (Poisson fusion images) respectively. The test set D(T) was used in each group of experiments, and it was invisible to the training process. TensorFlow deep learning framework is used to build a detection network to offer training to each training set, with the backbone as the pre-training model for ResNet50. The base learning rate is set to be 0.001 and the total iteration is 30000. The learning rate will be updated when the iteration reaches 10000 and 20000 respectively. The mini-batch of RPN is set to be 256, and the base anchor size is [32, 64, 128, 256, 512].

The quality of the detection model is measured by AP and the max recall rate. AP is an indicator reflecting global performance and is the area value of the Precision-Recall curve. The calculation formula is as follows.

$$AP = \int_0^1 P(R) dR \quad (1)$$

In the formula, P is the accuracy of the model. Under the set threshold, it is the ratio of the correct sample number identified by the model to all samples inferred by the model. R is the recall rate of the model. Under the set threshold, it is the ratio of the correct sample number identified by the model to the actual total positive samples.

$$P = \frac{TP}{TP + FP} \quad (2)$$

$$R = \frac{TP}{TP + FN} \quad (3)$$

The existence of defects is a serious potential safety hazard. Therefore, the missed detection rate deserves to be paid more attention than the false detection rate in the detection of industrial weld joints. In this paper, the maximum recall rate with a threshold of 0.1 is used as the detection rate of the model.

$$R_{\max} = \frac{TP}{TP + FN} (\text{threshold} = 0.1) \quad (4)$$

The comparison of AP results of three models is shown in Table 4.

Table 4. Comparison of AP results

AP	Crack	Bar	Round	mAP
D(S)	0.414	0.396	0.652	0.396
D(S)+D(G)	0.468	0.471	0.742	0.560
D(S)+D(P)	0.517	0.698	0.810	0.675

As can be seen from the results in the table, image augmented by the geometric method has a limited effect on improving the performance of the model. While with the

method proposed in this paper, the model experienced a significant improvement in its performance even though the increased number of defeats is less than that of geometric method, This shows that the data augmentation method based on statistical histogram and Poisson fusion proposed by this paper is more effective than geometric method in terms of the data augmentation of typical defects in X radiographic welds.

The Precision-Recall curves of three groups of experiments are shown in Fig. 9. It can be seen from the figure that the AP value and the maximum recall rate of all the three groups are in an increasing trend. The maximum recall rate of the crack defect and the AP value of bar defect are improved significantly in the D (P) model, and other performance indicators are also improved.

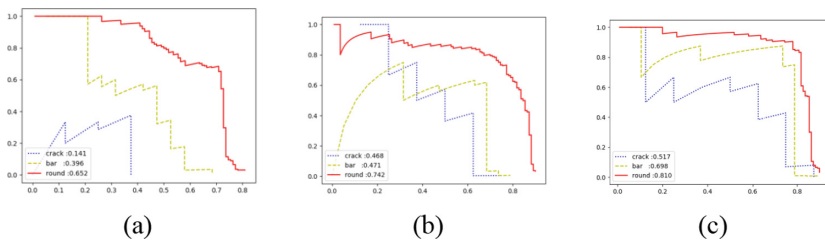


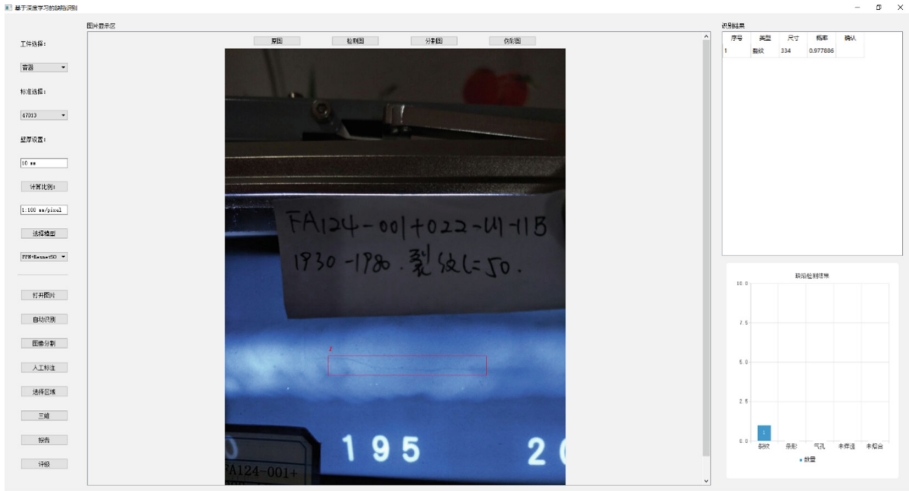
Fig. 9. Precision-Recall Curve (a) Experiment for D(S) (b) Experiment for D(S)+D(G) (c) Experiment for D(S)+D(P)

The maximum recall rate of three models for the above different data set is shown in Table 5. Compared with the geometric method, the proposed method can significantly improve the maximum recall rate of the model. For example, the recall rate of crack defects can reach 0.875. Crack is the most serious defect in a weld. If there is a crack in a weld, the weld must be sent back and repaired. Otherwise, it will cause serious accidents. Therefore, the improvement in the detection rate of crack defects is of great value for ensuring the safety of industrial welds.

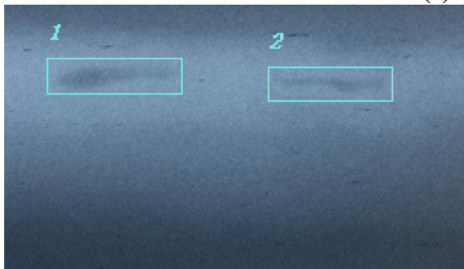
Table 5. Maximum recall rate of three models

R_{max}	Crack	Bar	Round
D(S)	0.375	0.684	0.809
D(S)+D(G)	0.750	0.789	0.890
D(S)+D(P)	0.875	0.895	0.900

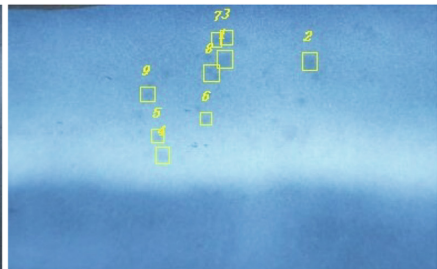
The automatic recognition system designed for X radiographic weld defects are shown in Fig. 10. It can be seen that the system has a relatively good detection effect for various defects when trained models are integrated into it. In addition, the quantitative and grading functions of defects have been completed in the system and can be preliminarily applied to the industrial field.



(a)



(b)



(c)

Fig. 10. Automatic Recognition System (a) Interface of System (b) Bar Defect Recognition (c) Round Defect Recognition

4 Conclusion

This paper has introduced a method based on histogram and Poisson fusion to simulate the edge corrosion effect of X radiographic film. The result shows that the data augmented by this method accord with the distribution characteristics of defects, and it has a significant improvement in the performance of the model. Because most defects are weak objects in industry, this paper uses FPN which is sensitive to fine-grained objects. The results show that the trained model has a good effect on the detection of typical weld defects. In addition, we have developed an intelligent detection system for industrial welds, which integrates the model into the system with strong performance so that it can be applied to the industrial field.

References

1. Xiao, H.: Research on automatic detection and recognition system of welding defect ray DR image. Nanchang Hangkong University (2017)
2. Ye, Z.: Research on automatic welding defect detection based on image processing. Nanjing University of Aeronautics and Astronautics (2017)
3. Mahmoudi, A., Rezagui, F.: Fast segmentation method for defects detection in radiographic images of welds. In: IEEE/ACS International Conference on Computer Systems & Applications. IEEE (2009)
4. Alaknanda, Anand, R.S., Kumar, P.: Flaw detection in radiographic weld images using morphological approach. *NDT & E Int.* **39**(1), 29–33 (2006)
5. Daum, W., Rose, P., Heidt, H.: Automatic recognition of weld defects in X radiographic-inspection. *Materialpruefung* **28**(6), 177–180 (1986)
6. Zou, Y., Du, D., Chang, B., et al.: Automatic weld defect detection method based on Kalman filtering for real-time radiographic inspection of spiral pipe. *NDT and E Int.* **72**, 1–9 (2015)
7. Shao, J., Du, D., Wang, L., et al.: Detection of low contrast thin line defect in X radiographic film digitized image of weld seam. *Nondestructive* **2010**(12)
8. Da Silva, R.R., Calôba, L.P., Siqueira, M.H.S., et al.: Evaluation of the relevant characteristic parameters of welding defects and probability of correct classification using linear classifiers. *Insight* **44**(10), 616–622 (2002)
9. Kumar, J., Anand, R.S., Srivastava, S.P.: Flaws classification using ANN for radiographic weld images. In: 2014 International Conference on Signal Processing and Integrated Networks (SPIN). IEEE, pp. 145–150 (2014)
10. Wang, Y., Sun, Y., Lv, P., et al.: Detection of line weld defects based on multiple thresholds and support vector machine. *NDT and E Int.* **41**(7), 517–524 (2008)
11. Boaretto, N., Centeno, T.M.: Automated detection of welding defects in pipelines from radiographic images DWDI. *NDT and E Int.* **86**, 7–13 (2017)
12. Liu, H., Guo, R.: Detection and identification of weld defects in petroleum steel pipes based on X radiographic image and convolutional neural network. *J. Instrum.* **2018**(4)
13. Chen, F.C., Jahanshahi, R.M.R.: NB-CNN: deep learning-based crack detection using convolutional neural network and Naïve Bayes data fusion. *IEEE Trans. Ind. Electron.* **65**, 4392–4400 (2017)
14. Suyama, F.M., Delgado, M.R., da Silva, R.D., et al.: Deep neural networks based approach for welded joint detection of oil pipelines in radiographic images with Double Wall Double Image exposure. *NDT E Int.* **105**, 46–55 (2019)
15. Qiang, T.: Radiographic Inspection. China Labor and Social Security press, Beijing (2007)
16. Pérez, P., Gangnet, M., Blake, A.: Poisson image editing. *ACM Trans. Graph. (TOG)* **22**(3), 313–318 (2003)
17. Sun, J., Li, L., Xiao, Z.: Image seamless Mosaic method based on adaptive gradient domain fusion. *Comput. Appl. Res.* **32**(09) (2015)
18. Krizhevsky, A., Sutskever, I., Hinton, G.E.: ImageNet classification with deep convolutional neural networks. *Commun. ACM* **60**(2), 2012 (2017)
19. Ren, S., He, K., Girshick, R., et al.: Faster R-CNN: towards real-time object detection with region proposal networks. *Comput. Vis. Pattern Recognit.* (2016)
20. Yun, R., Changren, Z., Shunping, X.: Small object detection in optical remote sensing images via modified faster R-CNN. *Appl. Sci.* **8**(5), 813 (2018)
21. Lin, T.Y., Dollár, P., Girshick, R., et al.: Feature pyramid networks for object detection. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2117–2125 (2017)



CARNet: Densely Connected Capsules with Capsule-Wise Attention Routing

Zhi-Xuan Yu, Ye He, Chao Zhu^(✉), Shu Tian, and Xu-Cheng Yin

School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, People's Republic of China
zhixuanYu@xs.ustb.edu.cn, YeHe.USTB@outlook.com,
{chaozhu, shutian, xuchengyin}@ustb.edu.cn

Abstract. Convolutional neural networks (CNNs) have been proven to be effective for image recognition, which plays an important role in cyber security. In this paper, we focus on a promising neural network, capsule network, which aims at correcting the deficiencies of CNNs. Routing procedure between capsules, which serves as a key component in capsule networks, computes coupling coefficients with complicated steps iteratively. However, the expensive computational cost poses a bottleneck for extending capsule networks deeper and wider to approach higher performance on complex data. To address this limitation, we propose a novel routing algorithm named *capsule-wise attention routing* based on attention mechanism. With a successful reduction of computational cost in the routing procedure, we construct a deep capsule network architecture named *CARNet*. Our CARNets are proven experimentally to outperform other state-of-the-art capsule networks on SVHN and CIFAR-10 benchmarks while reducing the amount of parameters by 62% at most.

Keywords: Cyber security · Image recognition · Capsule network · Attention mechanism

1 Introduction

Cyber security becomes more and more important nowadays as cyberspace infiltrates into our life rapidly. Every day billions of images containing massive information are generated and transmitted in cyberspace, which poses great challenges to the security of cyberspace. It is necessary for us to search for more efficient and robust methods of image recognition to retrieve useful information from images automatically.

Over the last decade, convolutional neural networks (CNNs) have been widely used in various challenging tasks in computer vision for its remarkable learning capacity. CNNs share weights across positions on the image to achieve translation invariance, which is reasonable but not robust enough when dealing with complex transformations caused by viewpoint changes or part deformation. To correct these deficiencies, Hinton et al. [5] proposed a concept of capsule, which

aims to learn features equivariant to transformations resulted from viewpoint changes. Built upon capsules, capsule networks [6, 11] had achieved state-of-the-art performance on MNIST and smallNORB benchmarks.

However, there is still a large room for capsule networks to approach state-of-the-art performance on natural image datasets. CapsNets [6, 11] comprise much fewer layers than current well-performed models such as ResNet [4] and DenseNet [7], which contain hundreds of layers. It has been empirically proven that neural networks with deeper and wider architecture are more capable of learning complex hierarchies inside visual entities. Naturally it is worthwhile to explore a deeper capsule network architecture for enhancing its performance on complex data. As discussed in [10], simply stacking up fully-connected capsule layers towards a deep architecture will lead to some undesired problems like expensive computational cost and gradient vanishing. To address these limitations, we start our work with an analysis of the routing algorithm which involves complicated computations.

Routing algorithm in the standard CapsNets routes capsules from low level to high level according to coupling coefficients, which are computed with multiple iterative steps. From another aspect, the routing procedure can be explained as a parallel attention mechanism. So we formulate the computation process as a regression of multiple attention maps and implement the computation of coupling coefficients by two fully-connected layers. Capsules at one position are taken as input to the two-layer subnetwork to output coupling coefficients. Weights in the fully-connected layers are shared across different positions, so capsules at different positions can be routed according to the same criterion. As a result, the routing procedure is feasible to be accomplished in one stage and performed with much less computational cost. We name this novel routing algorithm as *Capsule-wise Attention Routing*, since our motivation comes from attention mechanism. Besides the change in computing coupling coefficients, another modification is the adoption of 2D convolution with larger kernel to transform capsules from low level to high level. Since the original matrix multiplication is equivalent to 1×1 convolution, the modification can be regarded as an enlargement of the convolutional kernel. To prevent the amount of parameters increasing proportionally to the size of convolutional kernel, we implement the convolutions with the idea from depthwise separable convolutions [2].

As the computational cost in routing gets successfully reduced, we are able to build up a deeper capsule network with more capsule layers. We name our model as *CARNet* after the routing algorithm we proposed previously. In addition, we set skip connections between different levels of capsules to help transport gradient flow into low layers during training. With the skip connections, capsules at low level can be routed directly to the top capsules and involved in the final inference.

The rest of our paper is organized as follows. In Sect. 2, we review the related work on capsule networks. In Sect. 3 we introduce how capsule-wise attention routing works and elaborate the architecture of CARNet. In Sect. 4, we evaluate capsule-wise attention routing and CARNets on four object recognition

benchmarks including MNIST, Fashion-MNIST, SVHN and CIFAR-10. Finally we summarize our work and discuss possible future work in Sect. 5.

2 Related Work

Capsule is a neural unit aiming to learn viewpoint-equivariant instantiation parameters and viewpoint-invariant activation probability of some visual entity in images. In dynamic capsules [11], a capsule is organized as a vector called activation vector. Entries of the vector are explained as multiple implicitly defined instantiation parameters of the visual entity, while the length of the vector is the probability indicating the presence. In EM capsules [6], instantiation parameters and activation probability were separately represented by a 4×4 pose matrix and a logistic unit. The complicated internal structure determines that capsule has more complicated intra-computation and inter-computation than single neuron.

Routing procedure happens between adjacent capsule layers. Each capsule in the lower layer will first make predictions for capsules in the higher layer respectively. If two lower capsules make similar predictions for one higher capsule, they are supposed to be routed to that capsule. For every higher capsule, it will receive a cluster of predictions from capsules below, and aggregate them as output. With the routing-by-agreement mechanism, CapsNet not only achieved state-of-the-art performance on MNIST and smallNORB benchmarks but also showed out superiority in distinguishing overlapping digits [11] and resisting white box adversarial attacks [6].

Capsule networks have been further explored in the literature. Wang and Liu [12] formulated dynamic routing as an optimization problem of minimizing clustering loss with a KL regularization term and modified the routing procedure with motivation from solving a clustering object function. Lenssen et al. [9] proposed group equivariant capsule networks with provable equivariance and invariance properties. Zhang et al. [15] proposed two fast routing methods based on kernel weighted density estimation. These works improved the routing algorithm from different aspects but the networks were still relatively shallow.

Concurrent with our work, Rajasegaran et al. [10] proposed a deep capsule network architecture named DeepCaps with a similar motivation to ours. DeepCaps includes 17 capsule layers and impressively outperforms the state-of-the-art capsule networks on Fashion-MNIST, SVHN and CIFAR-10 with much less parameters than the original CapsNet. DeepCaps maintains the framework of dynamic routing and adopts 3D convolution to implement the transformation in routing. Weights among input capsules are shared so that the computational cost can be reduced. DeepCaps also proposes a class-independent reconstruction network at the top of network. Different from DeepCaps, we propose a novel routing algorithm in which the coupling coefficients are computed by a two-layer subnetwork and the transformation is performed by 2D convolution. Besides, our model uses skip connections to connect capsules at different levels in a different way from DeepCaps. And the reconstruction network is not considered for regularization. Performance of DeepCaps and our proposed approach will be compared in Sect. 4.

3 CARNet

In this section, the details of the proposed capsule-wise attention routing algorithm and the architecture of CARNet are presented.

3.1 Capsule-Wise Attention Routing

Consider an intermediate capsule layer that processes N_l input capsules and outputs N_{l+1} capsules. We denote the i -th capsule in layer l at some position by $\mathbf{u}_i^{(x,y)} \in \mathbb{R}^{a_l}$, where (x, y) is the coordinate of capsule and a_l is the dimension of activation vector.

First, capsules at one position are concatenated as a vector $\mathbf{u}^{(x,y)}$. Since the computation of coupling coefficients across positions are performed in the same way, we omit the coordinate for clarity below. Then we pass \mathbf{u} to two cascaded fully-connected layers to regress the log prior probabilities $\mathbf{h} \in \mathbb{R}^{N_l \times N_{l+1}}$. We choose vector \mathbf{u} as the input of the subnetwork because \mathbf{u} is supposed to aggregate all the semantic information of its local receptive field at current layer, which can help generate more proper coupling coefficients. The computation of \mathbf{h} is written as:

$$\mathbf{h} = \mathbf{W}_2 \cdot g(\mathbf{W}_1 \mathbf{u} + \mathbf{b}_1) + \mathbf{b}_2, \quad (3.1)$$

where $g(\cdot)$ is the ReLU function. We reorganize vector \mathbf{h} into an $N_l \times N_{l+1}$ matrix and subsequently feed it to the softmax function to get coupling coefficients \mathbf{c} .

$$\hat{\mathbf{u}}_{i|j} = c_{ij} \mathbf{u}_i, \quad c_{ij} = \frac{\exp(h_{ij})}{\sum_k \exp(h_{ik})}, \quad (3.2)$$

where c_{ij} is the coupling coefficient of capsule i and capsule j , $\hat{\mathbf{u}}_{i|j}$ is a weighted activation vector passed from capsule i to capsule j . Each capsule in the higher layer will receive N_L weighted activation vectors from the lower layer and then transform them into the higher capsule space. Dynamic routing implements the transformation from low level to high level by matrix multiplication (1×1 convolution), which makes no use of features in the neighbourhood. Here we adopt 2D convolution with larger receptive field to perform the transformation.

In details, for capsule j , all the weighted capsules $\{\hat{\mathbf{u}}_{i|j} \mid 1 \leq i \leq N_l\}$ are concatenated to be $\hat{\mathbf{u}}_j$, which is followed by a Conv-BN-ReLU block to generate output capsule \mathbf{v}_j . Parameters in the blocks are not shared among higher capsules, so these parallel blocks can learn part-whole relationship independently of each others.

These convolutions are performed parallelly in capsules, which are equivalent to group convolutions. So we implement the parallel convolutions with inspiration from depthwise separable convolution [2], which splits the original convolutional operation into a depthwise convolution and a pointwise convolution. First, we concatenate the weighted capsules and perform depthwise convolution on it. Second, we separate the tensor back to the form of capsules and perform pointwise matrix multiplication. When the receptive field is 1×1 , we would omit the

Algorithm 1. Capsule-wise attention routing algorithm.

Input: The set of capsules in layer l , $\mathbf{U} = \{\mathbf{u}_i^{(x,y)} \mid \mathbf{u}_i^{(x,y)} \in \mathbb{R}^{a_l}, 1 \leq i \leq N_l, 1 \leq x \leq W_l, 1 \leq y \leq H_l\}$, where N_l is the number of capsules, W_l and H_l are the width and height of the feature map.

- 1: **procedure** ROUTING(\mathbf{U})
- 2: for every position (x, y) :
- 3: $\mathbf{u} \leftarrow [\mathbf{u}_1; \mathbf{u}_2; \dots; \mathbf{u}_{N_l}]$;
- 4: $h \leftarrow \mathbf{W}_2 \cdot g(\mathbf{W}_1 \mathbf{u} + \mathbf{b}_1) + \mathbf{b}_2$;
- 5: for every capsule i in layer l :
- 6: for every capsule j in layer $(l+1)$:
- 7: $c_{ij} = \exp(h_{ij}) / \sum_k \exp(h_{ik})$
- 8: $\hat{\mathbf{u}}_{i|j} \leftarrow c_{ij} \mathbf{u}_i$;
- 9: $\hat{\mathbf{u}}_j \leftarrow [\hat{\mathbf{u}}_{1|j}; \hat{\mathbf{u}}_{2|j}; \dots; \hat{\mathbf{u}}_{N_l|j}]$;
- 10: for every capsule j in layer $(l+1)$:
- 11: $\hat{\mathbf{U}}_j \leftarrow \{\hat{\mathbf{u}}_j^{(x,y)} \mid 1 \leq x \leq W_l, 1 \leq y \leq H_l\}$;
- 12: $\mathbf{V}_j \leftarrow \text{Conv-BN-ReLU}_j(\hat{\mathbf{U}}_j)$;

return $\mathbf{V} = \{\mathbf{V}_j\}$

first step and perform the second step only, which is equivalent to the transformation in dynamic routing. By this method, we avoid using convolution for each capsule tensor iteratively and take advantage of the speed-up of convolution. In addition, for kernel size $k > 1$, our implementation would reduce the amount of parameters used for transformation by

$$\Delta N_{param} = k^2 N_l a_l + N_l a_l N_{l+1} a_{l+1} - k^2 N_l a_l N_{l+1} a_{l+1}. \quad (3.3)$$

Since $k^2 \ll N_l a_l$ for every layer l in practice, so the reduction rate of parameters is nearly $1/k^2$, which is considerable even when $k = 3$.

Activation probability of a capsule still depends on the length of the activation vector as in [11]. But we don't squeeze the length of vector into $[0, 1]$ at the end of routing by the squashing function. We only compute the activation probability by function

$$P(\mathbf{v}) = \frac{\|\mathbf{v}\|^2}{1 + \|\mathbf{v}\|^2} \quad (3.4)$$

if the probability is needed. We skip the vector-squashing operation in the intermediate capsules and choose ReLU as the activation function to prevent gradient vanishing.

Capsule-wise attention routing computes the coupling coefficients by a two-layer subnetwork, turning the mechanism behind from routing-by-agreement to routing-by-learning. In this way, we avoid computing coupling coefficients iteratively and reduce the cost. Besides, since the computation of coupling coefficients and the low-to-high transformation can both be implemented by convolutional operations, the speed of inference can be accelerated with GPUs. Thanks to the reduction of computational cost in each capsule layer, we can cascade more capsule layers to attain a higher learning capacity.

3.2 CARNet Architecture

The architecture of our proposed CARNet is shown in Table 1. Similar to the standard capsule networks, our deep capsule network starts with several convolutional layers, which extract low-level features from the original image. Then the feature map is reorganized into the form of capsule tensor and passed through cascaded capsule layers. At the top of the network, we compute the prediction probability of each category based on the corresponding capsule. The details of CARNet are demonstrated as follows.

Table 1. CARNet architecture for SVHN and CIFAR-10. Note that “conv” in the table refers to Conv-BN-ReLU block and “CAR” is short for “capsule-wise attention routing”. All the convolutional layers are performed with padding except the ones with superscript “*”. Layers bracketed together comprise a capsule block.

Stage	Output Size	N_{channel}	N_{capsule}	N_{atom}	Layer
Convolution	32×32	128	–	–	conv(5 × 5, stride 1)
	16×16	256	–	–	conv(3 × 3, stride 2)
	16×16	256	–	–	conv(3 × 3, stride 1) × 3
Primary Capsules	16×16	–	32	8	reshape
Capsule-1.x	4×4	–	16	8	$\begin{bmatrix} \text{CAR}(3 \times 3, \text{stride } 1) \\ \text{CAR}(3 \times 3, \text{stride } 2) \\ \text{CAR}(3 \times 3, \text{stride } 1) \end{bmatrix} \times 2$
Capsule-2.x	2×2	–	16	8	$\begin{bmatrix} \text{CAR}(1 \times 1, \text{stride } 1) \\ \text{CAR}(3 \times 3, \text{stride } 1)^* \\ \text{CAR}(1 \times 1, \text{stride } 1) \end{bmatrix}$
Final capsules	1×1	–	10	16	CAR(2 × 2, stride 1)*
Probability computing	1×1	–	10	–	$P(\mathbf{v}) = \frac{\ \mathbf{v}\ ^2}{1 + \ \mathbf{v}\ ^2}$

Low-Level Feature Extraction. CapsNet proposed in [11] uses a single convolutional layer with a relatively large receptive field to extract low-level features from the image. The convolution is performed without padding, so a large receptive field can help scale down the size of feature map and further reduce the computational cost in the subsequent capsule layers. While in CARNet, to reap the benefit of deeper networks, we replace the single convolutional layer by multiple cascaded convolutional layers with smaller receptive field. And we also use convolutions with zero padding to keep the size of some feature maps fixed.

Skip Connections. We combine three cascaded capsule layers as a single capsule block and set short paths to connect capsule blocks at different levels. The aim of short paths is to downsample lower capsules to make their size consistent with higher ones and then merge them together.

Let us denote the input and output of the n -th capsule block by \mathbf{U}_n and \mathbf{V}_n . Due to the convolutional operations in the capsule block, \mathbf{V}_n would get a smaller size than \mathbf{U}_n . We use a 1×1 pooling with the same stride and padding (as the convolutional layer) to downsample the input \mathbf{U}_n . So the receptive field of the downsampled tensors \mathbf{U}'_n are center-aligned to the receptive field of \mathbf{V}_n at every position. Subsequently \mathbf{U}'_n and \mathbf{V}_n are concatenated and fed to the next capsule block, i.e. $\mathbf{U}_{n+1} = [\mathbf{U}'_n; \mathbf{V}_n]$. In this way, lower capsules with the same receptive field centers are preserved and delivered to any higher capsule blocks by the skip connections, which means capsules at all levels would make contribution to the final result of classification. In other words, every capsule block is allowed to receive all the outputs of its preceding capsule blocks to generate its own output (Fig. 1).

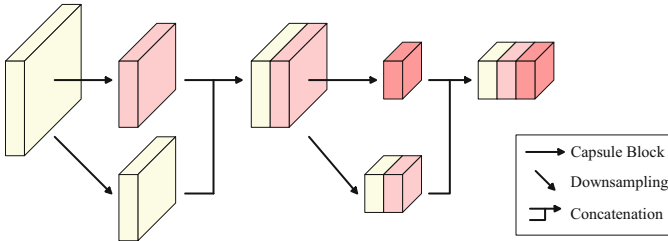


Fig. 1. Short paths connecting capsules in different levels.

Implementation Details. At the bottom of CARNet, we set five convolutional layers to extract features with 256 channels from input image. Each convolutional layer is followed by a BN layer and an activation function ReLU. Then we split up the tensor into 32 tensors with 8 channels, termed primary capsules. Primary capsules are subsequently fed to three cascaded capsule blocks. Every capsule layers in the blocks output $8D$ -capsules of 16 types. Skip connections merge capsules from preceding capsule blocks and transport them to the next capsule block. Finally, the primary capsules and capsules from three capsule blocks would be merged and fed to the final capsule layer to generate 10 $16D$ category-specified capsules, from which we compute the recognition probability by Eq. 3.4.

3.3 Loss Function

The loss function we adopted is margin loss proposed in [11], defined as

$$L = \max(0, m^+ - \|\mathbf{v}_t\|)^2 + \lambda \sum_{i \neq t} \max(0, \|\mathbf{v}_i\| - m^-)^2, \quad (3.5)$$

where t is index of the correct category. We use $m^+ = 0.95$ and $m^- = 0.05$ as the upper bound for the correct category and lower bound for the wrong category. The weight for losses from wrong categories λ is set as 0.5 for the whole training procedure.

4 Experiments

We empirically evaluated our capsule-wise attention routing and CARNet on four object recognition benchmarks including MNIST, Fashion MNIST, SVHN and CIFAR-10. Each of them collects images from 10 categories. We implemented CARNet in TensorFlow [1] framework and trained our models on GTX 1080 Ti GPUs. We used Adam optimizer [8] for the training and set the initial learning rate as 0.001, which would get reduced by 0.5 every 20,000 steps.

4.1 Datasets

MNIST and Fashion-MNIST. MNIST is a dataset of handwritten digit images while Fashion-MNIST is a dataset of fashion product images. MNIST and Fashion-MNIST provide images of the same amount (60,000 images for training and 10,000 for test) and in the same format (28×28 greyscale image). All images are captured in white background. For every training image, we randomly shifted it in every directions by up to 2 pixels. No preprocessing was performed for the test images.

SVHN. The Street View House Numbers dataset provides 32×32 RGB images containing numbers in natural scene. A large number of images are available for training (604,388) and test (26,032). Our training and test were performed without data preprocessing and data augmentation.

CIFAR-10. CIFAR-10 dataset is also a natural image dataset. The objects in images come from objects in our daily life. 50,000 training images and 10,000 test images are provided. The images are also 32×32 color images. During training, we perform random shift, random horizontal flipping and random adjustment of brightness and contrast as the data preprocessing. Both the training images and the test images are normalized to have zero mean and unit standard variance before they were fed to the network.

4.2 Capsule-Wise Attention Routing in CapsNet

To evaluate the effectiveness of our novel routing algorithm, we first designed an experiment to compare capsule-wise attention routing with dynamic routing in a shallow capsule network.

We trained a wider version of CapsNet¹, in which the number of intermediate capsules increased to 32 and the dimensions of activation vectors increased to 8 and 16 in primary capsule layer and final capsule layer. Then we got another model by replacing the dynamic routing procedure with two layers of capsule-wise attention routing in the final capsule layer. Note that we don't set reconstruction networks for both of them. Details of the networks are depicted in Table 2.

As shown in Table 3, CapsNet with capsule-wise attention routing consumes only half of parameters in its counterpart but achieves higher accuracies on both SVHN and CIFAR-10. The replacement of routing procedure also helps to speed up the training of CapsNet by about 50%.

Table 2. Architectures of two capsule networks. ‘‘CapsNet*’’ represents CapsNet with capsule-wise attention routing. Number n in ‘‘dynamic routing $\times n$ ’’ indicates the iteration times in dynamic routing.

Stage	N_{channel}	N_{capsule}	N_{atom}	Layer	
				CapsNet	CapsNet*
Convolution	64	–	–	conv(9×9 , stride 1)	
Primary capsules	256	–	–	conv(9×9 , stride 2)	
	–	32	8	reshape & vector squashing	
Final capsules	–	10	16	transformation	CAR(5×5 , stride 1)
				dynamic routing $\times 3$	CAR(4×4 , stride 1)
Probability computing	–	10	–	$P(\mathbf{v}) = \ \mathbf{v}\ $	$P(\mathbf{v}) = \frac{\ \mathbf{v}\ ^2}{1+\ \mathbf{v}\ ^2}$

Table 3. Accuracies (%) of CapsNet and CapsNet* on SVHN and CIFAR-10.

Model	Param.	FPS	SVHN	CIFAR-10
CapsNet	3.96M	1.12K	95.82	81.80
CapsNet*	1.94M	1.68K	96.83	82.56

4.3 Performance of CARNet

We trained our CARNet on four benchmarks and compared the performance with proposed capsule networks. We also evaluated the effect of skip connections

¹ The CapsNet we trained is wider than CapsNet for SVHN [11], which consists of a convolutional layer with 64 channels, a primary capsule layer with 16 $6D$ -capsules and a final capsule layer with 10 $8D$ -capsules.

in our model. In Table 4 we list out the error rates achieved by our models, CapsNet, DeepCaps and variants of ResNet and DenseNet. All the results are achieved by single model.

As capsule network goes deeper, the performance gets improved accordingly especially on natural image datasets. CARNet without skip connections leads the performance of capsule networks on SVHN and CIFAR-10 and performs close to the state-of-the-art capsule networks on MNIST and Fashion-MNIST. While with skip connections, the performance can be further improved on four benchmarks. Our best model achieves an accuracy of 97.72% on SVHN and 92.46% on CIFAR-10 that surpass DeepCaps by 0.56% and 1.45% respectively.

Besides, CARNets also show out a more efficient capability of utilizing parameters than the existing capsule networks. CARNet consumes 3.96M parameters, which can be cut down to 2.73M when the skip connections are removed. The amount of trainable parameters in CARNet is less than CapsNet for MNIST (8.2M) or DeepCaps for CIFAR-10 (7.22M), and much less than other well-performed CNN-based models listed in Table 4. The efficiency of utilizing parameters comes from the use of convolutions in the transformation step in capsule-wise attention routing, which allows capsules to leverage local features when learning part-whole relationship inside the visual entity. On the other hand, the increment in the amount of parameters is controlled within an acceptable limit thanks to the implementation based on depthwise separable convolutions.

Table 4. Accuracies (%) on MNIST, Fashion-MNIST, SVHN and CIFAR-10 datasets. “SC” is short for “skip connections”. Results in **bold** are the best in the domain of capsule networks.

Model	Param.	MNIST	F-MNIST	SVHN	CIFAR-10
ResNet v2 [5]	10.2M	–	–	–	95.38
ResNeXt [13]	68.1M	–	–	–	96.42
DenseNet [7]	27.2M	–	95.40	98.41	96.26
Wide ResNet [14]	36.5M	–	95.90	–	95.83
WRN + Random Erasing [16]	36.5M	–	96.35	–	96.92
CapsNet [11]	8.2M	99.75	93.62	95.70	–
FREM [15]	8M	99.62	93.80	–	85.70
HitNet [3]	–	99.68	92.30	94.50	73.30
DeepCaps [10]	7.22M	99.72	94.46	97.16	91.01
CARNet w/o SC (Ours)	2.73M	99.72	94.30	97.61	91.88
CARNet with SC (Ours)	3.96M	99.74	94.46	97.72	92.46

5 Conclusion

In this paper, we proposed a novel routing algorithm, capsule-wise attention routing, which uses a two-layer subnetwork to regress coupling coefficients as

multiple attention maps. We adopted 2D convolution to replace the linear transformation so that local features can be utilized in transforming capsules from low level to high level. In addition, we formulated the parallel transformation among capsules as group convolutions and implemented it with the inspiration from depthwise separable convolutions. The new implementation was consistent with the original transformation in dynamic routing and was proven to help utilize parameters more efficiently.

Based on capsule-wise attention routing, we further proposed a deep capsule network called CARNet. We stacked multiple capsule layers in our model and set skip connections to densely connect different levels of capsules. CARNet achieved state-of-the-art performance on MNIST and Fashion-MNIST and outperformed the state-of-the-art capsule network on SVHN and CIFAR-10, which are both datasets containing natural images. It is an inspiring step of capsule networks to approach the state-of-the-art performance on natural image datasets, but the performance gap still exists between capsule network based models and the state-of-the-art CNN models. In the future, we plan to explore more efficient routing algorithm and make further attempt to deepen the capsule network architecture for better performance on complex data.

Acknowledgements. This work was supported by National Natural Science Foundation of China under Grant 61703039 and Beijing Natural Science Foundation under Grant 4174095.

References

1. Abadi, M., et al.: Tensorflow: large-scale machine learning on heterogeneous distributed systems. CoRR abs/1603.04467 (2016)
2. Chollet, F.: Xception: deep learning with depthwise separable convolutions. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, 21–26 July 2017, pp. 1800–1807 (2017)
3. Deliège, A., Cioppa, A., Droogenbroeck, M.V.: HitNet: a neural network with capsules embedded in a hit-or-miss layer, extended with hybrid data augmentation and ghost capsules. CoRR abs/1806.06519 (2018)
4. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: 2016 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2016, Las Vegas, NV, USA, 27–30 June 2016, pp. 770–778 (2016)
5. Hinton, G.E., Krizhevsky, A., Wang, S.D.: Transforming auto-encoders. In: Honkela, T., Duch, W., Girolami, M., Kaski, S. (eds.) ICANN 2011. LNCS, vol. 6791, pp. 44–51. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21735-7_6
6. Hinton, G.E., Sabour, S., Frosst, N.: Matrix capsules with EM routing. In: 6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada, 30 April–3 May 2018, Conference Track Proceedings (2018)
7. Huang, G., Liu, Z., van der Maaten, L., Weinberger, K.Q.: Densely connected convolutional networks. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, 21–26 July 2017, pp. 2261–2269 (2017)

8. Kingma, D.P., Ba, J.: Adam: a method for stochastic optimization. In: 3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, 7–9 May 2015, Conference Track Proceedings (2015)
9. Lenssen, J.E., Fey, M., Libuschewski, P.: Group equivariant capsule networks. In: Advances in Neural Information Processing Systems 31: Annual Conference on Neural Information Processing Systems 2018, NeurIPS 2018, Montréal, Canada, 3–8 December 2018, pp. 8858–8867 (2018)
10. Rajasegaran, J., Jayasundara, V., Jayasekara, S., Jayasekara, H., Seneviratne, S., Rodrigo, R.: DeepCaps: going deeper with capsule networks. CoRR abs/1904.09546 (2019)
11. Sabour, S., Frosst, N., Hinton, G.E.: Dynamic routing between capsules. In: Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, Long Beach, CA, USA, 4–9 December 2017, pp. 3859–3869 (2017)
12. Wang, D., Liu, Q.: An optimization view on dynamic routing between capsules. In: 6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada, 30 April–3 May 2018, Workshop Track Proceedings (2018)
13. Xie, S., Girshick, R.B., Dollár, P., Tu, Z., He, K.: Aggregated residual transformations for deep neural networks. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, 21–26 July 2017, pp. 5987–5995 (2017)
14. Zagoruyko, S., Komodakis, N.: Wide residual networks. In: Proceedings of the British Machine Vision Conference 2016, BMVC 2016, York, UK, 19–22 September 2016 (2016)
15. Zhang, S., Zhou, Q., Wu, X.: Fast dynamic routing based on weighted kernel density estimation. In: Lu, H. (ed.) ISAIR 2018. SCI, vol. 810, pp. 301–309. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-04946-1_30
16. Zhong, Z., Zheng, L., Kang, G., Li, S., Yang, Y.: Random erasing data augmentation. CoRR abs/1708.04896 (2017)



A Malware Identification and Detection Method Using Mixture Correntropy-Based Deep Neural Network

Xiong Luo^{1,2,3(✉)}, Jianyuan Li⁴, Weiping Wang^{1,2,3}, Yang Gao⁵,
and Wenbing Zhao⁶

¹ School of Computer and Communication Engineering,
University of Science and Technology Beijing, Beijing 100083, China
xluo@ustb.edu.cn

² Beijing Key Laboratory of Knowledge Engineering for Materials Science,
Beijing 100083, China

³ Beijing Intelligent Logistics System Collaborative Innovation Center,
Beijing 101149, China

⁴ Department of Electrical and Computer Engineering, University of Pittsburgh,
Pittsburgh, PA 15261, USA

⁵ China Information Technology Security Evaluation Center,
Beijing 100085, China

⁶ Department of Electrical Engineering and Computer Science,
Cleveland State University, Cleveland, OH 44115, USA

Abstract. With the rapid development of CPS technology, the identification and detection of malware has become a matter of concern in the industrial application of CPS. Currently, advanced machine learning methods such as deep learning are popular in the research of malware identification and detection, and some progress has been made so far. However, there are also some problems. For example, considering the existing noise or outliers in the datasets of malware, some methods are not robust enough. Therefore, the accuracy of classification of malware still needs to be improved. Aiming at it, we propose a novel method thought the combination of correntropy and deep neural network (DNN). In our proposed method for malware identification and detection, given the success of mixture correntropy as an effective similarity measure in addressing complex dataset with noise, it is therefore incorporated into a popular DNN, i.e., convolutional neural network (CNN), to reconstruct its loss function, with the purpose of further detecting the features of outliers. We present the detailed design process of our proposed method. Furthermore, the proposed method is tested both on a popular benchmark dataset and a real-world malware classification dataset, to verify its learning performance.

Keywords: Mixture correntropy · Convolutional Neural Network (CNN) · Malware detection

1 Introduction

Cyber-physical systems (CPS) refer to a system that integrates computation, networking, and physical processes, where embedded computers and networks achieve real-time control of the physical process through the feedback mechanism [1]. With the development and popularization of CPS technologies, there are numerous physical equipments depending on computers and networks to achieve functional expansion, which will upgrade industrial products and technologies. For those large-scale complex systems, safety and reliability always are important issues. CPS intimately integrates the virtual world with the physical world, once the virtual world is attacked, it will inevitably affect the physical world. Hence, the information protection is essential for the CPS implementation. For the issue of information security in CPS, it has become critical to identify and detect malware on Android [2].

Generally speaking, malware refers to any cyber-attack performed in Internet. The increase of malware has become a serious issue. Due to the serious hazard the malware has brought to the internet, various methods have been proposed to defense the malicious software. Currently, there are two main methods to detect and analyze malware. One is the classical static and dynamic analysis method. Static malware feature analysis includes compile time, shell information, import functions, suspicious strings, and some others. For example, an algorithm was designed to achieve statistical binary content analysis of Fileprint [3], and a statistical value could be calculated to extract malicious communication pattern [4]. If the sample is highly encrypted, the static feature analysis may not provide much valuable information, therefore, dynamic behavior analysis technology is needed, which is also called behavior monitoring. For example, an approach was proposed for the network analysis of anomalous traffic events (NATE) [5]. The other one is based on machine learning methods, such as malware analysis based on long short-term memory (LSTM) [6], one-class support vector machine based malware detection [7], detecting malware using a deep belief network (DBN) [8], and many others. Then, with the rapid development of machine learning algorithms, more and more intelligent methods are accordingly developed to deal with malware issues.

However, these methods mentioned above also have their limitations. In particular, there may be noise or outliers in some malware data, and then the robustness of some methods is not satisfactory enough. Therefore, the accuracy of feature extraction and classification of malware is necessary to be further improved. In response to these limitations, motivated by the popular malware classification method on the basis of deep neural network (DNN) [9], we propose a novel algorithm through the use of a new similarity measure, i.e., mixture correntropy.

Correntropy is a kernel-based local similarity function [10]. Since one of the significant features of correntropy is robust to noise and large outliers [11], it is widely applied in various fields. Specifically, it can be also used within deep learning framework to improve the computational performance. For example, the stacked extreme learning machine was presented with the correntropy-optimized temporal principle component analysis (CTPCA) [12], furthermore the generalized correntropy-based stacked autoencoder (GC-SAE) was developed [13]. More recently, on the basis of correntropy, mixture correntropy is proposed and widely employed in various applications [14]. Considering that there is no application of mixture correntropy in

Android malware identification and detection, through the combination of a popular DNN, i.e., convolutional neural network (CNN) [15], we develop a novel application by proposing a mixture correntropy-based CNN, and thus using it to improve the classification accuracy for malware.

The main contributions of this paper can be summarized as follows.

- (1) In consideration of those advantages of mixture correntropy in addressing data more flexibly and stably, it is hereby incorporated into the implementation framework of CNN, through the reconstruction of loss function in CNN. Then, it is expected that the learning performance can be further improved by using our proposed method.
- (2) Our proposed method is used to handle an important but challenging issue in the guarantee of information security in CPS, which is the Android malware identification and detection. Compared to other traditional malware detection methods, the learning performance in relation to accuracy and robustness would be further improved owing to the use of mixture correntropy.

The remainder of this paper is organized as follows. In Sect. 2, we provide a simple analysis on the related technologies, including correntropy and mixture correntropy, CNN, and deep learning-based malware detection. In Sect. 3, the detailed design process of our proposed method is presented. The experiment results and discussion are given in Sect. 4. Finally, this paper is concluded in Sect. 5.

2 Background

2.1 Correntropy and Mixture Correntropy

Correntropy. Inspired by information theoretic learning (ITL) [16], correntropy is an extension of the basic definition of correlation function, which is a similarity measure function of two random variables (X, Y). It is defined as:

$$V(X, Y) = E[k_\sigma(X - Y)] = \int k_\sigma(x - y)dF_{XY}(x, y) \tag{1}$$

where $k_\sigma(\cdot)$ denotes any type of kernel function with bandwidth of σ , \mathbf{E} is the expectation operator, $F_{XY}(x, y)$ refers to the joint distribution of (X, Y) . Without mentioned otherwise, the kernel function in this paper takes Gaussian kernel:

$$k_\delta(x, y) = G_\sigma(e) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{e^2}{2\sigma^2}\right) \tag{2}$$

where e refers to $(x - y)$. Correntropy is symmetric, positive, and bounded, and contains all even moments of arbitrary variables [17]. Since in real-world data processing tasks, the joint probability density (PDF) of samples is usually unknown, and sample sets $\{x_i, y_i\}_{i=1}^N$ is limited, the sample estimator can be defined as:

$$\widehat{V}(X, Y) = \frac{1}{N} \sum_{i=1}^N k_\sigma(x_i - y_i) \tag{3}$$

which is also named as the empirical correntropy.

Mixture Correntropy. On the basis of correntropy, the concept of mixture correntropy is generated [14]. When correntropy is applied to process data, the kernel bandwidth σ directly affect the performance of the function. Concisely, a small value of bandwidth allows algorithms to perform better in processing data with noise and outliers, but it may also lead to a slow convergence. Conversely, a large value of bandwidth will cause the reduction of robustness. Therefore, the mixture correntropy is proposed to improve the original algorithm, and it is defined as:

$$M(X, Y) = E[\alpha k_{\sigma_1}(e) + (1 - \alpha)k_{\sigma_2}(e)] \tag{4}$$

where σ_1 and σ_2 are bandwidths of two kernel functions, and $0 \leq \alpha \leq 1$ refers to mixture coefficient that controls the ratio between two kernel functions. In addition, the sample estimator can be defined as:

$$\widehat{M}(e) = \frac{1}{N} \sum_{i=1}^N [\alpha k_{\sigma_1}(e_i) + (1 - \alpha)k_{\sigma_2}(e_i)] \tag{5}$$

where e_i refers to $(x_i - y_i)$. In this paper, we take the mixture of two Gaussian kernel. Here, $\widehat{M}(e)$ can be represented as:

$$\widehat{M}(e) = \frac{1}{N} \sum_{i=1}^N [\alpha G_{\sigma_1}(e_i) + (1 - \alpha)G_{\sigma_2}(e_i)] \tag{6}$$

2.2 Convolutional Neural Network (CNN)

CNN is a type of feedforward neural networks with convolutional computation, and it can be regarded as a DNN. As one of the representative algorithms of deep learning, it has been utilized in various fields, such as the image classification [18], object recognition [19], and natural language processing [20]. CNN mimics the visual perception mechanism of living organisms, and thus can be employed for the supervised learning and unsupervised learning.

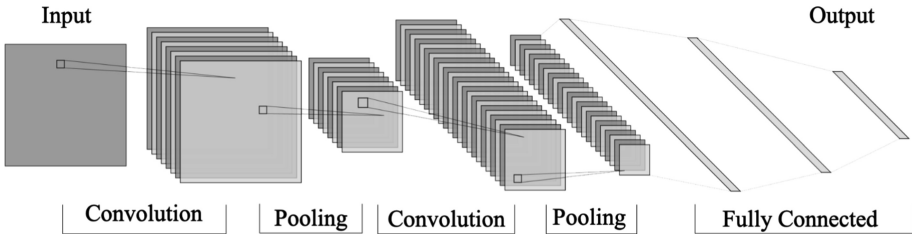


Fig. 1. LeNet-5 model.

Here, we implement a LeNet-5 model [15], which is a common model of CNN. As shown in Fig. 1, there are 7 layers in LeNet-5, including 2 convolutional layers, 2

pooling layers, and 3 fully-connected layers. Each layer contains different number of training parameters. The function of convolutional layer is to extract features from the input data. Thereafter, the feature graph will be transferred to the pooling layer for feature selection and information filtering. Fully-connected layers only pass signals to other fully-connected layers. The feature graph loses its spatial topology in the fully-connected layers and is expanded as a vector. The output layer uses the softmax function to output classification labels.

2.3 The Deep Learning-Based Malware Detection

Deep learning, as a kind of advanced data mining strategy in the machine learning area, has gained tremendous attention and inspired diverse practical applications. To address the security issues of CPS, a variety of deep learning-based malware detection methods have been proposed over the years. An originally designed deep learning model was performed to analyze more than 200 features extracted from static analysis and dynamic analysis of Android App [21]. Using convolutional and recurrent network layers, a neural network was constructed to achieve the best features of malware system [22]. Echo state networks (ESN) and recurrent neural networks (RNN) are utilized for the projection stage to realize the feature extraction [23]. Because the number of potential features would be very large, the random projections were explored to reduce the dimensionality of input data, and several large-scale neural network systems were trained to implement the classification [24].

However, none of the aforementioned methods specifically involved the issue of robustness in the algorithm. Hence, considering that there may be some noise and outliers in the malware data, our algorithm is proposed.

3 The Proposed Method

The application programming interface (API) call sequences are firstly inputted into our proposed method. After preprocessing these data, our mixture correntropy-based convolutional neural network model is used as a classifier to achieve classification for malware.

3.1 Training Convolutional Neural Network with Mixture Correntropy-Based Loss Function

Here, the loss means the cost for predicting the label to be $f(x)$, the predicted label, instead of the true label. In classification tasks, the algorithm aims to maximize the similarity between the output and the labels, in other word, the correntropy can be maximized, which is to minimize the expected loss. Therefore, a simple Gaussian kernel correntropy induced loss function can be defined as:

$$\hat{L}(e) = 1 - G_{\sigma}(e) \quad (7)$$

which is called the C-loss function [25].

The loss function based on two Gaussian kernel mixed correntropy can be defined as:

$$\begin{aligned}\widehat{L}(e) &= 1 - \widehat{M}(e) \\ &= 1 - \frac{1}{\sqrt{2\pi}N} \sum_{i=1}^N \left[\frac{\alpha}{\sigma_1} \exp\left(-\frac{e_i^2}{2\sigma_1^2}\right) + \frac{(1-\alpha)}{\sigma_2} \exp\left(-\frac{e_i^2}{2\sigma_2^2}\right) \right]\end{aligned}\quad (8)$$

With our proposed loss function, the pseudo-code of whole process for classification tasks is presented in Algorithm 1.

Algorithm 1 Mixture correntropy induced loss CNN

Input: Training set, test set, parameters σ_1 and σ_2 , number of iterations, T batch size, kernel size of each layers, $t = 0$.

Output: Loss, accuracy (Acc)

1. Construct the CNN model;
 2. Train the model:
 - a. Sample a batch of data from training set;
 - b. Process forward propagation through the data, and calculate the mixture correntropy induced loss according to (8);
 - c. Process backward propagation to calculate the gradients;
 - d. Update the layer parameters using the gradient;
 - e. $t = t + 1$. If $t < T$, loop from step a;
 3. Process test set in trained CNN model, and calculate Acc.
-

3.2 Testing Classifier Through Metrics

To evaluate the performance of classification algorithm, the Accuracy (Acc) is defined as:

$$\text{Acc} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (9)$$

where TP, TN, FP, FN refers to true positive, true negative, false positive, and false negative, respectively.

4 Experimental Results and Discussion

In this section, the experiments on a popular benchmark dataset and a real-world malware classification dataset are conducted to evaluate the performance of our proposed algorithm. Considering the noise in the real-world malware data is hard to be removed, to show the strengths of our algorithm clearly, we firstly applied algorithms

to the original image dataset, and then add noise factor. Here, our experiments are implemented with Python compiler environment running on a computer with a 1.6 GHZ CPU and an 8 GB RAM.

4.1 Classification Results on Benchmark Dataset

Experimental Results. The comparison is conducted among four methods, including the support vector machine (SVM), the traditional CNN classifier with the mean square error (MSE)-induced loss function (CNN+MSE), the CNN classifier with correntropy-induced loss function (CNN+Correntropy), and our method, i.e., the CNN classifier with mixture correntropy-induced loss function. In this experiment, we use Fashion-mnist dataset [26]. As shown in Fig. 2, Fashion-MNIST is a dataset of article images, each sample is a 28×28 grayscale image. There are 10 classes in this dataset, consisting training set of 60,000 examples and a test set of 10,000 examples.

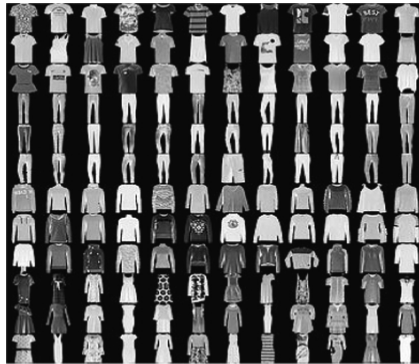


Fig. 2. Illustration of Fashion-mnist dataset.

Firstly, we apply each algorithm on original dataset, and then we add noise into original dataset to test the robustness of each algorithm.

Table 1. Performance of each algorithm on original Fashion-mnist dataset.

Algorithm	Accuracy
SVM	0.8575
CNN-MSE	0.9147
CNN-Correntropy ($\sigma = 0.8$)	0.9154
CNN-MixCorrentropy ($\sigma_1 = 0.5, \sigma_2 = 3, \alpha = 0.5$)	0.9170

As shown in Table 1, in the original dataset, the accuracy of CNN-MSE, CNN-Correntropy and CNN-MixCorrentropy is very close, and is better than that of SVM. Table 2 presents the performance of four classification method in dataset with Gaussian

noise. The accuracy of all the algorithms decreases, among which, the accuracy of SVM decreases significantly, CNN-MixCorrentropy achieves the best performance. The result shows the robustness of mixture correntropy induced loss function. Specifically, Figs. 3 and 4 show the loss and accuracy of CNN-MixtureCorrentropy on the original dataset and on the dataset with noise, respectively.

Table 2. Performance of each algorithm on Fashion-mnist dataset with normal distribution Gaussian noise (noise factor = 0.3).

Algorithm	Accuracy
SVM	0.6765
CNN-MSE	0.8489
CNN-Correntropy ($\sigma = 0.8$)	0.8575
CNN-MixCorrentropy ($\sigma_1 = 0.5 \sigma_2 = 4 \alpha = 0.3$)	0.8605

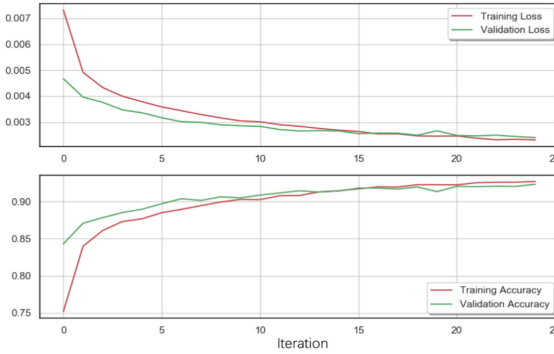


Fig. 3. Loss and accuracy of CNN-MixtureCorrentropy on the original dataset.

Impact of Parameters σ_1 and σ_2 . In the experiments, we set up different values of σ_1 and σ_2 , and apply them into Fashion-mnist dataset with noise. We define that $\sigma_1 < \sigma_2$. Figure 5 shows the results, which implies that when $0 < \sigma_1 < 1$, for different values of σ_1 and σ_2 , the performance is basically the same. But when we set $\sigma_1 > 1$, the accuracy decreases significantly.

Additionally, as shown in Fig. 6, when we set $0 < \sigma_1 < 1$, the value of α basically does not affect the performance of our algorithm.

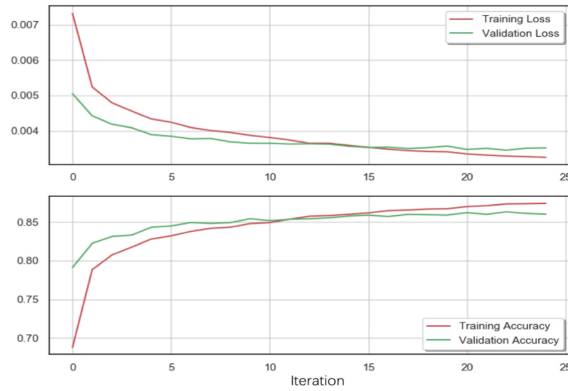


Fig. 4. Loss and accuracy of CNN-MixtureCorrentropy on the dataset with noise.

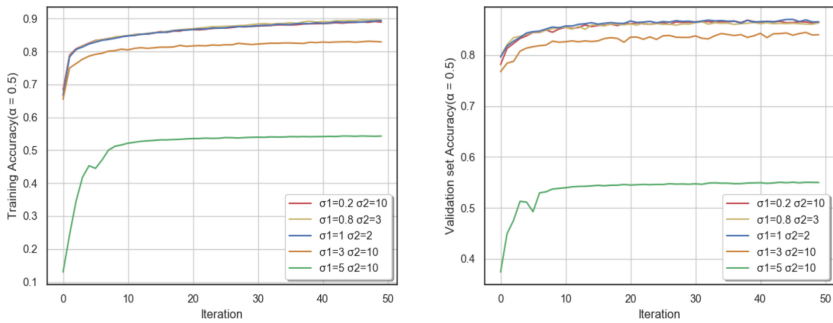


Fig. 5. Performance of CNN-MixtureCorrentropy ($\alpha = 0.5$).

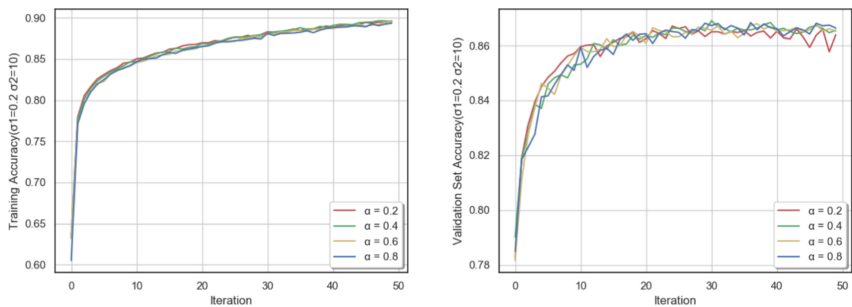


Fig. 6. Performance of CNN-MixtureCorrentropy ($\sigma_1 = 0.2, \sigma_2 = 10$).

4.2 Classification Results on a Real-World Malware Dataset

One of the most efficient ways in analyzing the malware data is to extract API call information [27]. The Windows API is a set of predefined Windows functions that control the behavior of various parts of Windows. Each action of the user triggers the

execution of one or more functions to tell Windows what is happening. API call information can be obtained statically and dynamically [28].

In this test task, we generate our dataset by randomly selecting malware samples from two malware datasets, Dasmalwerk [29] and VirusShare [30], and then use Cuckoo Sandbox to analyze malicious files. Dasmalwerk and VirusShare are the datasets of different types of executable malware from Internet. From the reports generated by Cuckoo, API call information is extracted (Fig. 7).

NtAllocateVirtualMemory	NtFreeVirtualMemory	NtAllocateVirtualMemory	GetFileType
NtAllocateVirtualMemory	SetErrorMode	LdrLoadDll	LoadStringA
LdrGetDllHandle	NtAllocateVirtualMemory	NtFreeVirtualMemory	NtAllocateVirtualMemory
GetSystemTimeAsFileTime	NtAllocateVirtualMemory	NtFreeVirtualMemory	NtAllocateVirtualMemory
GetFileAttributesW	NtCreateMutant	GetSystemTimeAsFileTime	NtOpenKey
FindResourceExW	LoadResource	FindResourceExW	LoadResource
GetFileAttributesW	NtCreateMutant	GetSystemTimeAsFileTime	NtOpenKey
GetSystemTimeAsFileTime	LdrGetDllHandle	LdrGetProcedureAddress	GetFileType
GetSystemTimeAsFileTime	LdrGetDllHandle	LdrGetProcedureAddress	GetFileType
NtAllocateVirtualMemory	SetErrorMode	LdrLoadDll	LoadStringA
GetSystemTimeAsFileTime	LdrGetDllHandle	LdrGetProcedureAddress	GetFileType
GetFileAttributesW	NtCreateMutant	GetSystemTimeAsFileTime	NtOpenKey
GetSystemTimeAsFileTime	LdrGetDllHandle	LdrGetProcedureAddress	GetFileType
LdrGetProcedureAddress	LdrGetDllHandle	NtAllocateVirtualMemory	GetFileType
LdrGetProcedureAddress	LdrGetDllHandle	LdrGetProcedureAddress	LdrGetDllHandle
SetErrorMode	NtCreateFile	NtAllocateVirtualMemory	SetFilePointer
GetSystemTimeAsFileTime	SetUnhandledExceptionFilter	NtAllocateVirtualMemory	CoInitializeEx
NtAllocateVirtualMemory	NtFreeVirtualMemory	NtAllocateVirtualMemory	GetFileType
GetSystemTimeAsFileTime	LdrGetDllHandle	LdrGetProcedureAddress	SetUnhandledExceptionFil
RegOpenKeyExA	NtClose	NtQueryAttributesFile	LoadStringA
MessageBoxTimeoutA	LdrGetDllHandle	LdrGetProcedureAddress	LdrGetDllHandle
GetSystemTimeAsFileTime	LdrGetDllHandle	LdrGetProcedureAddress	SetUnhandledExceptionFil
GetSystemTimeAsFileTime	NtAllocateVirtualMemory	NtFreeVirtualMemory	NtAllocateVirtualMemory
GetSystemTimeAsFileTime	LdrGetDllHandle	LdrGetProcedureAddress	GetFileType

Fig. 7. A part of malware API call report.

In this experiment, our proposed algorithm is specifically applied to binary classification task for malware. Aiming that distinguish the malware samples and normal benign sample, we need sufficient quantity of both malware samples and benign samples. We downloaded portable application from Internet and tested them by anti-virus software. If the application is safe, we take it as a benign sample. Firstly, we randomly select the same amount of benign sample and malware sample, precisely, 200 samples of each class. As shown in Fig. 8, the word vector is input into CNN model and trained for multiple times. Dropout is used to prevent over fitting. The output of the model is the predicted label. Input size is (400, 995, 128), which refers to (sample number, maximum number of API calls, embedding). SVM is a classical and common classification method, thus, we take SVM as one of comparison algorithm. We use five-fold cross validation, the original data is randomly partitioned into 5 subsamples. For each time, 4 subsamples are used as train data, 1 subsample is used as test data, which means we take 320 samples as train set, 80 samples as test set. The process is then repeated 5 times. The final Accuracy (Acc) is defined as:

$$Acc = \frac{1}{5} \sum_{i=1}^5 Acc_i \quad (10)$$

where Acc_i refers to the accuracy of each time.

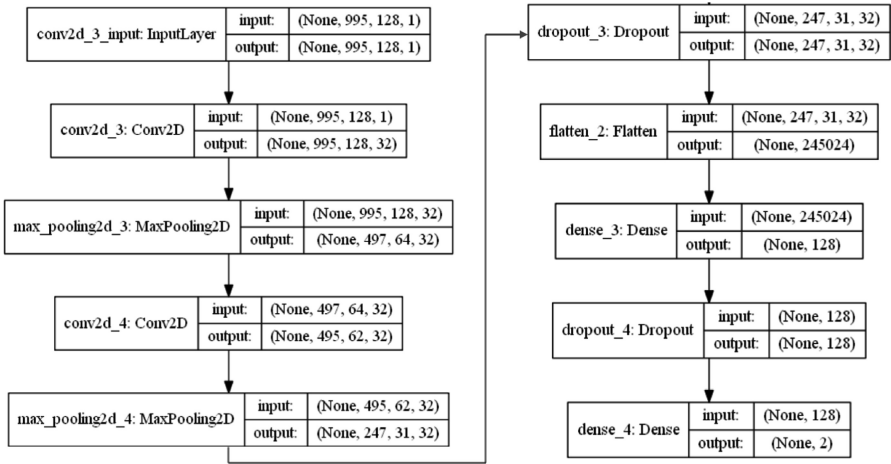


Fig. 8. Processing model.

Table 3. Performance of each algorithm on a real-world malware dataset.

Algorithm	Accuracy
SVM	0.7387
CNN-MSE	0.8025
CNN-Correntropy ($\sigma = 0.7$)	0.7937
CNN-MixCorrentropy ($\sigma_1 = 0.4 \sigma_2 = 3 \alpha = 0.5$)	0.8156

The word2vec method is used to transfer text document into vectors. Table 3 shows the accuracy of each algorithm. CNN with different lose function perform better than SVM. Obviously, CNN with mixture correntropy loss function performs best. Because of the noise factors in the real-world malware dataset, our method shows the strongest robustness among four algorithms. Moreover, we also find that compared to MSE loss function, mixture correntropy loss function has faster convergence speed, demonstrated in Fig. 9.

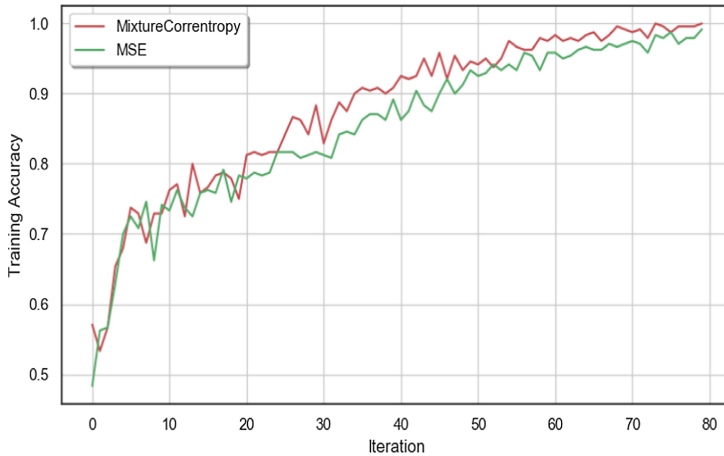


Fig. 9. Performance of convergence on training set.

5 Conclusion

This paper aims at dealing with a challenging issue in the achievement of malware identification and detection in CPS application, which is the Android malware classifier. Starting from the general analysis of related work on mixture correntropy and CNN, in this paper we present a novel malware identification and detection method on the basis of our proposed CNN classifier with mixture correntropy-induced loss function. Then, compared to other traditional classifiers, the data cloud be handled more flexibly and stably with a higher classification accuracy and a better robustness through the use of our mixture correntropy-based CNN model, due to the incorporation of mixture correntropy especially used to outlier learning problems. In the experiments, the classification performance of our proposed method and other popular algorithms are compared on a benchmark dataset and a real-world Android malware dataset. The experimental results verify the effectiveness and efficiency of our method.

Acknowledgement. This work was supported in part by the National Natural Science Foundation of China under grants U1836106 and U1736117, by the National Key Research and Development Program of China under grant 2018YFC0808306, and by the Beijing Intelligent Logistics System Collaborative Innovation Center under Grant BILSCIC-2019KF-08.

References

1. Lee, E.A.: Cyber physical systems: design challenges. In: 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), Orlando, pp. 363–369. IEEE (2008)
2. Neuman, D.C.: Challenges in security for cyber-physical systems. In: DHS Workshop on Future Directions in Cyber-Physical Systems Security, pp. 22–24 (2009)

3. Stolfo, S.J., Wang, K., Li, W.-J.: Fileprint analysis for malware detection. In: ACM CCS WORM (2005)
4. Thakar, N., Praveen, K.A., Vikas, T.: System and method to detect domain generation algorithm malware and systems infected by such malware. U.S. Patent Application 16/264,667 (2019)
5. Taylor, C., Alves-Foss, J.: NATE: network analysis of a nomalous traffic events: a low-cost approach. In: Proceedings of the 2001 Workshop on New Security Paradigms, pp. 89–96. ACM, New York (2001)
6. Xiao, X., Zhang, S., Mercaldo, F., Hu, G., Sangaiah, A.K.: Android malware detection based on system call sequences and LSTM. *Multimedia Tools Appl.* **78**(4), 3979–3999 (2019)
7. Peiravian, N., Zhu, X.: Machine learning for android malware detection using permission and API calls. In: 25th International Conference on Tools with Artificial Intelligence, Herndon, pp. 300–305. IEEE (2013)
8. Yuxin, D., Zhu, S.: Malware detection based on deep learning algorithm. *Neural Comput. Appl.* **31**(2), 461–472 (2019)
9. Tobiyama, S., Yamaguchi, Y., Shimada, H., Ikuse, T., Yagi, T.: Malware detection with deep neural network using process behavior. In: 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, vol. 2, pp. 577–582. IEEE (2016)
10. Liu, W., Pokharel, P.P., Principe, J.C.: Correntropy: a localized similarity measure. In: The 2006 IEEE International Joint Conference on Neural Network Proceedings, Vancouver, pp. 4919–4924. IEEE (2006)
11. Gunduz, A., Principe, J.C.: Correntropy as a novel measure for nonlinearity tests. *Sig. Process.* **89**(1), 14–23 (2009)
12. Luo, X., et al.: Towards enhancing stacked extreme learning machine with sparse autoencoder by correntropy. *J. Franklin Inst.* **355**(4), 1945–1966 (2018)
13. Chen, L., Qu, H., Zhao, J.: Generalized Correntropy based deep learning in presence of non-Gaussian noises. *Neurocomputing* **278**, 41–50 (2018)
14. Chen, B., Wang, X., Lu, N., Wang, S., Cao, J., Qin, J.: Mixture correntropy for robust learning. *Pattern Recogn.* **79**, 318–327 (2018)
15. LeCun, Y., Bengio, Y.: Convolutional networks for images, speech, and time series. In: *The Handbook of Brain Theory and Neural Networks*, vol. 3361, no. 10, p. 1995 (1995)
16. Principe, J.C.: *Information Theoretic Learning: Renyi's Entropy and Kernel Perspectives*. ISS. Springer, New York (2010). <https://doi.org/10.1007/978-1-4419-1570-2>
17. Liu, W., Pokharel, P.P., Principe, J.C.: Correntropy: properties and applications in non-Gaussian signal processing. *IEEE Trans. Signal Process.* **55**(11), 5286–5298 (2007)
18. Krizhevsky, A., Sutskever, I., Hinton, G.E.: ImageNet classification with deep convolutional neural networks. In: *Advances in Neural Information Processing Systems*, pp. 1097–1105 (2012)
19. Maturana, D., Scherer, S.: VoxNet: a 3D convolutional neural network for real-time object recognition. In: 2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Hamburg, pp. 922–928. IEEE (2015)
20. Kim, Y.: Convolutional neural networks for sentence classification. In: EMNLP 2014 - 2014 Conference on Empirical Methods in Natural Language Processing, pp. 1746–1751 (2014)
21. Yuan, Z., Lu, Y., Wang, Z., Xue, Y.: Droid-Sec: deep learning in android malware detection. *ACM SIGCOMM Comput. Commun. Rev.* **44**(4), 371–372 (2014)
22. Kolosnjaji, B., Zarras, A., Webster, G., Eckert, C.: Deep learning for classification of malware system call sequences. In: Kang, B.H., Bai, Q. (eds.) *AI 2016. LNCS (LNAI)*, vol. 9992, pp. 137–149. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-50127-7_11

23. Pascanu, R., Stokes, J.W., Sanossian, H., Marinescu, M., Thomas, A.: Malware classification with recurrent networks. In: 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brisbane, pp. 1916–1920. IEEE (2015)
24. Dahl, G.E., Stokes, J.W., Deng, L., Yu, D.: Large-scale malware classification using random projections and neural networks. In: 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, pp. 3422–3426. IEEE (2013)
25. Singh, A., Pokharel, R., Principe, J.C.: The C-loss function for pattern classification. *Pattern Recogn.* **47**(2), 441–453 (2014)
26. Xiao, H., Rasul, K., Vollgraf, R.: Fashion-MNIST: a novel image dataset for benchmarking machine learning algorithms. arXiv preprint [arXiv:1708.07747](https://arxiv.org/abs/1708.07747) (2017)
27. Shankarapani, M.K., Ramamoorthy, S., Movva, R.S., Mukkamala, S.: Malware detection using assembly and API call sequences. *J. Comput. Virol.* **7**(2), 107–119 (2011)
28. Idika, N., Mathur, A.P.: A survey of malware detection techniques, vol. 48. Purdue University (2007)
29. Dasmalwerk Homepage. <https://dasmalwerk.eu>. Accessed 10 Sept 2019
30. VirusShare Homepage. <https://virusshare.com>. Accessed 10 Sept 2019



An Improved Algorithm for Recruitment Text Categorization

Hui Zhao¹, Xin Liu², Wenjie Guo³, Keke Gai³, and Ying Wang⁴✉

¹ Educational Information Technology Laboratory, Henan University,
Kaifeng, Henan 475004, China
zhh@henu.edu.cn

² School of Software, Henan University, Kaifeng, Henan 475004, China
124761323@qq.com

³ School of Computer Science and Technology, Beijing Institute of Technology,
Beijing 100081, China
{guowenjie, gaikeke}@bit.edu.cn

⁴ Henan Intelligent Data Processing Engineering Research Center,
Kaifeng, Henan 475004, China
wangying@henu.edu.cn

Abstract. With the rapid development of the Internet, online recruitment has gradually become a mainstream. In the process of obtaining the text of recruitment information, a large volume of texts are not part of recruitment information. Currently, common text categorization algorithms include k-Nearest Neighbor, Support Vector Machine (SVM) and Naive Bayes. In addition, there are numerous related technical terms in the recruitment information, which affects the accuracy of the ordinary Bayesian text categorization algorithm. However, there is not uniform format for the text information of recruitment. This paper improves the original Naive Bayes algorithm and proposes a Reinforcement Naive Bayes (R-NB) algorithm to enhance the accuracy of recruitment information categorization. Experiments have demonstrated that the improved algorithm has a higher categorization accuracy and practicability than the original algorithm.

Keywords: Naive Bayes algorithm · Text categorization · Feature extraction · Recruitment categorization

1 Introduction

With a booming growth of the Internet, a large deal of recruitment information are put on the third-party recruitment website every day [5]. But there are some problems with those recruitment websites. For example, some recruitment information is actually a disguised skill training advertisement; some recruitment information is outdated and will never be updated; some recruitment pages keeps various advertisements. A representative application scenario is that the existence of these situations has brought troubles to job seekers, as it not only

causes time-wasting on browsing ineffective recruitment information but also wastes energy on analyzing the correctness and reasonability of the recruitment information. A detailed categorization methods adopted in various fields will be improving the efficiency [19,20].

It is found that most recruitment information is displayed in a text format. Knowledge discovery through artificial intelligence techniques has become a mainstream in web-based applications [6,7]. We can use a text categorization algorithm to classify texts collected from recruitment websites.

The purpose of this research is to quickly identify the category of text with a high accuracy by means of a categorization algorithm. Many methods such as Naive Bayes algorithm, Support Vector Machine (SVM) [15], Neural Network and K-NN [17], have been applied to text categorization. Naive Bayes algorithm is known for its simple operation, accurate categorization and low data sensitivity. This paper improves the original Naive Bayes text categorization algorithm, which effectively releases the impact of uncommon features in recruitment information, and effectively improve the accuracy of recruitment text categorization.

Main contributions of this paper include two aspects:

1. This paper studies the principle of Naive Bayes algorithm via investigating philosophy of outputs' deviation, and puts forward R-NB algorithm by improving the Naive Bayes algorithm to obtain a better recruitment categorization.
2. The collected data are preprocessed, including several methods such as Chinese word segmentation, feature extraction and so on, which provide the basic conditions for the latter categorization experiments.

This paper is organized as follows: Sect. 2 introduces the application of various improved Naive Bayes algorithms in different fields and points out current algorithms' shortcomings in recruitment categorization. In addition, Sect. 3 introduces main concepts involved in the paper and the technology used in this paper. Next, Sects. 4 and 5 proposes the model this paper and presents the improved Naive Bayes algorithm in details, respectively. Finally, experiment results and conclusions are given in Sects. 6 and 7.

2 Related Work

With the rapid development of computer technology, information is increasing exponentially. It becomes a research hotspot of the data mining field to present an effective and appropriate method to classify a large number of texts. The main text categorization algorithms include Naive Bayes, K nearest neighbor, neural network, SVM, Rocchio classifier of vector space model [13] and maximum entropy [12], etc. The Bayes categorization method simplifies the calculation of training and categorization process based on Bayes probability theory and Bayes statistics, which achieves effective categorization.

On the basis of Naive Bayes algorithm, many researchers have made innovations and modifications, and achieved good text categorization results in their

respective fields. For example, Shi et al. [14] combined the Naive Bayes algorithm with the support vector machine, the authors first used the SVM to establish the optimal categorization plane, then used whether the adjacent types were the same to make a choice, and finally used the Naive Bayes algorithm to classify emails. This work addresses the problem of space vector redundancy, not only reduces the space complexity, but also improves the categorization speed. The improved algorithm has high accuracy and recall rate in spam filtering.

Wang et al. [16] applied Naive Bayes categorization algorithm to social network text categorization, and proposed a bayes categorization algorithm based on variance filtering on the basis of Naive Bayes. Given the social message text categorization test set, each message can be classified according to its relevance to the information, and then the probability value of each category to which each message belongs can be calculated. Then this work uses the variance of the social network message text as the category feature value. If the variance of the message text is nearly to zero, which means the category characteristics of these message texts are not very distinct, in which case the algorithm will ignore text with a relatively small text variance. In social networks, the text with obvious differences only occupies a relatively small part of the text. Through the method of variance filtering, a large part of message text can be filtered out. The information text classified by this method has strong categorization characteristics, which can enhance the efficiency and accuracy of text categorization.

Xiang et al. [18] improved Naive Bayes algorithm based on attribute weighting. Due to the correlation between conditional attributes and categories, Naive Bayes algorithm would ignore some small correlation, thus significantly reducing the categorization effect. The authors quantifies the attributes associated with different categories by setting the weighted value of the attribute. The correlation of the larger attribute values will be a larger weighting coefficient, similarly, the correlation of the smaller attribute values lead to a smaller weighting coefficient. Since different attributes have different weighting coefficients, the posterior probability of the conditional term is more accurate in calculating each item and the weighted naive Bayesian algorithm has better categorization accuracy.

The existing improved Naive Bayes algorithm improves the performance of Naive Bayes text categorization algorithm, but there are some limitations in the application of Naive Bayes text categorization. When categorizing recruitment texts, professional terms in recruitment information belong to low-frequency words, which can easily lead to sparse data sets. Due to the expansion of the algorithm and the limitation of computing power, it is difficult to make sure the efficiency of data processing when running traditional Naive Bayes text categorization algorithm on a centralized platform [10]. Although the Naive Bayes categorization algorithm has been constantly improved after continuous studies by predecessors, there are still problems that have to be studied and solved. Due to the strict assumption of conditional independence, the original Naive Bayes algorithm does not do well for some specific problems. Particularly, for the recruitment information on the Internet, the current Naive Bayes categorization algorithm is still unable to solve the following problems:

- (1) *Massive Recruitment Information.* Due to the rapid development of the Internet, more and more companies are publishing job postings on the Internet and attracting a large number of job seekers. How to classify the massive recruitment information efficiently is a difficult problem at present.
- (2) *Diversification of the Characteristics of Recruitment Information.* For a recruitment message, various jobs may be recruited. If there is more than one job, there will be many features. When the number of features is too much, it may lead to error propagation and affect the categorization effect. Since the posterior chance of each feature word is usually small, when the feature dimension is large, the product of the posterior chance of all features will be nearly to zero, which will have an impact on the accuracy of recruitment information categorization.

In summary, this paper improves the Naive Bayes algorithm to address these two problems.

3 Concepts

3.1 Web Crawler

Web crawler is a program that starts from the first URL set, extracts all the links pointing to the web page, adds them into the URL set, then obtain the content of the web page. Through uniform resource locator address, hypertext transfer protocol is used to simulate the way of browser requesting access to the web server, encapsulate the necessary request limits, get the permission of web servers, and finally obtain the original data [9]. With the help of web crawler, we can quickly get the recruitment information on the major recruitment websites, and the obtained recruitment information can be invoked as the data set of our classification algorithm.

3.2 Text Preprocessing

The text document obtained from the web crawler can't be categorized directly. Text segmentation is the first step that has to be done. There are some common methods such as string matching based methods, rule-based methods and statistics-based methods [2]. Methods based on string matching are according to determinate strategy, that all the strings need to be matched with the entries from the "big dictionary" machine. The advantage of this approach is easy to operate, but the shortcoming is also very noticeable, that the matching speed is slow and the words not included cannot be matched.

Based on the statistical method, the frequency of adjacent text co-occurrence in the context can help to obtain the probability of word formation. By calculating the combination frequency of the adjacent words in the prediction, their mutual information is generated. Mutual information reflects the association between Chinese characters, when relativity value is higher than a definite threshold, it can be judged that the phrase is a word. The advantage of this

method is it is not restricted by the field of text to be processed, and it does not need a special dictionary. Based on probability theory, statistical word segmentation abstracts the emergence of Chinese character combination strings into a stochastic process. The limits of the stochastic process are determined by the results of large-scale corpus training.

Commonly used Chinese word segmentation packages include Ding Xie Niu word segmentation packages (for Lueene integration) [8], LingPipe (Java Open Source Toolkit for open source natural language processing) [3], and Python's *Jieba* module, etc. *Jieba* module has better performance for segmenting Chinese characters, specifically, sentences in documents can be cut precisely, and word segmentation speed is very fast, and long words can also be re-segmented, which can improve recall rate. So the word segmentation system we use in this paper is the *Jieba* module of Python.

3.3 Feature Extraction

Feature extraction is a important part, because the better feature extraction can improve the performance of the model and help us understand both characteristics and the underlying structure of the data, which plays an important role in further process of improving the model and algorithm. There are two main functions of feature extraction, one is reducing the number of features and dimensionality, that the model will have stronger generalization ability, another one is enhancing the understanding between features and eigenvalues. Currently, the commonly used methods for feature extraction include CHI statistics [4], information entropy, mutual information (MI) [1], Information Gain (IG) and the word bag model.

Each feature extraction method has its own advantages, by analyzing the advantages of the above methods, this paper adopts the word bag model for feature extraction. The word bag model focuses on whether the word is known in the document, and the word bag model has the following three steps:

- (1) *Collect Data.* Take collected text documents as samples.
- (2) *Design vocabulary.* List all the words in the model vocabulary.
- (3) *Create Document Vectors.* Convert each document into a text vector that serves as input and output to the machine learning model.

3.4 Naive Bayes Principle

Naive Bayes algorithm is a classical statistical method based on Bayesian theorem. Bayesian theorem is a branch of probability statistics, the core principle of it is the Bayesian formula. Set X as a test sample, $Y = \{y_1, y_2, \dots, y_k\}$ is a set of categories, and $P(Y|X)$ indicates the probability that sample X belongs to different categories Y . It can be considered that the class Y_i corresponding to the greatest probability value is the class allocated by the sample, which can be obtained by Bayesian formula in Eq. 1.

$$P(Y|X) = \frac{P(Y)P(X|Y)}{P(X)}. \quad (1)$$

where $P(Y|X)$ is the posterior probability of Y under the condition X , $P(X|Y)$ is the posterior probability of X under condition Y , $P(X)$ is the prior probability of X , and $P(Y)$ is the prior probability of Y .

The classification goal of Bayesian method is that the feature values of the given descriptive text are $\langle w_1, w_2, \dots, w_n \rangle$, the most probable target value V_{MAP} is obtained in Eq. 2.

$$V_{map} = arg\ max\ P(C_j|w_1, w_2 \dots w_n). \tag{2}$$

Using Bayesian formula, the expression is shown in Eq. 3:

$$V_{map} = arg\ max\ \frac{P(w_1, w_2 \dots w_n|C_j)}{P(w_1, w_2 \dots w_n)}. \tag{3}$$

It is easy to obtain $P(C_j)$ by calculating the frequency of each text class in the training data. Naive Bayes classifier is based on the following assumption, when the target value is given, attributes are conditionally independent of each other, as shown in Eq. 4.

$$P(w_1, w_2 \dots w_n|C_j) = \prod_i P(w_i|C_j). \tag{4}$$

In summary, the method of Naive Bayes Classifier can be obtained in Eq. 5:

$$V_{NB} = arg\ max\ P(C_j)\prod_i(w_i|C_j). \tag{5}$$

4 Model Design

Naive Bayes algorithm has a fast categorization speed and high accuracy when dealing with large-sized data sets. But when the training set is relatively small, the categorization accuracy is obviously lower than other categorization algorithms. When there are few training samples, the randomness of some uncommon feature will be very large. There will be a large number of technical terms in the recruitment text, which includes many ambiguous words. Naive Bayesian formula is help to calculate the value of continuous product, which means that

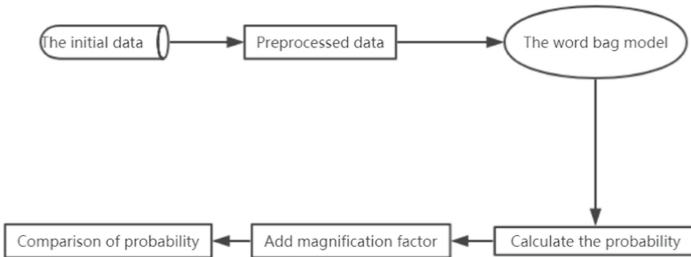


Fig. 1. The process of the improved algorithm.

Table 1. Symbols definition.

Symbol name	The meaning of representation
$MATRIX$	Document Matrix After Processing
$CATEGORY$	Processed categorization Label Set
P_0	The Probability of Words Appearing under the Conditions of Non-Recruitment Information
P_1	The Probability of Words Appearing under the Conditions of Recruitment Information
P_{ALL}	Probability of Documentation Belonging to Recruitment Information
$TRAINR - NB$	Improved Naive Bayesian Training Algorithms
$COUNT()$	A function for finding numbers
$NUMDOCS$	Number of documents
$NUMWORDS$	Document word number
$SUM()$	Summation function
P_0NUM	The sum of word vectors belonging to non-recruitment information
P_1NUM	The sum of word vectors belonging to Recruitment Information
$LOG()$	Take logarithmic function
K	Set magnification factor
P_1V	Probability that ultimately belongs to Recruitment Information
P_0V	Probability of eventual non-recruitment information
P_0DEMO	Number of Document Words Not Belonging to Recruitment Information
P_1DEMO	Number of Document Words Belonging to Recruitment Information

characteristics of obscure terminology will play a dominant role in text categorization. For example, when a feature appears once in a text of a certain category, the probability of this category is estimated to be: $\frac{1+1}{1+|Category|}$, where $|Category|$ is the total number of features in the training set, while other categories is estimated to be: $\frac{1+0}{0+|Category|}$, both above two are about to zero, but after calculating posterior probability $VNB = argmaxP(Cj) \prod_i P(wi|Cj)$, the categorization results will be updated.

In order to reduce above influence and result deviation which caused by continuous multiplication, Min et al. [11] changed continuous multiplication to continuous addition based on Naive Bayesian text categorization. In order to obtain the categorization result more accurately, our work adds the amplification factor K to the predecessors. Compared with the previous improved algorithms, the improved algorithm can improve the categorization accuracy.

The process of the improved algorithm is as follows. First, the initial data are obtained, then the initial data are preprocessed, then the bag of words model is constructed, and then the earlier probability and the posterior probability are calculated. Finally, the probability under different amplification coefficients can be obtained by adding amplification coefficients. As shown in Fig. 1:

After the above analysis, the specific process of the improved Naive Bayesian algorithm is as follows:

- (1) *Obtain the Recruitment Text and Preprocess the Initial Data.* After using the crawler to get the recruitment text on the recruitment website, it uses the word segmentation tool to preprocess the recruitment text.

- (2) *Construct the Word Bag Model and Extract the Text Deatures.* After word frequency statistics of preprocessed text, words with high frequency are selected to build the word bag model. Then we obtained the word vector to extract text features.
- (3) *Calculate Prior Probabilities Belonging to Recruitment Categories and Non-recruitment Categories.* The total number of texts in each class and the total number of texts in the entire training set are calculated, then we obtain the percentage of the total number of training texts of these two categories in the total number of training sets.
- (4) *Calculated the Posterior Probability of Recruitment Categories and Non-recruitment Categories.* For each item in the text to be categorized, the total number of texts with feature items in each class is calculated, and then get the percentage of the total number of texts with feature items in the two categories to the total number of texts in that class. In this step, the posterior probabilities belonging to recruitment and non-recruitment categories are calculated respectively after the original multiplication becomes additive.
- (5) *Add the Magnification Factor.* Because the Naive Bayesian categorization algorithm only needs to compare the probability calculation results of recruitment and non-recruitment, it will not affect the final categorization result if the probability calculation results of two categories are enlarged. In order to avoid large categorization deviation due to insufficient computer precision, which the output probability is zero, it is necessary to set the correct amplification factor through experiment results analysis.
- (6) *Judge the Recruitment Category.* According to the obtained probabilities, the categorization of recruitment is judged. The recruitment text is categorized by comparing the posterior Categories obtained. If the probability that the text belongs to the recruitment group is greater than the probability of the non-recruitment category, the text is recruitment information. Instead, it is non-recruitment information.

5 Algorithm

The R-NB algorithm proposed in this paper is implemented by adding an amplification coefficient on the basis of the previous changing from continuous multiplication to continuous addition. The symbols appearing in the algorithm are defined as follows, referring to Table 1.

Firstly, in the categorization trainer function, we need to use our processed text M_{MATRIX} and the $C_{CATEGORY}$ set of categorization tags, and then we can know the number of $NUMDOCS$ and the number of $NUMWORDS$ of documents collected. Then, it will be converted into word vectors P_0NUM and P_1NUM , and the probability P_{ALL} of the text belonging to the recruitment information is calculated, then the sum of the word vectors P_0NUM and P_1NUM is calculated. When it belongs to the recruitment information, the word vector P_1NUM belongs to the recruitment information is added, and the number of document words P_1DEMO belonging to the recruitment information is added at the same time.

Algorithm 1. R-NB Algorithm

Input: Document matrix M_{MATRIX} , categorization label $setC_{CATEGORY}$.

Output: The Probability of Words Appearing under the Conditions of Non-Recruitment Information P_0 , The Probability of Words Appearing under the Conditions of Recruitment Information P_1 , Probability of Documentation Belonging to Recruitment Information P_{ALL} .

```

1:  $T_{RAIN}R - NB(M_{MATRIX}, C_{CATEGORY})$ 
2:  $NUMDOCS \leftarrow COUNT(M_{MATRIX})$ 
3:  $NUMWORDS \leftarrow COUNT(M_{MATRIX}[1])$ 
4:  $P_{ALL} \leftarrow SUM(C_{CATEGORY}) / (NUMDOCS)$ 
5:  $P_0NUM \leftarrow SUM(NUMWORDS)$ 
6:  $P_1NUM \leftarrow SUM(NUMWORDS)$ 
7: for do  $i$  in  $NUMDOCS$ 
8:   if  $C_{category}[i] == 1$  then
9:      $P_1NUM \leftarrow P_1NUM + M_{MATRIX}[i]$ 
10:     $P_1DEMO \leftarrow P_1DEMO + SUM(M_{MATRIX}[i])$ 
11:   else
12:      $P_0NUM \leftarrow P_0NUM + M_{MATRIX}[i]$ 
13:      $P_0DEMO \leftarrow P_0DEMO + SUM(M_{MATRIX}[i])$ 
14:   end if
15: end for
16:  $P_1 \leftarrow LOG(P_1NUM / P_1DEMO)$ 
17:  $P_0 \leftarrow LOG(P_0NUM / P_0DEMO)$ 
18: return  $P_0, P_1, P_{ALL}$ 

```

Similarly, if the word vector belongs to non-recruitment information, the number of document words P_0DEMO that does not belong to recruitment information is added. Finally, the probability P_1 of each word in recruitment information and the probability P_0 of each word in non-recruitment information are calculated.

In the previous step, the probability P_0 of words appearing under the condition of non-recruitment information and the probability P_1 of words appearing under the condition of recruitment information were first obtained, then the amplification coefficients are added for comparison operation, and finally the probability P_1V of documents belonging to recruitment information and the probability P_0V of non-recruitment information are obtained. Then, by comparing the two probabilities, we can decide which category each word vector belongs to.

6 Experiments and Findings

Building Naive Bayesian classifier requires training text set and test set. The data in this paper are collected from 51job (<https://www.51job.com/>). 2500 recruitment information and 2500 non-recruitment information are invoked as training sets, and then the remaining documents are used as test sets. Finally, the

Algorithm 2. R-NB Algorithm

Input: Object word vector array form VECLASSIFY, The probability of each word in the recruitment categorization P1, The probability of each word appearing in a non-recruitment category P0, The probability that the document belongs to the recruitment information PCLASS1, Amplification factor K.

Output: Final categorization results Y/N.

```

1:  $C_{CLASSIFYNB}(VECLASSIFY, P_0, P_1, P_{CLASS1})$ 
2:  $P_1V \leftarrow ((K * SUM(VECLASSIFY)) + (P_{CLASS1}))$ 
3:  $P_0V \leftarrow ((K * SUM(VECLASSIFY)) + (1.0 - P_{CLASS1}))$ 
4: if  $P_1V > P_0V$  then
    return  $Y$ 
5: else
    return  $N$ 
6: end if

```

categorization accuracy is used as evaluation index. The categorization accuracy is decided by the correct number of text and the total number of text, as shown in Eq. 6.

$$C_{correct} = \frac{RightDos}{Total}. \quad (6)$$

Firstly, we use “Jieba” to segment one of the collected Recruitment Information documents. As shown in Fig. 2. Then we use the word bag model to process the document again, and select the words which seem more often as the document vector, as shown in Fig. 3.

As a classical text categorization algorithm, Naive Bayesian algorithm has a well categorization accuracy. Generally speaking, accuracy rate can reach more than 90% in theory and more than 80% in practice under some specific circumstances. However, due to its high dimensionality, sparsity, standardization, uneven distribution of topics and colloquial recruitment information, it cost too much time. Additionally, the posterior probability of the feature words of documents to be classified is generally small. When the number of feature words is large, the calculated probability value may be very small. In experiments, we find the calculated posterior probability is nearly to zero many times. So using the original Naive Bayesian algorithm to classify the recruitment text, the results is not ideal.

In order to cut the propagation of this error as much as possible and obtain the higher categorization accuracy, we need to add a coefficient. The principle of the algorithm is comparing the posterior probability of different categories, so this work selects the categories with high probability as the corresponding text. To be noticed, when the magnification factor is too large, the calculation result of posterior probability will be zero. By referring to earlier studies, this paper intends to set the amplification coefficient to 2, 3, 4, 5, 6, 7, 8, 9 in the case of 500, 1000, 1500, 2000, 2500 samples. The experiment results are as shown in Fig. 4, 5, 6, 7, 8, 9, 10 and 11.

```

Building prefix dict from the default dictionary ...
Loading model from cache c:\users\admin\appdata\local\temp\jieba.cache
岗位职责: /
Loading model cost 0.288 seconds.
/1/.根据/需求/文档/进行/程序设计/与/代码/编写/. /进行/单元测试/. /
/2/.编制/与/项目/相关/的/技术/文档/. /加/设计/文档/. /操作手册/等/. /
/3/.根据/项目/具体/要求/. /承担/开发/任务/. /并/按计划/完成/项目/目标/. /
/4/.独立/完成/软件系统/及/模块/的/编码/. /
/5/.协助/测试人员/完成/软件系统/及/模块/的/测试/. /
Prefix dict has been built successfully.
/职位/要求: /
/1/.本科/及/以上/学历/. /计算机/或者/相关/专业/. /
/2/.毕业3/年/以上/且/有1/年/以上/Java/开发/经验/. /扎实的/Java/基础/. /webservice//restful//soa//esb//soap/等/要/有/较
/深刻/的/理解/与/认识: /
/3/.熟悉/Spring/. /ibatis/. /Hibernate/等/开源/框架: /
/4/.熟悉/DB2//MySQL//Oracle/等/常用/数据库: /
/5/.熟悉/大规模/Web/应用/开发/. /有/一定/的/性能/优化/和/系统安全/的/实践: /
/6/.具有/大规模/高/开发/访问/的/web/应用/架构设计/和/开发/经验: / /有/后台/系统/构架/经验/者/优先:

Process finished with exit code 0

```

Fig. 2. The segment result based on “Jieba”.

```

list = [['开发', '经验', '软件', '设计', '设计', '工作', '技术', 'java', 'JAVA', '数据持久化', '分
[ 'Spring', 'MVC', '工程师', '数据库', 'SQL', '非关系型数据库', 'mongodb', '精通', '代码',
[ '团队', '优化', '职责', '精通', '前端', '服务器', '学习', '互联网', '工程师'],
[ '平台', '研发', '测试', '扎实', '模块', '积极', '乐观', 'maven', '热爱工作'],
[ '完成', '架构', '框架', '过程', '独立', '后台', '性能', '原理', '岗位'],
[ '业务', '需求', '主流框架', '实施', '部署', 'linux', '开源', '二次开发', '学习'],
[ '数据持久化', '分布式', '高级', '技能', '全面', '高并发', '处理', '提供', '带薪'],
[ '算法', '善于', 'javascript', '操作系统', '对象', '大型', '存储', '规范', '关系',
[ '优秀', '运用', 'Oracle', '压力', '项目经验', '方向', '概要', '行业', '攻关'],
[ '协助', '责任心', 'MyBatis', '稳定性', '社区', '配置', '奖金', '抗压', '监控'],
[ '主动', 'JSP', 'jsp', '员工', '运营', 'HTTP', 'MySQL', 'JVM', 'JDBC'],
[ 'SpringBoot', 'UML', 'maven', 'MAVEN', 'SVN', 'jQuery', 'nosql', 'SOCKET', 'Se
[ 'Unix', 'Web', '常规', '待遇', '底薪', '电子商务', '从事', '热爱', '认真'],
[ '单元测试', '功能', '更新', '进度', '开朗', '扩展', '面向对象', '培养', '设备'],
[ 'HBASE', 'HADOOP', 'ETL', 'EJB', 'Eclipse', '任职', '开发流程', '体系', '事业心',
[ 'HDFS', 'licks', 'jFreeChart', 'js', 'KAFKA', '招聘', '知识', '网站', '网络'],
[ 'hive', 'HIVE', 'sql', 'strom', 'steak', 'Xml', '版本', '帮助', '需求'],

```

Fig. 3. The segment result based on word bag model.

By comparing the data from the experiment results above, it is found that the improved algorithm achieves better categorization accuracy than the original Naive Bayesian algorithm, where the greatest difference between the original Naive Bayesian algorithm and the improved algorithm without amplification factor is 1.1%. The improved algorithm with amplification factor has the same accuracy as the original Naive Bayesian algorithm without amplification factor. And the greatest difference is 5.7% between the improved algorithm with amplification factor and the one without amplification factor. Because the original Naive Bayesian algorithm is not appropriate for dealing with the features in recruitment information, it will affect the categorization accuracy of the original algorithm. And it is shown that with the increase of the magnification factor, the accuracy of text categorization of the improved algorithm increases gradually, but when the magnification coefficient exceeds a threshold, the categorization accuracy decreases, but compared with the original algorithm, the categorization accuracy still increases.

In order to clarify the relationship between the magnification factor and categorization accuracy, the average probability of magnification factor between 3 and 20 is obtained when the number of samples is 500, 1000, 1500, 2000 and 2500, respectively. The results are shown in Fig. 12.

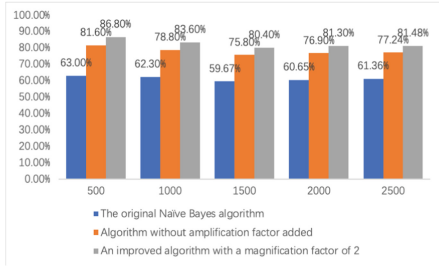


Fig. 4. Amplification factor is 2.

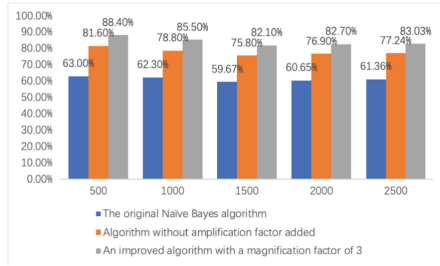


Fig. 5. Amplification factor is 3.

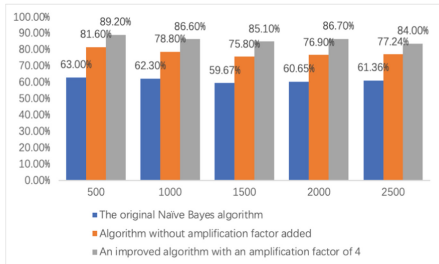


Fig. 6. Amplification factor is 4.

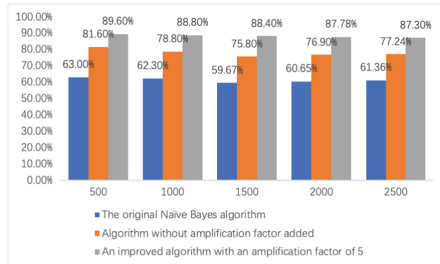


Fig. 7. Amplification factor is 5.

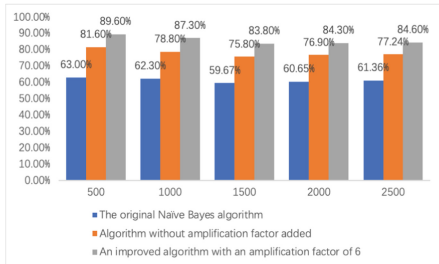


Fig. 8. Amplification factor is 6.

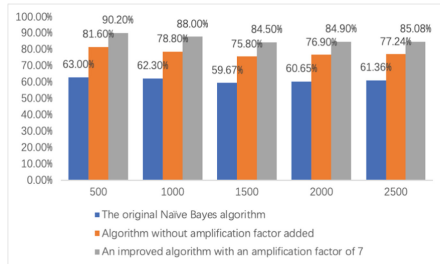


Fig. 9. Amplification factor is 7.

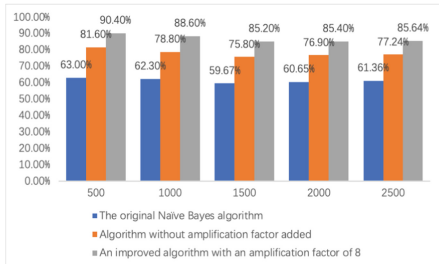


Fig. 10. Amplification factor is 8.

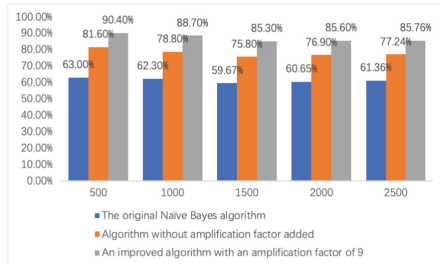


Fig. 11. Amplification factor is 9.

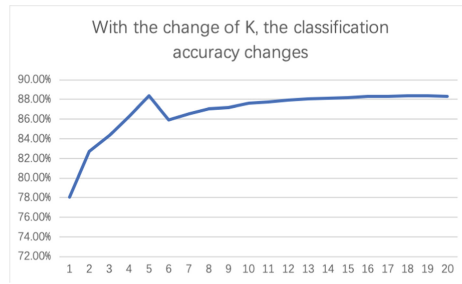


Fig. 12. Accuracy Rate of With Different K Values.

7 Conclusion

Aiming at the existing problems of the original Naive Bayesian algorithm in the text categorization of recruitment, this paper proposes the R-NB algorithm, which can mitigate the influence of unfamiliar professional terms on the text categorization results. Experiment results show that the improved algorithm with amplification coefficient has better categorization accuracy. In addition, the experiment shows that the categorization effect is better when the amplification coefficient is between 5 and 6.

Acknowledgement. This work is sponsored by Natural Science Foundation of Henan (No. 182300410164).



References

1. Bennasar, M., Hicks, Y., Setchi, R.: Feature selection using joint mutual information maximisation. *Exp. Syst. Appl.* **42**(22), 8520–8532 (2015)
2. Bojanowski, P., Grave, E., Joulin, A., Mikolov, T.: Enriching word vectors with subword information. *Trans. Assoc. Comput. Linguist.* **5**, 135–146 (2017)
3. Carpenter, B.: LingPipe for 99.99% recall of gene mentions. In: *Proceedings of the 2nd BioCreative Challenge Evaluation Workshop*, vol. 23, pp. 307–309. BioCreative (2007)
4. Fienberg, S.: The use of chi-squared statistics for categorical data problems. *J. Roy. Stat. Soc.: Ser. B (Methodol.)* **41**(1), 54–64 (1979)
5. Gai, K., Qiu, M.: Reinforcement learning-based content-centric services in mobile sensing. *IEEE Netw.* **32**(4), 34–39 (2018)
6. Gai, K., Qiu, M., Zhao, H.: Energy-aware task assignment for mobile cyber-enabled applications in heterogeneous cloud computing. *J. Parallel Distrib. Comput.* **111**, 126–135 (2018)
7. Gai, K., Xu, K., Lu, Z., Qiu, M., Zhu, L.: Fusion of cognitive wireless networks and edge computing. *IEEE Wirel. Commun.* **26**(3), 69–75 (2019)
8. Goetz, B.: The Lucene search engine: powerful, flexible, and free. *JavaWorld*. <http://www.javaworld.com/javaworld/jw-09-2000/jw-0915-lucene.html> (2000)
9. Heydon, A., Najork, M.: Mercator: a scalable, extensible web crawler. *World Wide Web* **2**(4), 219–229 (1999)

10. Mendoza, M.: A new term-weighting scheme for naïve bayes text categorization. *Int. J. Web Inf. Syst.* **8**(1), 55–72 (2012)
11. Min, Z., Zeng, G., Tu, X.: Study on an improved Naive Bayesian classifier used in the Chinese text categorization. In: *Second International Conference on Modeling* (2010)
12. Phillips, S., Anderson, R., Schapire, R.: Maximum entropy modeling of species geographic distributions. *Ecol. Model.* **190**(3), 231–259 (2006)
13. Selvi, S., Karthikeyan, P., Vincent, A., Abinaya, V., Neeraja, G., Deepika, R.: Text categorization using Rocchio algorithm and random forest algorithm. In: *Eighth International Conference on Advanced Computing* (2017)
14. Shi, H., Liu, Y.: Naïve Bayes vs. support vector machine: resilience to missing data. In: Deng, H., Miao, D., Lei, J., Wang, F.L. (eds.) *AICI 2011. LNCS (LNAI)*, vol. 7003, pp. 680–687. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23887-1_86
15. Tong, S., Koller, D.: Support vector machine active learning with applications to text classification. *J. Mach. Learn. Res.* **2**(Nov), 45–66 (2001)
16. Wang, B., Zhang, S.: A novel text classification algorithm based on Naïve Bayes and KL-divergence. In: *International Conference on Parallel and Distributed Computing Applications and Technologies* (2006)
17. Wang, Y., Chaib-draa, B.: KNN-based kalman filter: an efficient and non-stationary method for Gaussian process regression. *Knowl.-Based Syst.* **114**, 148–155 (2016)
18. Xiang, Z., Yu, X., Kang, D.: Experimental analysis of Naïve Bayes classifier based on an attribute weighting framework with smooth kernel density estimations. *Appl. Intell.* **44**(3), 611–620 (2016)
19. Yin, H., Gai, K.: An empirical study on preprocessing high-dimensional class-imbalanced data for classification. In: *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, pp. 1314–1319. IEEE (2015)
20. Yin, H., Gai, K., Wang, Z.: A classification algorithm based on ensemble feature selections for imbalanced-class dataset. In: *2016 IEEE 2nd International Conference on Big Data Security on Cloud*, pp. 245–249. IEEE (2016)



Seizure Prediction Using Bidirectional LSTM

Hazrat Ali¹  , Feroz Karim², Junaid Javed Qureshi¹,
Adnan Omer Abuassba³, and Mohammad Farhad Bulbul⁴

¹ Department of Electrical and Computer Engineering, COMSATS University
Islamabad, Abbottabad Campus, Abbottabad, Pakistan
hazrat.ali@cuiatd.edu.pk, jjqureshi123@gmail.com

² Institute for Interdisciplinary Information Sciences, Tsinghua University,
Beijing, China
ferozkundani@gmail.com

³ Arab Open University-Palestine, Ramallah, Palestine

⁴ Department of Mathematics, Jashore University of Science and Technology,
Jashore, Bangladesh
farhad@just.edu.bd

Abstract. Approximately, 50 million people in the world are affected by epilepsy. For patients, the anti-epileptic drugs are not always useful and these drugs may have undesired side effects on a patient's health. If the seizure is predicted the patients will have enough time to take preventive measures. The purpose of this work is to investigate the application of bidirectional LSTM for seizure prediction. In this paper, we trained EEG data from canines on a double Bidirectional LSTM layer followed by a fully connected layer. The data was provided in the form of a Kaggle competition by American Epilepsy Society. The main task was to classify the interictal and preictal EEG clips. Using this model, we obtained an AUC of 0.84 on the test dataset. Which shows that our classifier's performance is above chance level on unseen data. The comparison with the previous work shows that the use of bidirectional LSTM networks can provide significantly better results than SVM and GRU networks.

Keywords: Seizure prediction · Bidirectional LSTM · Deep learning · EEG

1 Introduction

Epilepsy is a neurological disorder characterized by spontaneous seizures. "Approximately, 50 million people in the world are affected by epilepsy and roughly 80% of them belong to low- and middle-income countries [1]." Medications for epilepsy might not be effective in almost half a cases. Although seizures occur infrequently, the patients under a continuous stress due to the fear of occurrence of seizure [2]. Similarly, the care taker person also suffers due to uncertain conditions of the patient. According to multi-center clinical studies, 6.2% of patients reported premonitory symptoms, and some of the epilepsy patients interviewed felt "auras" [3]. All these indicated that seizures might be predicted. Early detection can enable a patient as well as the care-taker to ensure precautionary steps for minimizing the associated risks by bringing the patient into a more comfortable and safer environment or bring him/her to rest if moving.

The brain activity can be classified into four states: Interictal (between seizures, or baseline), Preictal (prior to seizure), Ictal (seizure), and Post-ictal (after seizures) [2]. The *American Epilepsy Society* (AES) announced a competition on the platform of Kaggle (Kaggle, Inc) on the seizure prediction task. Our task is to develop a model to differentiate between Preictal and Interictal states. The data is collected from seven subjects, five canines, and two humans. The data consisted of 10-minute clips labeled “Preictal” or “Interictal”. The participants of the competition are required to distinguish between interictal and preictal clips. Preictal data segments are the six 10-minutes clips prior to seizure with a 5-minute margin from seizure, as shown in Fig. 1. This 5-minute interval has been left to predict seizure on a minimum onset of 5 min so that the patient may be enabled to take preventive measures before occurrence of seizure. From Fig. 1, it can also be seen that there are more than one recordings for each segment in the figure. These recordings are from different electrodes placed at different positions of the brain.

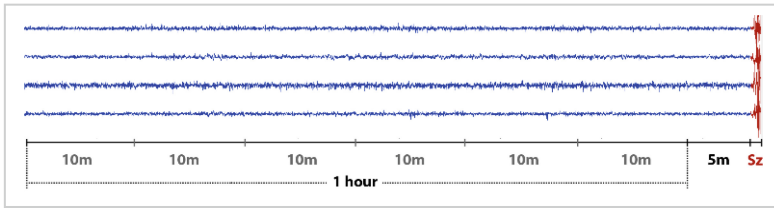


Fig. 1. Ten minutes pre-ictal clips and a five minute interval before the seizure can be seen (Source: kaggle.com)

The classification of data into preictal and interictal segments makes this a binary classification task, in which the computational model has to predict the class of a given clip. The evaluation method used in the competition is area under the ROC curve (AUC). A higher AUC means that the model has given a higher probability to preictal clips. For a perfect classification result, the AUC would be 1. The computational model is trained on the intracranial encephalogram (iEEG) data from different subjects and tested on the unseen data.

In this paper, we investigate the use of bidirectional long short-term memory (LSTM) network for seizure prediction, which to the best of our knowledge has not been addressed before. In a recent study, Random Forests and Convolutional Neural Networks (CNN) were trained and achieved AUC score in the range of 0.82–0.86 range [4].

CNN models have been more successful on image data or where a problem can be addressed such that the data is treated as images (e.g., spectrogram of speech data). However, for time-series data, RNN model would be a better suit. In a comparative study of RNN and CNN for natural language processing, which mainly involves processing of sequential data, it can be proved that RNN outperforms CNN on most of the tasks [5]. CNN model would not be able to capture the time dependencies of the data while an LSTM model look after the time dependencies both in forward and backward direction. This is one major motivation for the use of Bi-directional LSTM on the given EEG data. The rest of the paper is organized as follows: In Sect. 2, we provide a

description of the data and explain the features. Section 3 discusses the LSTM model usage. Results are reported in Sect. 4. Finally, the paper is concluded in Sect. 5.

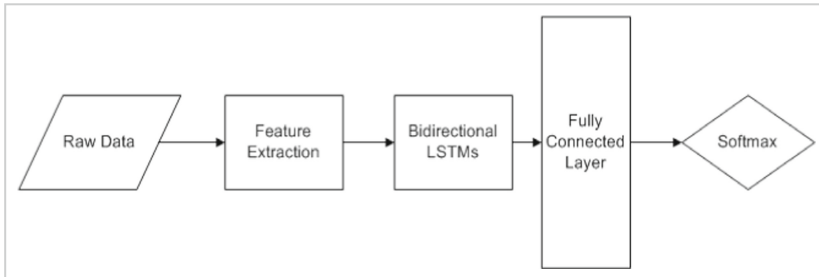


Fig. 2. Diagram showing the overall approach used in this work

Table 1. Total number of labeled clips available in the dataset

Subject	Total clips	Preictal clips	Interictal clips
Dog1	504	24	480
Dog2	542	42	500
Dog3	1512	72	1440
Dog4	901	97	804

2 Data Description and Feature Extraction

The iEEG Data used for this paper was recorded as 10-minute long clips from different subjects with a sampling frequency of 400 Hz. The data is provided by AES and hosted on Kaggle. In this work, data from four canines has been used for training of the model [6, 7].

Each clip consists of a 10-minute long recording from 16 different electrodes at a sampling frequency of 400 Hz. This implies that each clip has $600 \text{ s} \times 400 \text{ Hz} \times 16 \text{ channels} = 3.84 \text{ million samples}$. Table 1 shows that canines we selected to have 3459 recordings. This is a huge number. Thus, in order to train the model, it is important to extract useful features.

Feature extraction is done to reduce the dimensionality and extract fruitful information from the data. For this purpose, each 10-minute clip is split into 20 smaller clips of 30 s each. As each clip consists of 16 channels recordings so at the end of this process, we get $20 \times 16 = 320$ segments from each clip. Features extracted from the data are stated below.

2.1 Power Spectral Intensity

Power spectral intensity (PSI) is computed for each bin using PyEEG library [8]. PyEEG follows the below pattern to compute PSI.

- (i) Fast Fourier Transform, $X = [X_1, X_2, X_3, \dots, X_N]$ is obtained for each 30-second clip.
- (ii) PSI is calculated in eight different frequency bins using this mathematical relation.

$$PSI = \sum_{i=f_1}^{f_2} |X_i|,$$

Where f_1 and f_2 are the lower and higher values of a bin. The bins are: $\{[0.1, 4], [4, 8], [8, 12], [12, 30], [30, 50], [50, 70], [70, 100], [100, 180]\}$ in Hz. The first four frequency bins correspond approximately to the δ , θ , α and β bands respectively. These bands are used frequently in neurophysiology [9].

2.2 Standard Deviation

In addition, the standard deviation for each 30-second segment is measured as one of the features. For a smaller clip, 9 features are extracted from each channel resulting in a total of $16 \times 9 = 144$ features obtained for that clip. From a single 10-minute clip, 2880 features are mined. A random shuffle is applied to the data for faster convergence [11]. After this, the data is divided into training and test sets. A total of 2900 samples are used to train the model, and the rests 559 are used as a test set.

3 Model Training

We train Bidirectional LSTM units followed by a fully connected layer of artificial neural network (ANN). Figure 2 shows the overall approach used in this work. The features extracted from the data are used to train the model. At the last layer, a softmax layer is used to classify pre-ictal and inter-ictal EEG clips.

In this work, we have considered only the Bidirectional LSTM model, and the model is trained without any regularization technique applied. In this section, we will discuss Bidirectional LSTM [11] unit and how we used these to obtain good results.

LSTM unit is a variant of Recurrent Neural Networks (RNN). Due to the vanishing and exploding gradient problems, it is hard to train standard RNN [10, 12]. In an LSTM, the activation function is an identity function having derivative equal to 1. This stops the gradient from vanishing or exploding and rather keeps it constant. The architecture of the LSTM was presented in [10] and is formulated as:

$$f_t = \sigma_g(W_f x_t + U_f h_{t-1} + b_f) \quad (1)$$

$$i_t = \sigma_g(W_i x_t + U_i h_{t-1} + b_i) \quad (2)$$

$$o_t = \sigma_g(W_o x_t + U_o h_{t-1} + b_o) \quad (3)$$

$$\tilde{c}_t = \tanh(W_c x_t + U_c h_{t-1} + b_c) \quad (4)$$

where W_f , W_i , W_o , and W_c are the weight matrices mapping the hidden layer input to the three gates and the input cell state, while the U_f , U_i , U_o , and U_c are the weight matrices.

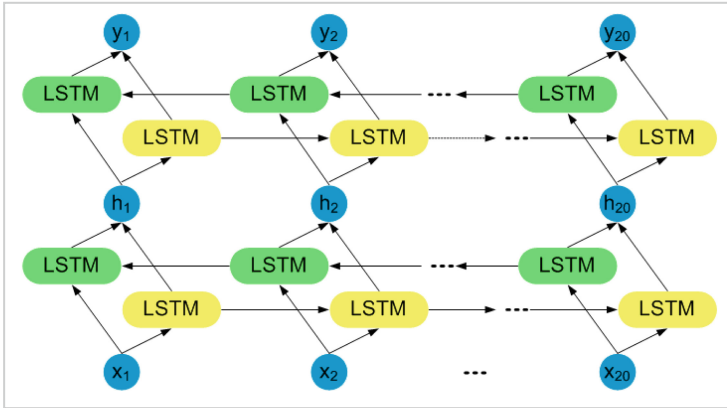


Fig. 3. A double Bidirectional LSTM layer network: each layer contains 512 hidden nodes

The b_f , b_i , b_o , and b_c are four bias vectors. The σ_g is the gate activation function, which normally is the sigmoid function, and the \tanh is the hyperbolic tangent function. With the above four equations, at each time iteration t , the cell output state, C_t , and the layer output, h_t , can be calculated as follows:

$$C_t = f_t \times C_{t-1} + i_t \times \tilde{c}_t \quad (5)$$

$$h_t = o_t \times \tan(C_t) \quad (6)$$

The LSTM architecture selected for this problem in Fig. 3 consisted of 20 forward and 20 backward LSTM cells per layer. Each cell accepts 144-dimensional vector corresponding to a single 30-second clip. The output is obtained by connecting the final LSTM cell output to fully connected layer that outputs the probabilities for both classes. We used Xavier initialization method [13] to initialize our fully connected layer variables. Adam optimization algorithm [14] is used for the training of network. The batch size is kept equal to 290.

4 Results

The performance of the model is tested with Area under the ROC curve (AUC). The importance is given to correctly predict pre-ictal events. Hence, the goal is to maximize true positive rate (TPR) and to keep a false-positive rate (FPR) reasonably low. And thus, we use Receiver Operating Characteristics (ROC) curve and Area Under ROC curve (AUC) to assess the overall performance of the model. ROC curve is a plot between TPR and FPR. The higher values of AUC indicate the better results and vice versa.

Table 2. Maximum AUC achieved using bidirectional LSTM

	Training dataset AUC	Test dataset AUC
Split1	0.88	0.84
Split2	0.93	0.81

Table 3. AUC obtained by [15] using 2 layer GRU network

	Validation dataset AUC	Test set AUC
Split 1	0.94	0.46
Split 2	0.69	0.61
Split 3	0.87	0.63
Split 4	0.82	0.64
Split 5	0.86	0.71

Table 4. Average AUC obtained by [16] using three different classifiers.

Model	Average AUC
Linear least squares	0.78
Linear discriminant analysis	0.69
Regularized SVM	0.80

To calculate TPR and FPR, we need True Positives (TP), False Positives (FP), False Negative (FN), and True Negative (TN). TP is the number of examples predicted pre-ictal and labeled pre-ictal as well. FP is the number of examples incorrectly predicted as pre-ictal. FN is the number of examples predicted incorrectly as inter-ictal. TN is defined as the number of examples predicted correctly inter-ictal by the classifier.

The results obtained using the double Bidirectional LSTM layers are encouraging. Two different splits of Training and Test datasets are used in this work. The AUC obtained in Split1 and Split2 is 0.84 and 0.81 respectively, which are better than compared to the AUC obtained by [15]. The maximum AUC reported by [15] is 0.71 and the maximum AUC reported by [16] is 0.80. This shows that our approach achieves better AUC. Results are compared with [15] and [16] as reported in Tables 2, 3 and 4.

The ROC curves for both split1 and split2 are shown in Figs. 4 and 5 respectively. From these figures, we can clearly see that the ratio of true positives is higher than false positives. The similarity between the AUC obtained for training and test sets indicates that we do not have an overfitting situation. To compare our results, we selected [15] as the authors have used the same subjects (data) with similar features' sets and trained a GRU model. In comparison, we have used a bidirectional LSTM which has given us better performance.

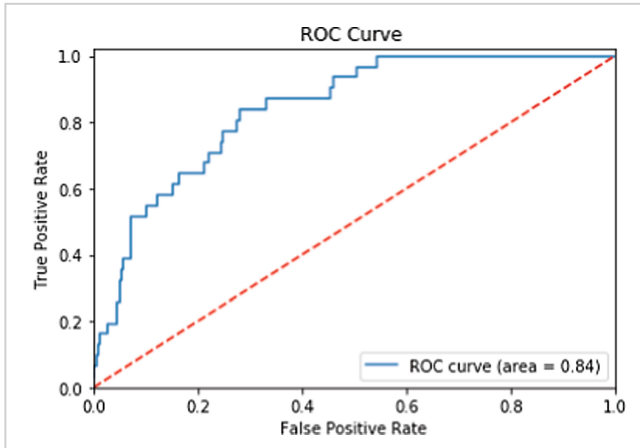


Fig. 4. Receiver operator characteristics for the split1 test dataset

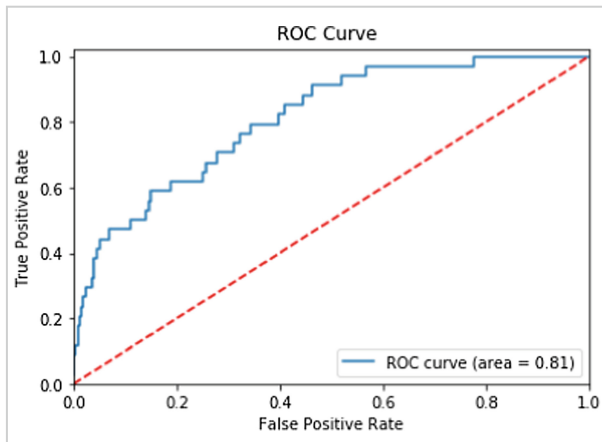


Fig. 5. Receiver operator characteristics for the split2 test dataset

5 Conclusion and Future Work

In this paper, we have investigated the use of Bidirectional LSTM on EEG data for seizure prediction. A double Bidirectional LSTM layer was trained on the features extracted from raw data. The proposed model has shown promising results when tested on unseen test set. We received test set AUC of 0.84 and 0.81 for Split1 and Split2 respectively, which is better than AUC values 0.71 and 0.80, reported by [15] and [16] respectively. The predictions of the model with unseen data are notable. We did not allow the model to overfit and the test set performance is in close resemblance with performance for train set. The EEG data is typically challenging for understanding by

humans, but with machine learning tools, we can process it and extract useful features from it. In future, much longer recordings of EEG data can be used to train the model which may then help to have even better insights into the data.

References

1. World Health Organization: Atlas: epilepsy care in the world. World Health Organization, Geneva (2005)
2. AES Seizure Prediction Challenge (2014). <https://www.kaggle.com/c/seizure-prediction>
3. Rajna, P., et al.: Hungarian multicentre epidemiologic study of the warning and initial symptoms (prodrome, aura) of epileptic seizures. *Seizure* **6**, 361–368 (1997). [https://doi.org/10.1016/S1059-1311\(97\)80035-0](https://doi.org/10.1016/S1059-1311(97)80035-0)
4. Brinkmann, B., et al.: Crowdsourcing reproducible seizure forecasting in human and canine epilepsy. *Brain* **139**(Pt 6), 1713–1722 (2016). <https://doi.org/10.1093/brain/aww045>
5. Yin, W., Kann, K., Yu, M., Schütze, H.: Comparative study of CNN and RNN for natural language processing (2017). arXiv preprint [arXiv:1702.01923](https://arxiv.org/abs/1702.01923)
6. Potschka, H., Fischer, A., Rüden, E.-L., Hülsmeier, V., Baumgärtner, W.: Canine epilepsy as a translational model? *Epilepsia* **54**, 571–579 (2013). <https://doi.org/10.1111/epi.12138>
7. Patterson, E.E.: Canine epilepsy: an underutilized model. *ILAR J.* **55**, 182–186 (2014). <https://doi.org/10.1093/ilar/ilu021>
8. Bao, F.S., Liu, X., Zhang, C.: PyEEG: an open source python module for EEG/MEG feature extraction. *Comput. Intell. Neurosci.* **2011**, 406391 (2011). <https://doi.org/10.1155/2011/406391>
9. Deuschl, G., Eisen, A., et al.: Recommendations for the practice of clinical neurophysiology: guidelines of the International Federation of Clinical Neurophysiology, Elsevier (1999)
10. Meng, Q., Chen, W., Wang, Y., Ma, Z.-M., Liu, T.-Y.: Convergence analysis of distributed stochastic gradient descent with shuffling. *Neurocomputing* **337**, 46–57 (2019). <https://doi.org/10.1016/j.neucom.2019.01.037>
11. Cui, Z., Ke, R., Wang, Y.: Deep Bidirectional and Unidirectional LSTM Recurrent Neural Network for Network-wide Traffic Speed Prediction (2018). arXiv preprint [arXiv:1801.02143](https://arxiv.org/abs/1801.02143)
12. Iqbal, T., Ali, H.: Generative adversarial network for medical images (MI-GAN). *J. Med. Syst.* **42**(11), 231 (2018). <https://doi.org/10.1007/s10916-018-1072-9>
13. Glorot, X., Bengio, Y.: Understanding the difficulty of training deep feedforward neural networks. In: Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics, in PMLR, vol. 9, pp. 249–256 (2010)
14. Kingma, D., Ba, J.: Adam: a method for stochastic optimization (2014). arXiv preprint [arXiv:1412.6980](https://arxiv.org/abs/1412.6980)
15. Larmuseau, M.: Epileptic seizure prediction using deep learning, MS Thesis, Ghent University (2016)
16. Gonzenbach, M.: Prediction of epileptic seizures using EEG data, MS Thesis, ETH Zurich (2015)



Hybrid Machine Learning Models of Classifying Residential Requests for Smart Dispatching

Tianen Chen, Jincheng Sun, Hongyi Lin, and Yan Liu^(✉)

Concordia University, Montreal, QC H3G 1M8, Canada
yan.liu@concordia.ca

Abstract. This paper presents a hybrid machine learning method of classifying residential requests in natural language to responsible departments that provide timely responses back to residents under the vision of digital government services in smart cities. Residential requests in natural language descriptions cover almost every aspect of a city's daily operation. Hence the responsible departments are fine-grained to even the level of local communities. There are no specific general categories or labels for each request sample. This causes two issues for supervised classification solutions, namely (1) the request sample data is unbalanced and (2) lack of specific labels for training. To solve these issues, we investigate a hybrid machine learning method that generates meta-class labels by means of unsupervised clustering algorithms; applies two-word embedding methods with three classifiers (including two hierarchical classifiers and one residual convolutional neural network); and selects the best performing classifier as the classification result. We demonstrate our approach performing better classification tasks compared two benchmarking machine learning models, Naive Bayes classifier and a Multiple Layer Perceptron (MLP). In addition, the hierarchical classification method provides insights into the source of classification errors.

Keywords: Machine learning · Natural language processing · Text classification

1 Introduction

The context of smart cities relates to the capability of analyzing and responding to specific requests from residents. In addition to social media networks such as Twitter and Chinese Weibo, an important source of city events down to the county level are service requests directly reported from metropolitan residents. These requests are through phone calls, emails and chatbots sent to metropolitan residential service centers that employ Human agents to dispatch the requests manually to corresponding service sectors for handling such issues. However, the processing capacity of call centers is bounded by the limitation of human operation. Therefore an artificial intelligence-enabled system helps to automatically

convert audio-based reported requests into text content and then dispatches the request to the corresponding sector of services. Such automation improves service responsiveness.

The core of such an automated request analysis and dispatching system is a machine learning model that classifies a request in natural language to an organization that is responsible for handling the case. To scope the research problem, this paper has the assumption that requests are all text-based. Any audio request is converted to the text-based content. The issues of classifying these text-based request data are two aspects. First, the labels for classification require processing on the raw datasets to produce suitable labels. It could be assumed that the field called the responsible department in the original dataset should be the labels. However, the responsible departments are also presented in natural language description that contains abbreviation, location information and less precise rename of a department. In addition, future requests may even result in new department names that are not part of the historical labels. Another issue is the request distribution over the corresponding responsible departments by nature are not evenly distributed. Some responsible departments are of small request cases and lead to the overall datasets unbalanced.

In this paper, we propose a hybrid method to address the above two issues. Our method consists of (1) an NLP processing workflow for feature extraction; (2) a clustering algorithm for generating meta-classes for hierarchical training; (3) multiple classifiers with a Naive Bayes model, a fully connected neural network model and a residual neural network model to produce an optimal inference for a certain request. Training the classification with generated meta-classes, we gain insights into the classification errors.

A use case of our hybrid method has been developed on over 80,000 sample requests in Chinese that involve 157 responsible departments. Our method achieves with testing precision of 76.42% and log loss value of 1.192 over 35,663 test data that collected in different time period than the training datasets. Our code and samples of the dataset are open-sourced on Github¹.

The **contribution** of this paper is three-fold as follows:

- We build an NLP-based feature engineering workflow with a rigorous measure of feature prediction power using information values;
- We demonstrate a hybrid machine learning method with both unsupervised and supervised machine learning to classify residential requests over unbalanced data sample distribution;
- We develop three classifiers to ensemble the best classification result. We compare the classification performance with two benchmarking models.

The structure of this paper is organized as follows: Sect. 2 presents the related work. In Sect. 3, we introduce our dataset and feature engineering techniques. Section 4 describes a hierarchical classification method of generating meta-classes for classification of a large number of classes. The hybrid machine learning models in Sect. 5. Finally, we present our assessment metrics and experiment results of the classification performance in Sect. 6. We conclude our paper in Sect. 7.

¹ <https://github.com/OneClickDeepLearning/classificationOfResidentialRequests>.

2 Related Work

Learning from Few Labeled Data. Kamal et al. proposed an Expectation-Maximization based method [1] to train a classifier with few labeled data and use the classifier to label the high-confidence unlabelled data, then use the labeled data to train a new classifier, and repeat this process until the classifier converge. Blum et al. [2] proposed a co-training method that allows learning from two views of the features. Rajat et al. proposed a Self-taught method that uses Auto-Encoder to learn higher-level representations with unlabelled data [3].

Imbalance Dataset. Nitesh et al. presented a method of SMOTE (Synthetic Minority Over-sampling Technique) [4] to over-sampling the minority class by creating synthetic minority samples that fall between the minority data and their nearest neighbors. If the distance between the minority data and the neighbors is far, the synthetic data will have a large range of noise. Hui et al. presented a Borderline-SMOTE method [5] ensures that the sampling happens only when the majority of the selected neighbors are minority data to lower the randomness of noise.

Ensemble of Classifiers. Breiman proposed a bootstrap aggregating method [6] using bootstrap to extract several sub training sets from the original training set and train a classifier for each sub training set. Then each classifier gives a weighted vote for the classification. Yoav and Robert proposed a boost-based method called AdaBoost that uses weighted data to train weak classifiers. The data miss-classified by a weak classifier gains more weight to train the next weak classifier. The weak classifiers are weighted to form a confident classifier. Based on AdaBoost [7] method, Wei et al. proposed a cost-sensitive Boosting [8] that increases the weight of misclassified training data that have a higher cost.

Hierarchical Classification. Pei-Yi et al proposed a hierarchically SVM text classification method that split a problem into sub-problems in the classification tree that can be solved accurately and efficiently [9]. A hierarchical softmax architecture [10] was proposed by Morin and Bengio when dealing with a huge number of output classes. It significantly speeds up the training time compared to feed-forward networks.

Convolutional Neural Networks on NLP Tasks. Convolutional Neural Network (CNN) models have been demonstrated performing well in the NLP tasks of sentence classification [11, 12]. A CNN model consists of layers of convolutions with non-linear activation function such as *ReLU* or *tanh*. In a CNN model, convolutions over the input layer are used to compute the output. As illustrated by Zhang [13], each region of the input is connected to a neuron in the output. Then each layer applies a filter to detect higher-level features. These features further go through a pooling layer to form a univariate feature vector for the penultimate layer. The final softmax layer then receives this feature vector as input and uses it to classify the sentence.

Kim applied a single convolutional layer on top of Word2Vec embeddings [14] of words in a sentence to perform classification tasks. His work proves that

convolutional neural network, with a good representation of the words, can provide promising results on NLP problems. Conneau et al. proposed ResNet-like deep convolutional neural network [15] that can learn the different hierarchical representation of the input text. They use small convolutions and let the network learn what is the best combination of these extracted features. Their work allows the network to be deeper and finer-grained. Prabowo and Thelwall proposed a series of hybrid classifiers [16] that combine different rule-based classifiers and SVM as a pipeline to solve sentiment analysis problems and achieved good performance.

3 Feature Engineering

Feature engineering processes and transforms the dataset in texts to word vectors as inputs of machine learning models. The original dataset contains eight features with *id*, *time stamp*, four *categories* of responsible departments, *request description*, and *responsible department description*.

The feature engineering workflow is depicted in Fig. 1. Feature engineering first removes invalid data samples in which the values of the responsible department description are missing or originally marked as non-available. The training dataset contains 849,861 records, including 145,542 records originally marked as invalid and 58,394 records without a responsible department description. Finally, valid dataset contains 645,924 records.

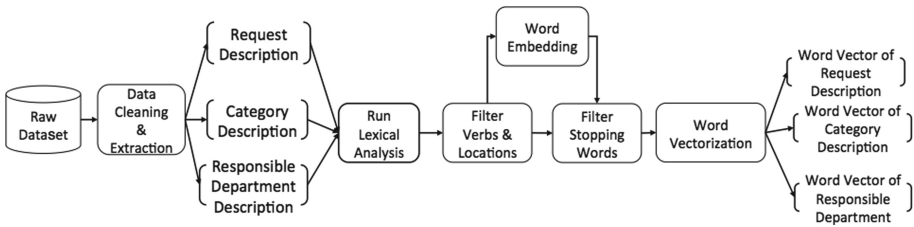


Fig. 1. The major steps of feature engineering on two features of request description and responsible department description

3.1 Data Preprocessing

Sentences are segmented into tokens before feature extraction. Two major methodologies of tokenization and segmentation are dictionary-based and statistics-based. The dictionary-based methods recognize words based on a maintained vocabulary [17], while the statistics-based approach uses corpus as a resource to build a word-segmentation model. In this paper, we process the tokenization and segmentation with the second method using a tool called LTP, a Chinese language technology platform [18]. LTP consists of six Chinese processing modules, including (1) Word Segmentation (WordSeg); (2) Part-of-Speech

Tagging (POSTag); (3) Named Entity Recognition (NER); (4) Word Sense Disambiguation (WSD); (5) Syntactic Parsing (Parser) and Semantic Role Labeling (SRL).

Further on, the segmented tokens are filtered by lexical analysis modules of LTP to eliminate tokens that include digits, words in other languages, punctuation, and stop words. A combined list of public available stopping-words is applied to the LTP tool. In addition, verbs, adjectives, adverbs are also excluded. Organization names and location-relevant nouns consist of more than one tokens. The NER module of LTP recognizes and merges these nouns into single words.

3.2 Data Distribution

The feature that contains the labeling information is *responsible department description*. A simplified illustrating sample is depicted in Fig. 2. The description needs further processing to generate labels for training and inference. The reason is the description usually contains location phrases with various levels of metropolitan granularity, national, provincial, county, and local communities. This means the records with the same responsible department but different location nouns become separate classes. As a result, the dataset distribution over the labels is spread widely with a large number of classes and the density of classes is diluted. Such a circumstance degrades the training quality and inference accuracy.

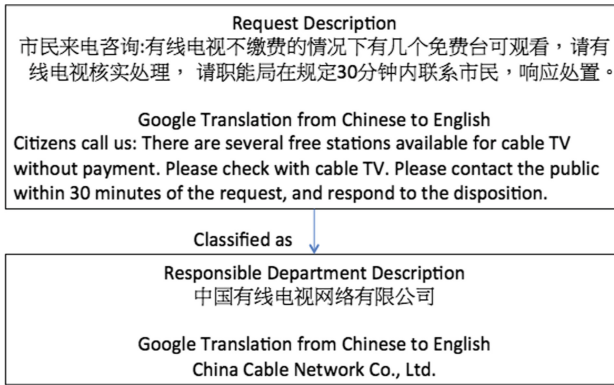


Fig. 2. One data sample with features of request description and responsible department description

To solve the above problem, we separate the location nouns from department names and titles. Only the organization names and titles remain to generate training labels. For cases that the department names and titles are in abbreviation, we set up a dictionary and manually create an entry mapping between the standard full name and any forms of variation including abbreviation. This

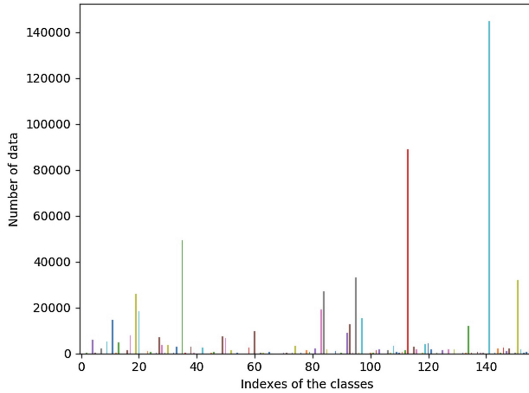


Fig. 3. Data distribution statistic for 157 classes, the x-axis is the index of the classes and the y-axis is the total number of data of a class

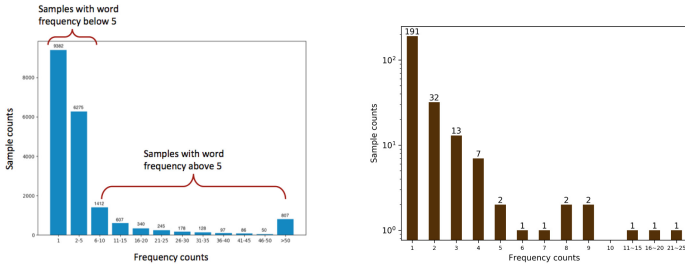
leads to 157 unique department names and titles, which are considered as the labels for classification. We further plot the data sample distributions over the 157 classes in Fig. 3. Among them, there are 101 classes whose data sample sizes are below 1000 samples (approximately 1000 out of a portion of 0.15%).

We further explore the dataset characteristics upon observations of data distribution. We develop an inverted index of words in each request description record. The Bag-of-Words (BoW) algorithm [19] is used to build the word pairs with their word counts per record. The word and the sample become a vector that is stored. Such a vector allows us to trace the word occurrence in samples. Therefore we compute the statistics of sample counts grouped by the word occurrence frequency.

Figure 4(a) plots the word frequency distribution. This plot is interrupted as 9382 data samples contain words that only occur once in the whole request description text; 6275 data samples contain words occur 2 to 5 times in the whole request description text. The words of high frequency (such as over 50) only appear in a limited number of samples (such as 807 samples). Since stopping words are already filtered, this plot in Fig. 4(a) indicates words with low frequency should be further measured with their relevance of other words in the feature space. Likewise, we produce the plot of word frequency and distribution of 157 labels as shown in Fig. 4(b). Our solution is training the Word2Vec model to generate the word embedding that represents the relations of word tokens in a high dimensional space. The details are presented in Sect. 3.4.

3.3 Information Values of Features

Information values and Weight-of-Evidence (WoE) are techniques of feature selection. Information values measure the prediction power of a feature. The decision to select the four categories of responsible departments as features is evaluated by their information values. The value of each category are tags edited



(a) Data sample distribution over word frequency in request description (b) Label distribution over word frequency

Fig. 4. Data and label distribution



Fig. 5. Data sample of categories

by customer service operators. A data sample is depicted in Fig. 5. The bottom textbox shows the corresponding responsible department. The four categories represent four levels of tags as a whole capturing context of the request. The tokenization and segmentation workflow is applied to each category. We combine tags of four categories as a combo for the information value analysis. By statistics, there are 418 unique values of category tag combo.

$$[tag_1, tag_2, \dots, tag_n], n = 418$$

The information values (IVs) are calculated to measure the prediction power of the category tag combo to the class label as the responsible department. Therefore, the 157 responsible departments and the 418 category tag combo form a 157×418 vector. Each entry of this vector is notated as $TagCombo_{i,j}$, which represents the counts of data samples with tag combo j that belong to responsible department i . Then the notation of $Non - TagCombo_{i,j}$ represents the total counts of data samples with tag combo $l \neq j$, that is

$$Non - TagCombo_{i,j} = \sum_{l=1, l \neq j}^{418} \#tag - combo_{i,l}$$

住房保障-物业服务管理-停电-故障停电 Housing security - property service management - power outage - power outage				
<i>Responsible Department_i</i>	<i>TagCombo_j</i>	<i>NonTagCombo_j</i>	<i>WoE_{ij}</i>	<i>IV_{ij}</i>
供电政府服务中心 (Power Supply Service Center)	9	409	0.18598	0.01893

Fig. 6. Sample calculation of IV

Now, we can calculate the value of WoE as

$$WOE_{i,j} = \ln\left(\frac{TagCombo_{i,j}}{Non - TagCombo_{i,j}}\right)$$

Hence, we calculate the information value vectors for each category tag combo *j* for responsible department *i* as shown in Fig. 6.

Finally, the IV values of each category tag combo are summed up for all 157 responsible departments to measure the prediction power of each tag combo as

$$IV_{i,j} = (TagCombo_j\% - Non - TagCombo_j\%) * WOE_{i,j}$$

$$IV_{TagCombo_j} = \sum_{i=1}^{157} IV_{i,j}$$

According to the rule of thumb described above, we find only 13 out of 418 category-combos are weak predictions, that is IV value is in the range of (0.02,0.10]. The rest of category-combos have IV values below 0.02, which indicates not useful for prediction. In another word, it means category-combo is not an important feature for classifying responsible departments. They are not selected as input features for classifiers.

3.4 Feature Extraction

Feature extraction is to produce the word tokens into word vectors with numerical values. In this paper, we apply two methods namely Term-frequency-inverse document frequency (TF-IDF) [20], and Word2Vec [17].

Generating Word Vector Using TF-IDF. TF-IDF measures the relevance of words, not frequency. That is, word counts in the inverted index discussed in Sect. 3.2 are replaced with TF-IDF relevance weight across the whole dataset. With TF-IDF, the more samples a word appears in, the less valuable that word is as a signal to differentiate a given request. The relevance weight of a word is calculated in Eq. 1.

$$w_{i,j} = tf_{i,j} \times \log\left(\frac{N}{df_i}\right) \tag{1}$$

where N is the number of samples; $tf_{i,j}$ represents the number of occurrence of word token i in sample request j ; df_i represents the number of occurrence of request samples that contain the token i . The vector of $w_{i,j}$ is a normalized data format that adds up to one for all the samples. This TF-IDF vector is used as input to the Naive Bayes classifier discussed in Sect. 4.3.

Word Embedding Using Word2Vec. Word embedding maps word tokens of varied length to a fixed-length word vector as inputs to machine learning models. In nature, word embedding reconstructs linguistic contexts of words and produces a vector space. The algorithm of Word2Vec uses a group of related models that are two-layer neural networks that are trained over a large corpus of text and produces a vector space, typically of several hundred dimensions. Each unique word in the corpus is assigned a corresponding vector in the vector space so that words that share common contexts in the corpus are located in close proximity to one another in the space [17].

We have trained the Continuous Bag-of-Words structure (CBOW) of the Word2Vec model with a corpus collected from the whole dataset. We segment the whole dataset of 65,9421 samples with sentences into data blobs of every five continuous words as input. The central word is the target for output. Empirical experiments indicate using the training dataset as corpus produces a better classification performance. The details of the experiments are not central to the research scope of this paper, thus omitted.

By statistics, we observe the word length in a request description of the dataset ranges from 1 to 780 with a weighted average of 46. Over 90% of the request descriptions have less than 100-word tokens. Thus we set the word vector dimension as 100, and pad zero if the word length is less than 100.

4 Hierarchical Classification Method

A hierarchical classification method handles classification of a large number of possible classes [21]. The current training dataset contains 157 unique labels and thus 157 classes. We develop a hierarchical classification method to evaluate whether it works for our dataset. There are two kinds of hierarchical classification. One uses meta-classes as a two-hierarchy structure where leaf classes are grouped by similarity into intermediate classes (the meta-classes) [9]. The other one copes with a pre-defined class hierarchy, a type of supervised learning. In this paper, our method is the former case by means of which we build the hierarchy during the training by a clustering method, and then classify a sample from the meta-classes to the leaf-classes.

4.1 Meta-Class Generation Using K-Means and GMM

To create meta-classes for 157 labels according to similarity, we first apply the K-Means clustering algorithm [22]. The K-Means algorithm first assigns each

sample to the cluster whose mean values have the least squared Euclidean distance. Secondly, it calculates the new means to be the centroids of the observations in the new clusters. Finally, the algorithm converges when the assignments no longer change. K-Means applies hard clustering by assigning data points to a cluster. This implies a data sample is assigned to the closest cluster. K-Means is simple to train but does not guarantee convergence to the global optimal whereby degrades the clustering accuracy.

The Gaussian Mixture Model (GMM) [23] is a finite mixture probability distribution model. The parameters of GMM are estimated iteratively by using the Expectation-Maximization (EM) algorithm [23]. GMM/EM determines a sample's probability of belonging to a cluster, which is a soft clustering process. Each cluster, therefore, can have different options to constrain the covariance such as spherical, diagonal, tied or full covariance, instead of only spherical in K-Means, which means the clustering assignment is more flexible in GMM than in K-Means. The EM algorithm has its limitation. One issue is the number of mixtures affects the overall performance of EM and this number is an unknown prior. Therefore, the optimal number of mixtures is important to ensure an efficient and accurate estimation.

Our solution is applying K-Means to obtain values of centroids (or geometric centers), then initializing GMM with centroids values [24]. The input to K-means is a word vector with 100 dimensions of 157 class labels produced from the feature extraction process described in Sect. 3. We apply silhouette coefficients to select the optimal value of K . A silhouette coefficient of a range of $[-1, 1]$ indicates (1) a sample is far away from the neighboring clusters with the value near $+1$; (2) or a sample is on or very close to the decision boundary between two neighboring clusters with the value of 0 ; (3) or a sample might have been assigned to the wrong cluster if the value is negative. Figure 7 plots the clustering result with the optimal K value as 5. We derive the silhouette coefficients by setting the K value range in $[3, 10]$. After the silhouette analysis, we consider $K = 5$ is the optimal value for K-Means/GMM/EM clustering. Figure 7 plots the 5 clusters of 157 labels.

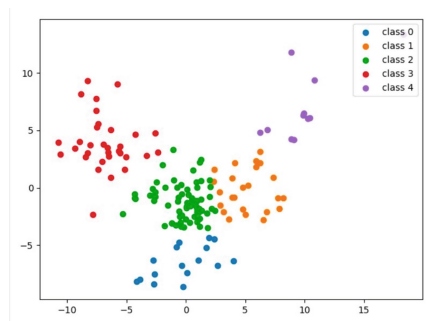


Fig. 7. The plot of K-means and GMM clustering

4.2 Meta-Class Generation Using Topic-Based Clustering

We develop another clustering method that considers the 157 labels as topics to cluster them into groups with similar themes. In this method, we apply the clustering method of OPTICS (Ordering Points To Identify the Clustering Structure Closely) [25] that finds a core sample of high density and expands clusters from them. The output from OPTICS provides K clusters. In our method, we apply LDA (Latent Dirichlet Allocation) to output K topics. Each topic consists of a fixed size of words and their associated weights. LDA assumes the Dirichlet prior distribution of topics. In practice, the Dirichlet prior distribution assumes documents (or labels in our case) cover only a small set of topics and topics consist of a small set of words frequently. Finally, we assign labels to a cluster by an entropy-based algorithm. The algorithm is listed below. The input to this topic-based algorithm is the output of the word vector representation of the 157 labels in 157×10 dimensions. The output is K clusters of 157 labels. The clustering result is shown in Fig. 8.

Algorithm 1. Topics and Entropy Based Clustering

Input: $\hat{k} \leftarrow \{k_j\}, j \in [1, 157]$ word vector of 157 labels
Output: Clusters of 157 labels
 $\varsigma \leftarrow$ number of clusters output from OPTICS on Input
 $num_topics \leftarrow \varsigma$ to initialize LDA;
 $\hat{v}_t \leftarrow$ output from LDA; {a topic vector of $\varsigma \times 10$; each entry is a tuple t of [word: weight]}

```

foreach  $\hat{v}_t[i], i \in [1, \varsigma]$  do
   $l \leftarrow |\hat{v}_t[i]|$ ; {number of tuples}
   $c_i = \frac{1}{|l|} \sum_{t \in \hat{v}_t[i]} t.weight$  {calculate the centroid}
  foreach  $k_j, j \in [1, 157]$  do
     $p(k_j) = \frac{sim(k_j, c_i)}{\sum_{r=1}^{\varsigma} sim(k_j, c_r)}$ 
     $e_{k_j}^i = -p(k_j) \cdot \log(p(k_j))$  {calculate the entropy of  $k_j$  to a topic  $\hat{v}_t[i]$ }
  end
end
Assign  $k_j$  to the topic cluster  $m$  whose entropy  $e_{k_j}^m$  is minimal;

```

4.3 Hierarchical Classification

The clustering algorithms generate the meta-classes of 157 labels for training a classifier. The classification is of the structure of a two-level tree as depicted in Fig. 9. The leaves are 157 labels and the non-leaf nodes are the K meta-classes.

A classifier is first trained with the meta-classes, noted as $Model_{meta}$. The classification decides the meta-class that a sample belongs to. As a result, the original data samples are grouped into K clusters. Furthermore, each meta-class i contains L_i labels and $\sum_{i=1}^K L_i = 157$. The data samples classified to one

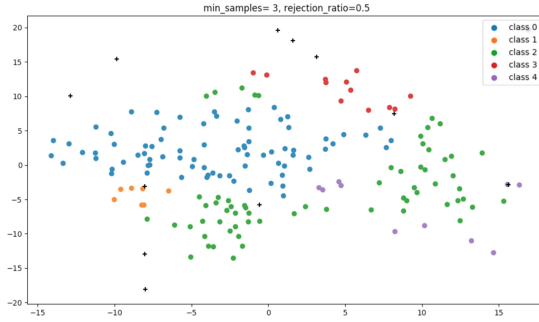


Fig. 8. Topic based clustering result

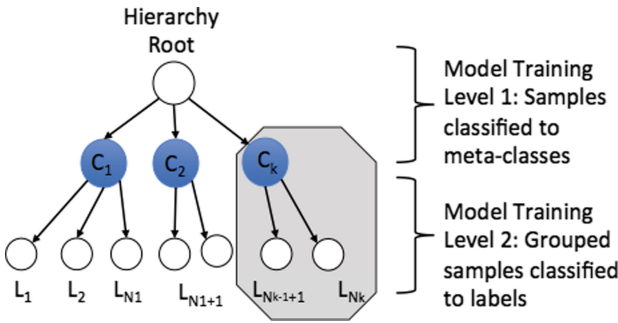


Fig. 9. The two-level hierarchy of classes

specific meta-class are used again to train a sub-model to further classify these samples to the leaf classes. The hierarchical training produces one meta-class model, noted as $Model_{meta}$ and K number of leaf-class models, one for each cluster. In total, we have $K + 1$ models.

When it comes to inference, there are two methods. The first method inputs the test sample to $Model_{meta}$. Based on the classification on the meta-class, the test sample is further fed to one of the leaf-class models. The second method directly inputs the test samples to each of the leaf-class models. The classification with the highest probability is selected to be the classification result. The first method has shorter inference time as it runs two models, while the second methods run K models. In term of accuracy, the second method tends to be more accurate as it reduces the error propagation from the meta-class level.

Hierarchical Naive Bayes Classifier. Both the meta-class model and leaf-class model use the Naive Bayes classifier. The difference is the meta-class model has five classes for classification as the results of topic clustering of the labels.

In the context of the inputs, X contains the word tokens of the request description. Further, we adopt the Bernoulli Naive Bayes classifier to encode the input of word tokens. The Bernoulli Naive Bayes classifier assumes each feature

has only binary values. In this case, the word token is encoded as a one-hot bag of words model that means 1 indicating the presence of the term or 0 indicating absence of the term. This leads to 19,607 dimensions of input features from the request description of 40,000 training set. The limitation of this approach is that when the training set changes, the input needs to be encoded again. For example, 80,000 training set leads to 32,698 dimensions of word token one-hot encoding. To avoid the zero value of $P(x_i|y_j)$ causing the posterior probability always being zero, 0.2 smooth value is added to each conditional probability $P(x_i|y_j)$. y represents a set of 157 responsible departments $\{y_1, \dots, y_{157}\}$. The classification is calculated as the class y_j that produces the maximum probability given the feature set of X .

$$P(\hat{y}|x_0, \dots, x_n) \propto \max_{j=1}^{157} P(y_j) \cdot \prod_{i=1}^n P(x_i|y_j) \quad (2)$$

$$\hat{y} = \arg \max_{j=1}^{157} \prod_{i=1}^n P(x_i|y_j) \cdot P(y_j)$$

Hierarchical MLP Neural Network. By applying a neural network model to the task of text classification, we assume the complex function created using the network of neurons is close to the true relationship between the input features (such as word tokens of request description) and the output (in our case the 157 classes of responsible departments). In other word, a neural network with a certain number of hidden layers should be able to approximate any function that exists between the input and the output according to the Universal Approximation Theorem [11].

We develop a Multiple Layer Perceptron neural network classifier in the hierarchical model. In this model, both the meta-class model and the leaf-class model have the same network structure as listed in Table 1 except that the output layer of the meta-class is 5 instead of 157. Accordingly, the weight size is 128×5 of the meta-class model. Within this structure, each input neuron is connected to each output neuron in the next layer, referred to as a Dense layer. Given the input to the first Dense layer is of the size of $10,000 = 100 \times 100$, the output of the Dense layer is 512, then the size of weights of this Dense layer is $10,000 \times 512$. We stack two Dense layers with one output layer of 157 classes. The network structure is listed in Table 1.

Table 1. The structure of fully connected neural network

Layers	Input size	Output size	Kernel (Weight) size
Dense	10,000	512	$10,000 \times 512$
Dense	512	128	512×128
Output	128	157	128×157

5 Hybrid Machine Learning

This hierarchical classification method is useful to deal with a large number of classes by means of training a classifier for a much smaller number of classes (at the level of meta-classes) while keeping comparable levels of confidence. The main issue with hierarchy classification is error propagation. Since the error in the meta-class level classification propagates to the leaf-class classification directly.

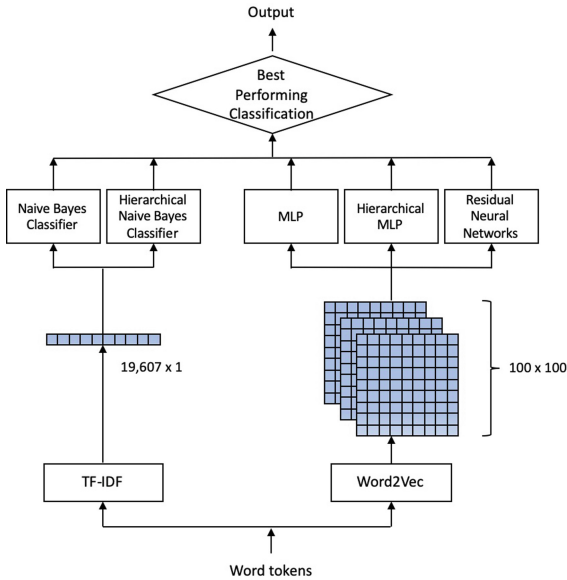


Fig. 10. Overview of hybrid machine learning models with word embeddings

To improve the classification performance, we further develop a residual neural network classifier inspired by ResNet [26]. By ensembling, the hierarchical model and the residual neural network model, the structure of a hybrid learning method is depicted in Fig. 10. We add in two basic models as benchmarks Naive Bayes classifier, and an MLP classifier. In totally, we have 5 classifier outputs on the same datasets. A simple ensembling method selects the best performing classification results according to metrics of *log loss*. Classifiers based on Naive Bayes use inputs from word embedding of TF-IDF as a 19,607-dimension word vector. Other three neural network models based on Word2Vector embedding as $100 * 100$ dimension vectors.

5.1 Residual Convolutional Neural Network

In this paper, we apply the *Full pre-activation* structure proposed by He et al. [27] to build our convolutional layers. To minimize the gradient vanishing

problem when a CNN model grows with deep layers, residual skip connections or identity mapping are added to convolutional layers. The input to a layer $F(X)$ is added to convolutional output as a combined input to the next layer, $y = F(X, \{W_i\}) + W_s X$. This structure allows the gradient to be propagated without loss of representations. It is considered that the skip connection and the convolutional layer together form a Residual Block layer. In our model, a Residual Block contains two convolutional layers as shown in Fig. 11.

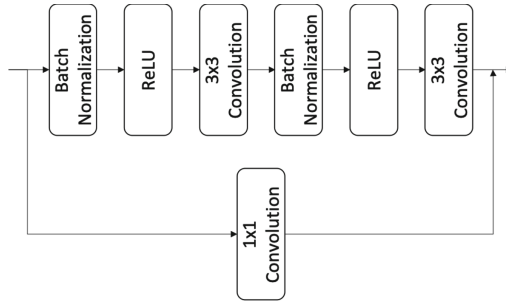


Fig. 11. Structure of the residual block

A *Batch Normalization-Activation* layer is placed in-between two convolutional layers. As discussed in the paper [27], 1×1 convolution can be useful when there are fewer layers, thus we choose the 1×1 convolution layer as the skip connection method. Based on the Residual Block structure, we build our 20-layer residual convolutional neural network model shown in Table 2.

6 The Evaluation

The evaluation focuses on the assessment of the classification performance. We compare the metrics of training five models with different sizes of training data and testing the models with data collected at different time spans.

6.1 The Data Setup

The dataset contains 659,421 samples. We split the data with a ratio of 80%:20% for the training set and the test set. We further partition the training set into shards of 40,000 samples for each shard. Likewise, we partition the test set into shards with 4,000 samples in each shard. Hence, the usage of the dataset is in the unit of a shard. We set up experiments of running 5 models on two data settings: (1) one shard of training set with one shard of test set; and (2) two shards of the training set with one shard of the test set.

In addition to the 659,421 samples, we also test the best performing model using the data collected in a different time period that contains 35,663 valid samples.

Table 2. Structure of Residual CNN

Layers	Kernel	Output size
Convolution	$[3 \times 3, 32] \times 1$	100×100
Residual block	$\begin{bmatrix} 3 \times 3, 32 \\ 3 \times 3, 32 \end{bmatrix} \times 1$	100×100
Residual block	$\begin{bmatrix} 3 \times 3, 64 \\ 3 \times 3, 64 \end{bmatrix} \times 2$	50×50
Residual block	$\begin{bmatrix} 3 \times 3, 128 \\ 3 \times 3, 128 \end{bmatrix} \times 2$	25×25
Residual block	$\begin{bmatrix} 3 \times 3, 256 \\ 3 \times 3, 256 \end{bmatrix} \times 2$	13×13
Residual block	$\begin{bmatrix} 3 \times 3, 512 \\ 3 \times 3, 512 \end{bmatrix} \times 2$	7×7
Dense		157

6.2 The Model Assessment

The evaluation defines model assessment metrics as Precision and Recall. For a multi-classes classification model, the Precision and Recall score should be calculated for each class and take the average score as the final score. There are two averaging methods, *micro*, and *macro*. The macro method considers every class has the same weight, while in the micro method every data has the same weight. The calculation is as shown below, P_i is the Precision of the i th class, and R_i is the Recall of the i th class. l is the total number of classes.

$$\begin{aligned}
 P_{macro} &= \frac{1}{l} \sum_{i=1}^l P_i & P_i &= \frac{TP_i}{TP_i + FP_i} \\
 R_{macro} &= \frac{1}{l} \sum_{i=1}^l R_i & R_i &= \frac{TP_i}{TP_i + FN_i} \\
 P_{micro} &= \frac{\sum_{i=1}^l TP_i}{\sum_{i=1}^l TP_i + \sum_{i=1}^l FP_i} \\
 R_{micro} &= \frac{\sum_{i=1}^l TP_i}{\sum_{i=1}^l TP_i + \sum_{i=1}^l FN_i}
 \end{aligned} \tag{3}$$

where

TruePositive(TP): the real label is positive and the predicted label is also positive;

FalsePositive(FP): the real label is negative and the predicted label is positive;

TrueNegative(TN): the real label is negative and the predicted label is also negative;

FalseNegative(FN): the real label is positive and the predicted label is negative.

The above metrics focus on if the classification is correct or not. Log Loss measures the distance between the predicted label and the real label. It takes the prediction probability for each class of a model as the input and outputs a log loss value as calculated in Eq. 4. The lower the log loss value (such as close to zero), the better performance of a model is. l is the total class number, y_i is the real label and p_i is the predicted probability of class i .

$$LogLoss = \sum_{i=1}^l y_i \log(p_i) + (1 - y_i) \log(1 - p_i) \tag{4}$$

6.3 The Experiment Results

The first set of experiments evaluate the classification performance of the five models. The training data sets are of one shard (40,000 samples) and two shards (80,000 samples) respectively. The test data set is one shard of 4,000 samples. Both the training set and test set are from data samples collected within the same span of time. Table 3 list the metrics measured for 5 classification models.

Table 3. Classification performance on five models

Models	Training subset	Metrics			
		Precision		Recall	
		Micro	Macro	Micro	Macro
Hierarchical MLP	40,000	0.633	0.247	0.633	0.214
	80,000	0.686	0.332	0.686	0.288
MLP	40,000	0.662	0.276	0.662	0.236
	80,000	0.689	0.281	0.689	0.233
Hierarchical naive bayes	40,000	0.746	0.439	0.746	0.367
	80,000	0.719	0.375	0.719	0.288
Naive bayes	40,000	0.734	0.358	0.734	0.254
	80,000	0.700	0.296	0.700	0.194
Residual CNN	40,000	0.754	0.420	0.754	0.389
	80,000	0.787	0.510	0.787	0.444

Training Sample Size. By doubling the training sample size, we observe three models improve the classification performance, including MLP, Hierarchical MLP, and Residual CNN.

Both Naive Bayes and Hierarchical Naive Bayes metrics decrease. As presented in Sect. 4.3, we obtain 19,607 dimensions of input features from the request description of 40,000 training set and 32,698 dimensions of word token one-hot encoding from 80,000 training set. The observation from this experiment indicates increasing the feature size impacts the performance of our implementation of Naive Bayes classifier. Our Naive Bayes classifier learns one shard of the training set more linearly separable than the doubled size of the training set. In comparison, the word embedding method applied allows the MLP and the Residual CNN classifiers remain the same feature size of 100 dimensions of word token vectors regardless of the size of training data.

Hierarchical vs Non-hierarchical. Hierarchical classification improves the marginal performance of Naive Bayes classifier. For MLP and Residual CNN, they both perform better than hierarchical classification. In all experiments, Residual CNN outperforms other models. Hierarchical classification overall has lower performance than non-hierarchical classification. The benefit of introducing meta-class through the hierarchical classification method is observing the source of classification errors. Figure 12 shows the classification results with 5 meta-classes. It indicates the classification errors are mainly from the fact that class 2 and 4 are misclassified to class 1; class 1, 3, and 4 are misclassified to class 2. We also observe from the experiments that all the five classifiers produce over 80% precision for the 5 meta-class classifications. The precision is higher than the classification performance of 157 classes. Due to the space limitation, we skip the values in details.

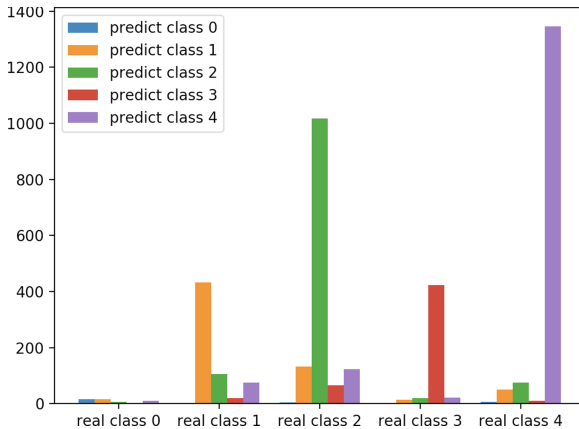


Fig. 12. Distribution of predicted classes vs real classes

Blind Test. The second set of experiments run on a blind test. We select the best performing model trained from each of the 5 classifiers and further test them using the whole 35,663 data samples collected from a different span of time than the first set of experiments. The result is shown in Table 4. Two classifiers, Naive Bayes and Residual CNN produce better classification performance than other three classifiers. Still, Residual CNN performs the best on the blind test data.

Table 4. Classification performance of blind test

Models	Metrics			
	Precision		Recall	
	Micro	Macro	Micro	Macro
Hierarchical fully connected NN	0.650	0.244	0.650	0.192
Fully connected NN	0.689	0.259	0.689	0.214
Hierarchical naive Bayesian	0.678	0.251	0.678	0.201
Naive bayesian	0.726	0.295	0.726	0.256
Residual network	0.764	0.417	0.764	0.352

Log Loss. We further evaluate the Residual CNN performance on the blind test data using log loss to measure the distance between the predicted label and the real label. The result is listed in Table 5. When applied to different test data, the Residual CNN has marginal log loss change.

Table 5. Log loss of hybrid classifiers

Models	Test data size	Log loss
Best performing residual CNN	4,000	1.152
	35,663	1.192

Inference Time. We further measure the inference time taken on the 4,000 test data set. Note that the classifiers of Naive Bayes and Hierarchical Naive Bayes run on a CPU node while other three neural network models run on a GPU node. Therefore the comparison between Navie Baye models and neural network models should not be evaluated against the absolute values. Instead, we observe the hierarchical classification introduce approximately 10 times inference computing delays. The inference time taken by Residual CNN is over 20 times than MLP.

Summary. The experiments set up different sizes of training data and test data. The observation shows the residual convolutional neural network model produces the best performance over other classifiers. We also observe that Naive

Bayes model with the one-hot encoding of word tokens performs reasonably well with the limitation of handling increasing feature sizes. A simple two-layer fully connected neural network model has the advantage of fast inference time.

6.4 Threat to Validity

This paper presents the first stage towards automated smart dispatching of residential service requests. The focus of this paper is exploring a combination of word embedding techniques, and machine learning models to improve classification performance. Our hybrid machine learning model follows a simple ensemble approach for selecting the best performing classifier based on metrics of log loss. For our model to be deployed as an online machine learning service handling requests, the model selection mechanism needs to be in the feedback loop based on actual inference results and quality. A weighted score of multiple metrics that best reflect the online service requirements should be further developed to replace the current simple selection based a single metrics (Fig. 13).

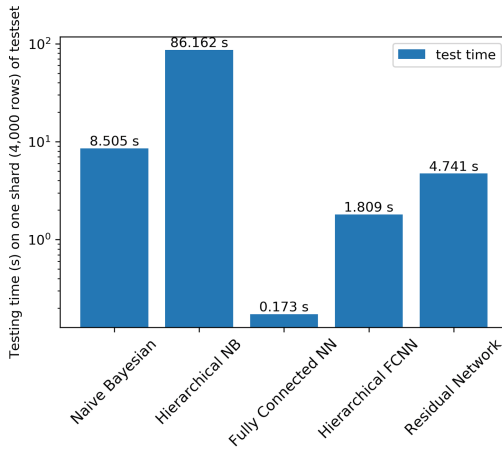


Fig. 13. Inference time on the test data of 4,000 samples

Our evaluation compares with two benchmarking models of Naive Bayes and MLP classifiers. In the literatures, NLP based machine learning methods on news classifications, customer review sentiment analysis, movie review classifications have related work to our method. However, the datasets are specific to the domains without a direct solution to address the problems in our datasets that are not directly labeled for training. Combining our hybrid word embedding and learning models with exiting mining and learning methods become a new stream of investigation that requires a dedicated project to develop that is beyond the current funding budget.

7 Conclusion

In this paper, we present a machine learning based method of natural language classification task for a real-world application. We carry out a rigorous analysis of the dataset and design a feature engineering process that select and extract features with statistical evidence. We apply two-word embedding techniques and develop five classification models. This hybrid machine learning method produces benefits, namely (1) generating suitable labels for supervised learning; (2) clustering data samples into meta-class for training and initializing models to improve classification performance over unbalanced data samples; (3) producing the best performing model through comprehensive experiments and evaluation; and (4) understanding the source of error with the hierarchical classification method. It remains our future work to explore newly published word embedding model to study the effects of word embedding on classification performance.

References

1. Nigam, K., McCallum, A.K., Thrun, S., Mitchell, T.: Text classification from labeled and unlabeled documents using em. *Mach. Learn.* **39**(2–3), 103–134 (2000)
2. Blum, A., Mitchell, T.: Combining labeled and unlabeled data with co-training. In: *Proceedings of the Eleventh Annual Conference on Computational Learning Theory*, pp. 92–100. ACM (1998)
3. Raina, R., Battle, A., Lee, H., Packer, B., Ng, A.Y.: Self-taught learning: transfer learning from unlabeled data. In: *Proceedings of the 24th International Conference on Machine Learning*, pp. 759–766. ACM (2007)
4. Chawla, N.V., Bowyer, K.W., Hall, L.O., Kegelmeyer, W.P.: Smote: synthetic minority over-sampling technique. *J. Artif. Intell. Res.* **16**, 321–357 (2002)
5. Han, H., Wang, W.-Y., Mao, B.-H.: Borderline-SMOTE: a new over-sampling method in imbalanced data sets learning. In: Huang, D.-S., Zhang, X.-P., Huang, G.-B. (eds.) *ICIC 2005*. LNCS, vol. 3644, pp. 878–887. Springer, Heidelberg (2005). https://doi.org/10.1007/11538059_91
6. Breiman, L.: Bagging predictors. *Mach. Learn.* **24**(2), 123–140 (1996)
7. Freund, Y., Schapire, R.E.: A decision-theoretic generalization of on-line learning and an application to boosting. *J. Comput. Syst. Sci.* **55**(1), 119–139 (1997)
8. Fan, W., Stolfo, S.J., Zhang, J., Chan, P.K.: Adacost: misclassification cost-sensitive boosting. *ICML* **99**, 97–105 (1999)
9. Hao, P.Y., Chiang, J.H., Tu, Y.K.: Hierarchically svm classification based on support vector clustering method and its application to document categorization. *Expert Syst. Appl.* **33**(3), 627–635 (2007)
10. Morin, F., Bengio, Y.: Hierarchical probabilistic neural network language model. In: *AISTATS 2005 - Proceedings of the 10th International Workshop on Artificial Intelligence and Statistics* (2005)
11. Cybenko, G.: Approximation by superpositions of a sigmoidal function. *Math. Control, Signals Syst.* **2**(4), 303–314 (1989). <https://doi.org/10.1007/BF02551274>
12. Zhang, X., Zhao, J., LeCun, Y.: Character-level convolutional networks for text classification. In: *Proceedings of the 28th International Conference on Neural Information Processing Systems - Volume 1, NIPS 2015*, pp. 649–657. MIT Press, Cambridge, MA, USA (2015). <http://dl.acm.org/citation.cfm?id=2969239.2969312>

13. Zhang, Y., Wallace, B.C.: A sensitivity analysis of (and practitioners' guide to) convolutional neural networks for sentence classification. CoRR abs/1510.03820 (2015). <http://arxiv.org/abs/1510.03820>
14. Kim, Y.: Convolutional neural networks for sentence classification. arXiv preprint (2014). [arXiv:1408.5882](https://arxiv.org/abs/1408.5882)
15. Conneau, A., Schwenk, H., Barrault, L., Lecun, Y.: Very deep convolutional networks for text classification. arXiv preprint (2016). [arXiv:1606.01781](https://arxiv.org/abs/1606.01781)
16. Prabowo, R., Thelwall, M.: Sentiment analysis: a combined approach. *J. Inform.* **3**(2), 143–157 (2009)
17. Mikolov, T., Chen, K., Corrado, G., Dean, J.: Efficient estimation of word representations in vector space. arXiv preprint (2013). [arXiv:1301.3781](https://arxiv.org/abs/1301.3781)
18. Che, W., Li, Z., Liu, T.: Ltp: a chinese language technology platform. In: Proceedings of the 23rd International Conference on Computational Linguistics: Demonstrations, COLING 2010, pp. 13–16. Association for Computational Linguistics, Stroudsburg, PA, USA (2010). <http://dl.acm.org/citation.cfm?id=1944284.1944288>
19. Harris, Z.S.: Distributional structure. *Word* **10**(2–3), 146–162 (1954)
20. Sparck Jones, K.: A statistical interpretation of term specificity and its application in retrieval. *J. Documentation* **28**(1), 11–21 (1972)
21. Silla, C.N., Freitas, A.A.: A survey of hierarchical classification across different application domains. *Data Min. Knowl. Disc.* **22**(1), 31–72 (2011). <https://doi.org/10.1007/s10618-010-0175-9>
22. Kanungo, T., Mount, D.M., Netanyahu, N.S., Piatko, C.D., Silverman, R., Wu, A.Y.: An efficient k-means clustering algorithm: analysis and implementation. *IEEE Trans. Pattern Anal. Mach. Intell.* **7**, 881–892 (2002)
23. Bilmes, J.A., et al.: A gentle tutorial of the em algorithm and its application to parameter estimation for gaussian mixture and hidden markov models. *Int. Comput. Sci. Inst.* **4**(510), 126 (1998)
24. Figueiredo, M.A.T., Jain, A.K.: Unsupervised learning of finite mixture models. *IEEE Trans. Pattern Anal. Mach. Intell.* **3**, 381–396 (2002)
25. Ankerst, M., Breunig, M.M., Kriegel, H.P., Sander, J.: Optics: ordering points to identify the clustering structure. In: ACM SIGMOD Record, vol. 28, pp. 49–60. ACM (1999)
26. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770–778 (2016). <https://doi.org/10.1109/CVPR.2016.90>
27. He, K., Zhang, X., Ren, S., Sun, J.: Identity mappings in deep residual networks. In: Leibe, B., Matas, J., Sebe, N., Welling, M. (eds.) ECCV 2016. LNCS, vol. 9908, pp. 630–645. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-46493-0_38



Data Driven Faster R-CNN for Transmission Line Object Detection

Xin Zhou¹, Bin Fang¹(✉), Jiye Qian², Gangwen Xie², Bangfei Deng²,
and Jide Qian³

¹ Chongqing University, Chongqing 400030, China
{20171402042t,fb}@cqu.edu.cn

² State Grid Chongqing Electric Power Research Institute, Chongqing 401123, China
qianjiye@cqu.edu.cn

³ Civil Aviation Flight University of China, Sichuan 618307, China

Abstract. Full functional apparatus on high-voltage transmission line, such as insulators, dampers, wires, etc., is the guarantee of stable power supply in urban and rural areas. For this reason, apparatus fault detection on high-voltage transmission line has received a significant attention from research fields of developing inspection robots. Along with fault detection, object detection on high-voltage transmission line is very important, thereby challenging accurate detection of insulators, dampers, wires, etc. at the same time. In this paper, we created a dataset on high-voltage transmission line scene, and detected a group of objects on high-voltage transmission line scene successfully by using base Faster R-CNN. Aiming to improve object detection performance of base Faster R-CNN, we carefully analyzed the Region Proposal Network (RPN) of Faster R-CNN, fine-tuned parameters associated with anchors based on our dataset, and combined PCA Jittering with base Faster R-CNN. Comprehensive experimental results on our dataset showed that each individual work contributed to object detection on high-voltage transmission line scene and improved the object detection performance of base Faster R-CNN. And our approach improved about 47.8% compared to the base Faster R-CNN.

Keywords: Apparatus detection · High-voltage transmission line · Anchors · PCA Jittering · Faster R-CNN

1 Introduction

In the high-voltage transmission system, some objects, such as insulators, dampers, wires and so on, have a great effect on normal power supply. These objects are prone to be damaged in changeably natural environment. E.g., damaged insulators are mostly caused by self-explosion [16]. Once a part of system is damaged, it may cause the high-voltage transmission system to malfunction. To avoid malfunction, a regular inspection tour of high-voltage transmission grid is absolutely critical. Previously, inspecting high-voltage transmission line was

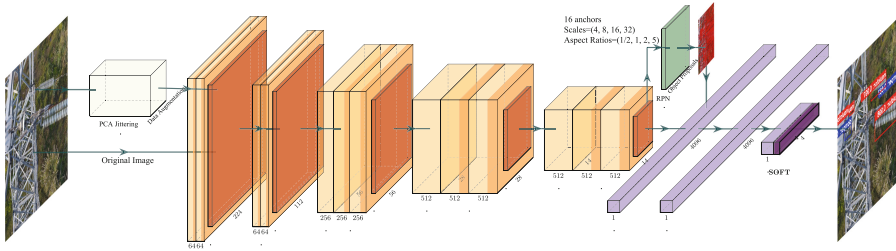


Fig. 1. The network framework of Faster R-CNN combined with PCA Jittering. Original data and the data augmented by PCA Jittering, are feed into convolutional network of Faster R-CNN, then bounding boxes of objects are output by Region Proposal Network (RPN), finally the fully connected layer of Faster R-CNN performs classification of the bounding boxes of objects.

labor-intensive work. But in recent years, robots, especially unmanned air vehicle(UAV) [2], which carry equipments of detection and communication, are in charge of inspecting work.

In the field of computer vision, equipment of detection piggybacked on robots typically includes infrared equipment, camera, etc. And, there have been many research studies on infrared images and general images. These studies included not only different types of object detection on high-voltage transmission line, but also its defect detection, such as [2,4,8,17]. It should be noted that object detection on high-voltage transmission line is extreme prominent in its defect detection. So, most of them make full use of image features for detecting more objects in the power high-voltage transmission system. Threshold method and modified balloon force Snake method were adopted for detecting dampers by Wu et al. [6]. Ebru Karakose et al. [7] located high-voltage transmission line by using morphological processing step and Canny edge extraction. Liao et al. [8] proposed a insulator detection algorithm based on local features and partial orders for aerial images.

Besides, many researchers combined special objects feature with machine learning and deep learning algorithm to detect objects on high-voltage transmission line. The insulators were extracted by using k-means clustering and SVM was applied to classification of the insulators in [11]. Gao et al. [4] took advantage of insulators characteristics extracted from the convolution neural network to detect the location of the insulators. Neural network and SVM methods were joined together by Wu et al. [17], which were exploited to achieve high-voltage transmission line position recognition. A approach to inspect the insulators with Deep Convolutional Neural Networks (CNN) was proposed by Zhao et al. [19], and then classified insulators by SVM. Their approach shown excellent reliability in detecting single-class objects on high-voltage transmission line, but few have focused on simultaneously detecting multiple types of objects on high-voltage transmission line, especially the small-sized insulators, dampers, wires, etc.

It is undeniable that deep learning is a good choice in object recognition work. Generally speaking, object recognition research works on deep learning are divided into two technical routes. One of them is one-stage framework, such as YOLO [12], SSD [10], YOLO9000 [13], etc., which is a regression problem to spatially separate bounding boxes and class probabilities, and other one is two-stage framework, such as Fast R-CNN [5], Faster R-CNN [14], RFCN [1], etc., which is composed of positioning network and classification network. One-stage framework is faster than two-stage framework during training and testing. While compared with one-stage framework, two-stage framework has better accuracy. Considering comprehensively, we focus on Faster R-CNN [14] to ensure object recognition accuracy.

In this paper, we created a dataset which includes 2000 images on high-voltage transmission line, and we analyzed the key point of object detection in baseline Faster R-CNN. Following analyses, we fine-tuned the parameters associated with anchors and combined PCA Jittering with Faster R-CNN [14] for detecting more objects in our dataset. Finally, we evaluated our approach with mAP in our dataset and found that our approach improved about 47.8% compared to the baseline Faster R-CNN. Fine-tuning parameters associated with anchors increased the performance of Faster R-CNN in our dataset by 31.6%. PCA Jittering continue to improved the performance of Faster R-CNN in our dataset by 12.3%.

2 Our Approach

In our work, we created a dataset which includes different types of objects on high-voltage transmission line. And, we found the best hyperparameter settings based on the distribution of our dataset. Besides, we combined PCA Jittering with Faster R-CNN for extending our dataset. Figure 1 shows the framework of Faster R-CNN combined with PCA Jittering. All works are shown as followings.

2.1 Our Dataset

We collected 2000 images containing insulators, dampers, wires, iron pylons, etc. All these images were taken by unmanned air vehicle (UAV). And we labeled insulator, damper, wire with rectangular bounding boxes to generate a dataset.

In our dataset, a total number of 23024 objects are labeled, including 7468 dampers, 6897 insulators, and 8641 wires. Referring to detection metrics of the Microsoft COCO dataset [9], we also categorised different sizes of objects, including small objects (area $< 32 \times 32$), medium objects ($32 \times 32 < \text{area} < 96 \times 96$), and large objects (area $> 96 \times 96$). The numbers of objects corresponding to the three kinds of categories are 6433, 8312, 8279, respectively. Small objects take 28% in our dataset. So, small objects should be focused on during training Faster R-CNN.

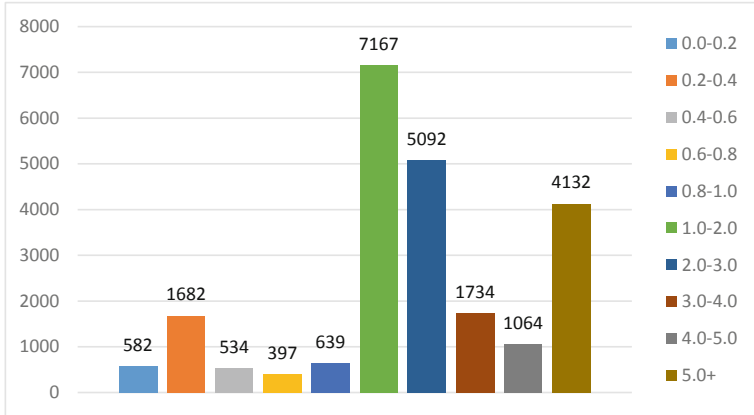


Fig. 2. The aspect ratio distribution of objects in our dataset. Specifically, 31.1% of objects have aspect ratio between 1.0 and 2.0, objects with aspect ratio between 2.0 and 3.0, are 22.1%, and for aspect ratio greater than 5.0 the percentage is 17.9%. Only 16.7% of objects have aspect ratio less than 1.0.

2.2 Anchors in Faster R-CNN

As a representative algorithm of two-stage framework, Faster R-CNN consists of Region Proposal Network (RPN) and Fast R-CNN. The two networks share five convolutional layers in the ZF model [18] and 13 convolutional layers in the VGG model [15]. The Region Proposal Network (RPN) take the conv feature map output by last shared conv layer as input and outputs k rectangular object proposals at each location of feature map output by last shared conv layer [14]. The k rectangular object proposals are generated by translation-invariant anchors. To ensure that region proposals are generated at each location of the feature map, Region Proposal Network (RPN) slips upon feature map output of last shared conv layer.

Each anchor is determined by a scale and aspect. In baseline Faster R-CNN, 9 anchors associated with 3 scales (8, 16, 32) and 3 aspect ratios (1/2, 1, 2) yielded by Region Proposal Network (RPN) at each sliding-window location. But we analyzed our dataset in details and found that the aspect ratios of most objects were concentrated between 1 and 2, or greater than 5. Specifically, 31.1% of objects have aspect ratio between 1.0 and 2.0, objects with aspect ratio between 2.0 and 3.0, are 22.1%, and for aspect ratio greater than 5.0 the percentage is 17.9%. Only 16.7% of objects have aspect ratio less than 1.0. The aspect ratio distribution of objects in our dataset is shown in Fig. 2. So, we fine-tuned the aspect ratios to (1/2, 1, 2, 5). Based on the distribution of object size in the dataset described earlier, we added 4 to scales to train more small-sized objects. That is, 16 anchors associated with 4 scales (4, 8, 16, 32) and 4 aspect ratios (1/2, 1, 2, 5) were used for the Region Proposal Network (RPN).

2.3 PCA Jittering

Compared to the PASCAL VOC [3] and Microsoft COCO datasets [9], our dataset is very small. Taking into account the limited number of images in our dataset, we did data augmentation with PCA Jittering. The algorithm for calculating the principal component of an RGB image $I_{xy} = [I_{xy}^R, I_{xy}^G, I_{xy}^B]^T$ is as following.

Algorithm 1. PCA Jittering

Data: I_R, I_G, I_B : RGB image I ;
 M : 3×3 covariance matrix of RGB image I ;
 $ev = \{ev_0, ev_1, ev_2\}$: the eigenvector of M ;
 $\lambda = \{\lambda_0, \lambda_1, \lambda_2\}$: the eigenvalue of M ;
 α_i : a random variable;
 $Cov(A, B, C)$: calculating covariance matrix of A, B and C;
 $EigVecVal(A)$: calculating eigenvector and eigenvalue of A;
 $GaussRand(a, b)$: calculating the random variable which is drawn from a Gaussian with mean 0 and standard deviation 3;

Result: I_{pca} : RGB image;

```

1  $M = Cov(I_R, I_G, I_B)$ ;
2  $ev, \lambda = EigVecVal(M)$ ;
3 for each  $i \in \{0, 1, 2\}$  do
4   |  $\alpha_i = GaussRand(0, 3)$ ;
5 end
6  $I_{pca} = [ev_0, ev_1, ev_2][\alpha_0\lambda_0, \alpha_1\lambda_1, \alpha_2\lambda_2]^T$ ;
7  $I_{pca} = I_{pca} + I$ ;

```

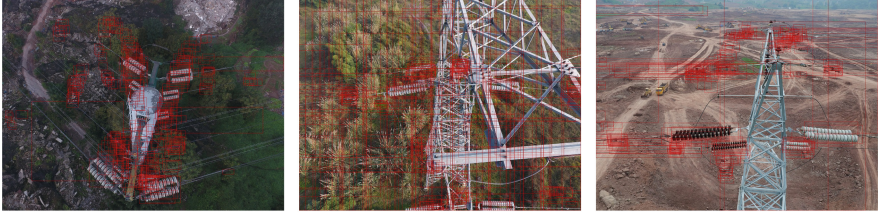
3 Experiment

In our experiments, we chose Faster R-CNN, which is the two-stage framework, to solve the problem of object recognition on high-voltage transmission line. Firstly, we trained and tested our dataset directly using baseline Faster R-CNN, and found that many objects could not be detected. Especially it is hard to detect small-sized objects, such as some dampers. We analyzed the problem why the object could not be detected, followed by fine-tuned the parameters associated with anchors. Additionally, we combined PCA Jittering and retrained Faster R-CNN. It greatly improved the performance of Faster R-CNN in our dataset.

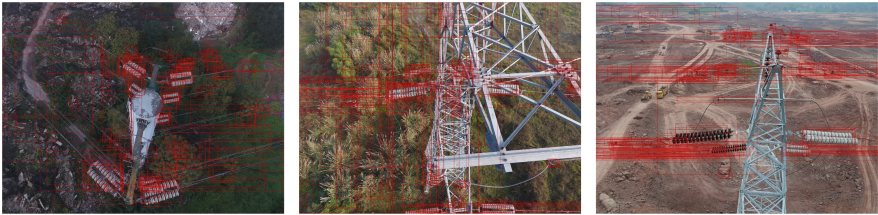
3.1 Dataset and Train Preparation

Dataset. To improve the quality of data annotation, we had a uniform annotation rule. Following that rule, we checked every annotation image, modified the error annotation and adjusted rectangular annotation box whose range is too large or too small.

A total of 2000 images in our dataset, we randomly assigned training set, validation set, and test set in 3:1:1. That is, 1200 images were selected as the training set, 400 images were selected as the validation set, 400 images were selected as test set.



(a) Object detection result of RPN of Faster R-CNN(Baseline)



(b) Object detection result of RPN of Faster R-CNN(Fine-tuning anchors)



(c) Object detection result of RPN of Faster R-CNN(Fine-tuning anchors & PCA Jittering)

Fig. 3. Object detection result of Region Proposal Network (RPN). 300 object boxes were drawn on each image. Most of the bounding boxes of objects covered insulators, dampers and wires.

Training Network Model. We set initial learning rate to 0.001, reducing the learning rate by 10 times for every 5 epochs, and trained 20 epochs in total. For faster convergence, we chose the VGG16 pre-trained model. Besides, we fine-tuned parameters which include scales, aspect ratios. Finally, every object in training set will be learnt 20 times.

3.2 Region Proposals of RPN

Both stages of Faster R-CNN are critical and indispensable for detecting objects. The first stage of Faster R-CNN is Region Proposal Network (RPN), which is used to select all possible object region proposals. All possible object region proposals are sorted by Region Proposal Network (RPN) calculation score, and the first 300 object region proposals are fed into the fully connected layer for classification as positive samples. So, Region Proposal Network (RPN) directly determines whether objects can be detected. The second stage of Faster R-CNN is the classification network of Fast R-CNN composed of fully connected layer, which classifies object region proposals based on feature map of object.

To inspect whether the object is detected by the Region Proposal Network (RPN), we directly drew the 300 object boxes, and found that most of the objects have been detected. We observed that most of the region proposals cover the wires and insulators, while a few region proposals cover the dampers. Object detection result of Region Proposal Network (RPN) of baseline Faster R-CNN are shown in Fig. 3(a).

Because the object aspect ratios are mostly concentrated between 1 and 2, or greater than 5, the neural network can not learn object structure properly. So, we fine-tuned anchors which include scales and aspect ratios, in the Region Proposal Network (RPN) of Faster R-CNN based on the area and aspect ratio distribution of objects in our dataset. Object detection result of Region Proposal Network (RPN) after anchors fine-tuning are shown in Fig. 3(b).

Because the neural network lacks the feature representation of the object, the classification score of most objects is too low. Especially for small-sized objects, such as partial dampers, it is hard to distinguish it from the background. So, we did data augmentation through PCA Jittering which expanded our dataset, provided more object for neural network learning. Object detection result of the Region Proposal Network (RPN) of Faster R-CNN combined with PCA Jittering are shown in Fig. 3(c).

Compared with baseline Faster R-CNN, the region proposals detected by Region Proposal Network (RPN) of Faster R-CNN combined with PCA Jittering is more concentrated around objects.

Table 1. Experimental results of object detection on high-voltage transmission line

	Damper	Insulator	Wire	Mean
FRCNN(B) ^a	0.2261	0.4297	0.4110	0.3556
FRCNN(FA) ^b	0.2847	0.5908	0.5285	0.4680
FRCNN(FA+PCA) ^c	0.3626	0.6184	0.5955	0.5255

^a Baseline Faster R-CNN.

^b Faster R-CNN & Fine-tuning anchors.

^c Faster R-CNN & Fine-tuning anchors & PCA Jittering

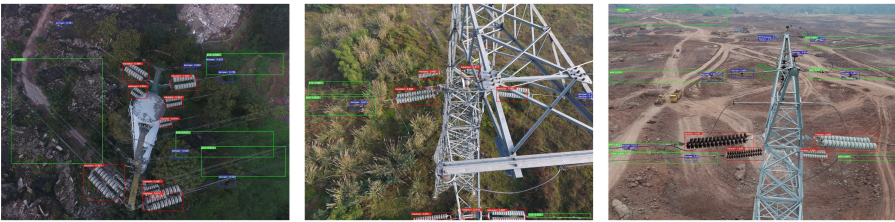
3.3 Detection and Classification Results

Evaluation in Our Dataset. To show the significance of setting reasonable parameters associated with anchors and the effectiveness of Faster R-CNN combined with PCA Jittering in our dataset, we compared them with the baseline Faster R-CNN. We evaluated the detection mAP on the same test dataset and draw the following conclusions.

Baseline Faster R-CNN has an mAP of 0.3556. The detection mAP can be raised to 0.4680, if we only fine-tune the parameters associated with anchors. After fine-tuning the parameters associated with anchors, Faster R-CNN combined with PCA Jittering has an mAP of 0.5255. That is, for our dataset, fine-tuning the parameters associated with anchors can increase the performance of Faster R-CNN by 31.6%, and PCA Jittering can keep improving the performance



(a) Object detection result of Faster R-CNN(Baseline)



(b) Object detection result of Faster R-CNN(Fine-tuning anchors)



(c) Object detection result of Faster R-CNN(Fine-tuning anchors & PCA Jittering)

Fig. 4. Object detection result of Faster R-CNN. Insulators: red rectangular object proposals. Wires: green rectangular object proposals. Dampers: blue rectangular object proposals. (Color figure online)

of Faster R-CNN by 12.3%. The detection mAP of dampers, insulators, wires and the mean mAP of all objects are shown in Table 1.

As can be seen from Table 1, the parameters associated with anchors have the greatest impact on insulator. The detection mAP of insulator is 0.4297, 0.5908, 0.6184 in FRCNN(B), FRCNN(FA), and FRCNN(FA+PCA), respectively. The detection mAP of insulator increased by 37.49% by fine-tuning the parameters associated with anchors. And, through fine-tuning the parameters associated with anchors and data augmentation with PCA Jittering, the mAP of damper increased by 60.4% compared to baseline Faster R-CNN.

Object Detection Results. To show the improvement of object detection performance more clearly, we illustrate the detection results of some images in Fig. 4.

In 4(a), because of the limitations of parameters associated with anchors, most of insulators are not detected by baseline Faster R-CNN. In 4(b), basically all the insulators are detected after fine-tuning parameters associated with anchors. Experimental results prove that the detection performance of the insulators are improved by fine-tuning parameters associated with anchors. In 4(c), some undetected dampers are detected, but some insulators are misdetected. So, we will continue to optimize Faster R-CNN in our dataset in future work.

4 Conclusions

In this paper, we created a dataset for objects detecting which includes dampers, insulators, and wires on high-voltage transmission line. We trained and tested this dataset using baseline Faster R-CNN, and analyzed why small-sized objects could not be detected. To detect more objects on high-voltage transmission line, we carefully analyzed the Region Proposal Network (RPN) of Faster R-CNN, fine-tuned parameter associated with anchors based on our dataset, and combined PCA Jittering. Each work improved the performance of object detection on high-voltage transmission line. The experimental results showed that fine-tuned parameters associated with anchors is beneficial for insulator detection, and PCA Jittering is beneficial for small-sized object detection. Compared with baseline Faster R-CNN, our approach improved the mAP of damper by 60.4%, the mAP of insulator by 43.9%, the mAP of wire by 44.9%, respectively.

Acknowledgment. This research has been supported by the National Natural Science Foundation of China (No. 61876026, No. 61906022), Chongqing Special Key Project of Technology Innovation and Application Development (No. cstc2019jscx-mbdx0113), the Special Foundation for Chongqing Postdoctoral Research (No. Xm2016060).

References

1. Dai, J., Li, Y., He, K., Sun, J.: R-fcn: Object detection via region-based fully convolutional networks. In: *Advances in Neural Information Processing Systems*, pp. 379–387 (2016)
2. Dong, G., et al.: Inspecting transmission lines with an unmanned fixed-wings aircraft. In: *2012 2nd International Conference on Applied Robotics for the Power Industry (CARPI)*, pp. 173–174. IEEE (2012)
3. Everingham, M., Van Gool, L., Williams, C.K., Winn, J., Zisserman, A.: The pascal visual object classes (voc) challenge. *Int. J. Comput. Vis.* **88**(2), 303–338 (2010)
4. Gao, F., et al.: Recognition of insulator explosion based on deep learning. In: *2017 14th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 79–82. IEEE (2017)
5. Girshick, R.: Fast r-CNN. In: *Proceedings of the IEEE International Conference on Computer Vision*, pp. 1440–1448 (2015)
6. Haibin, W., Yanping, X., Weimin, F., Xiaoming, S., Li, J.: Damper detection in helicopter inspection of power transmission line. In: *2014 Fourth International Conference on Instrumentation and Measurement, Computer, Communication and Control*, pp. 628–632. IEEE (2014)
7. Karakose, E.: Performance evaluation of electrical transmission line detection and tracking algorithms based on image processing using UAV. In: *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, pp. 1–5. IEEE (2017)
8. Liao, S., An, J.: A robust insulator detection algorithm based on local features and spatial orders for aerial images. *IEEE Geosci. Remote Sens. Lett.* **12**(5), 963–967 (2014)
9. Lin, T.-Y., et al.: Microsoft COCO: common objects in context. In: Fleet, D., Pajdla, T., Schiele, B., Tuytelaars, T. (eds.) *ECCV 2014*. LNCS, vol. 8693, pp. 740–755. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10602-1_48
10. Liu, W., et al.: SSD: single shot multibox detector. In: Leibe, B., Matas, J., Sebe, N., Welling, M. (eds.) *ECCV 2016*. LNCS, vol. 9905, pp. 21–37. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-46448-0_2
11. Prasad, P.S., Rao, B.P.: Lbp-hf features and machine learning applied for automated monitoring of insulators for overhead power distribution lines. In: *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 808–812. IEEE (2016)
12. Redmon, J., Divvala, S., Girshick, R., Farhadi, A.: You only look once: Unified, real-time object detection. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 779–788 (2016)
13. Redmon, J., Farhadi, A.: Yolo9000: better, faster, stronger. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 7263–7271 (2017)
14. Ren, S., He, K., Girshick, R., Sun, J.: Faster r-CNN: towards real-time object detection with region proposal networks. In: *Advances in Neural Information Processing Systems*, pp. 91–99 (2015)
15. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. *arXiv preprint* (2014). [arXiv:1409.1556](https://arxiv.org/abs/1409.1556)
16. Wang, W., Wang, Y., Han, J., Liu, Y.: Recognition and drop-off detection of insulator based on aerial image. In: *2016 9th International Symposium on Computational Intelligence and Design (ISCID)*, vol. 1, pp. 162–167. IEEE (2016)

17. Wu, Y., Luo, Y., Zhao, G., Hu, J., Gao, F., Wang, S.: A novel line position recognition method in transmission line patrolling with uav using machine learning algorithms. In: 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), pp. 491–495. IEEE (2018)
18. Zeiler, M.D., Fergus, R.: Visualizing and understanding convolutional networks. In: Fleet, D., Pajdla, T., Schiele, B., Tuytelaars, T. (eds.) ECCV 2014. LNCS, vol. 8689, pp. 818–833. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10590-1_53
19. Zhao, Z., Xu, G., Qi, Y., Liu, N., Zhang, T.: Multi-patch deep features for power line insulator status classification from aerial images. In: 2016 International Joint Conference on Neural Networks (IJCNN), pp. 3187–3194. IEEE (2016)



A Deep Learning-Based Hybrid Data Fusion Method for Object Recognition

Weishan Zhang^{1,2(✉)}, Zongchao Zheng¹, Yuanjie Zhang², Liang Xu³,
and Jiehan Zhou⁴

¹ China University of Petroleum, Qingdao, China
zhangws@upc.edu.cn

² West Coast Artificial Intelligence Institute, Qingdao, China

³ Beijing University of Science and Technology, Beijing, China

⁴ Oulu University, Oulu, Finland

Abstract. Multi-source heterogeneous data are playing increasingly important roles. It becomes important to harness multi-source heterogeneous data for effectively managing and mining data intelligence. This paper presents a hybrid data fusion model called FD-DFM (Feature and Decision-Data Fusion Model) based on deep learning. The FD-DFM integrates feature fusion and decision fusion into neural networks with the D-S evidence theory. The experiment shows that the FD-DFM model has higher accuracy than other existing methods with fruit recognition.

Keywords: Deep learning · Feature fusion · Object recognition · Data fusion

1 Introduction

With the rapid development of internet of things, multi-source, large volume and heterogeneity data are collected in a very fast manner. Multi-source means data come from multiple physical or virtual sources, such as mobile phones, various sensors, etc. Heterogeneity refers to different structure of data, such as text data, image data, etc. How to manage multi-source heterogeneous data for efficient usage is very important [1]. Data fusion is a data processing technology that integrates and analyzes multi-source heterogeneous data according to specific application scenarios and purposes, which aims to fully exploit all potentials of data [2].

JDL (Joint Directors of Laboratories) is an existing conceptual data fusion system [3]. The original JDL model consists of four incremental abstraction layers of objects, situations, influences, and refinement. The JDL model has limitations in flexibility and scalability [4]. Kokar et al. [5] proposed a relatively new abstract fusion framework based on classification theory. The framework covers all types of fusion, including data, feature, decision, and relational information fusions. It's the first formal theory for data fusion. However, the framework is a conceptual model and needs to be exemplified.

Deep learning is an important breakthrough in the field of artificial intelligence, especially for object recognition in images. There are many available models such as VGGNet [6], ResNet [7], etc. Chen et al. [8] proposed a bearing fault detection method based on deep learning and multi-sensor feature fusion. They used SAE (Sparse

Autoencoder) to fuse the data features from different sensors and then trained Deep Belief Network with the fused features. This work is mainly used for fusing the accelerator features and not for object recognition. Chen et al. [9] proposed a crack detection approach named NB-CNN by using CNN (Convolutional Neural Network) and Bayesian data fusion. Firstly, the CNN identifies the cracks in multiple frames, and then the Bayes makes a decision. Ghamisi et al. [10] proposed a spectral data fusion method that uses EPS(Extinction Profiles) and CNN to classify radar and hyper-spectral data. This method mainly deals with the radar and hyper-spectral images. It is limited and difficult to cope with feature superposition for object recognition in other scenes. Jing et al. [11] proposed an adaptive multi-sensor fusion method based on deep learning for gear fault diagnosis. They integrated data, feature and decision fusion into a DCNN (Deep Convolutional Neural Networks) model, which improves the gear fault detection accuracy. In general, the combination of data fusion and deep learning is most applied in the field of fault detection. At present, there is no deep learning-based data fusion method for object recognition.

This paper presents a deep learning-based data fusion model for object recognition, called Feature and Decision-Data Fusion Model (FD-DFM). The FD-DFM integrates feature and decision fusion into neural networks with the D-S evidence theory and improves the recognition accuracy.

The remainder of the paper is organized as follows. Section 2 introduces the hybrid fusion method based on deep learning-FD-DFM. Section 3 presents the application and evaluation of the method with fruit recognition. Section 4 presents the related work. Section 5 presents conclusions and future work.

2 Design of the FD-DFModel

The FD-DFM is a hybrid and deep learning-based approach. It integrates data, feature and decision fusion for improving recognition accuracy in some specific scenes with multi-source data. The model enables to train heterogeneous data such as descriptive data and feature vectors simultaneously. The FD-DFM trains the input data and obtains the fusion results first. To the end, The FD-DFM constructs and manages three data fusions at different levels.

Data for object recognition include not only images, such as optical and infrared images but also descriptive data such as weight and volume. The FD-DFM applies deep learning for image data into extracting multi-layer features of the target, and different networks into further enriching these features, that makes the FD-DFM becomes a multi-feature fusion model. The FD-DFM deals with descriptive data and extract features prior knowledge base, and makes preliminary judgment to obtain the results respectively. The FD-DFM fuses both results using the decision algorithm and obtains the decision fusion model. Next, we introduce the FD-DFM model in detail for multi-source data fusions.

2.1 Overall FD-DFM Structure

The FD-DFM model consists of data, feature, and decision fusions. The feature fusion generally includes state data and feature data fusion. Target states data usually contains descriptive data such as weight and volume. They are extracted by the corresponding

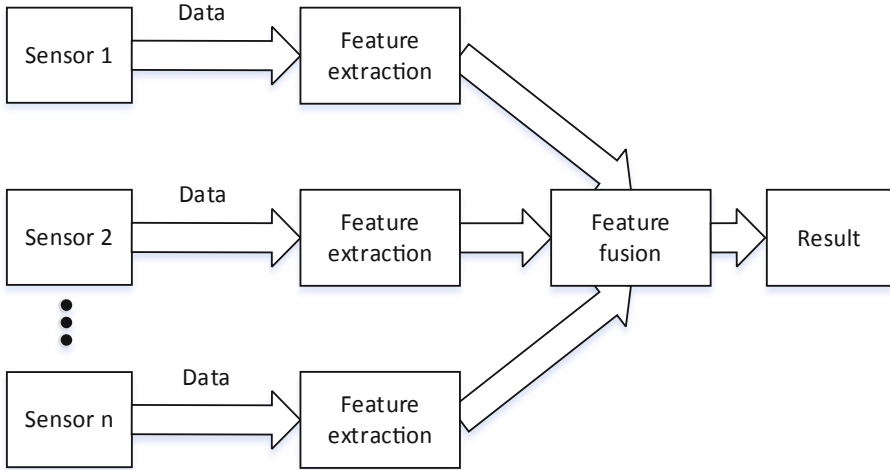


Fig. 1. The feature fusion structure

feature extraction algorithm. After the feature extraction, the data are fused by the feature fusion algorithm to obtain final results. In our work, image features are extracted by the CNN, and the extracted features are fused by an artificial neural network to obtain final results. Figure 1 presents the feature fusion process.

Decision fusion extracts and identifies data features using a decision fusion algorithm. Figure 2 presents the decision fusion structure. Decision fusion extracts image features by CNNs and obtains recognition results. It builds a priori knowledge base using description data such as weight and volume and recognizes objects through decision fusion algorithms, such as the D-S evidence theory, Bayesian estimation, and fuzzy logic reasoning. The decision fusion obtains preliminary results for each object and then get final result through fusion algorithms. That is different from the feature fusion.

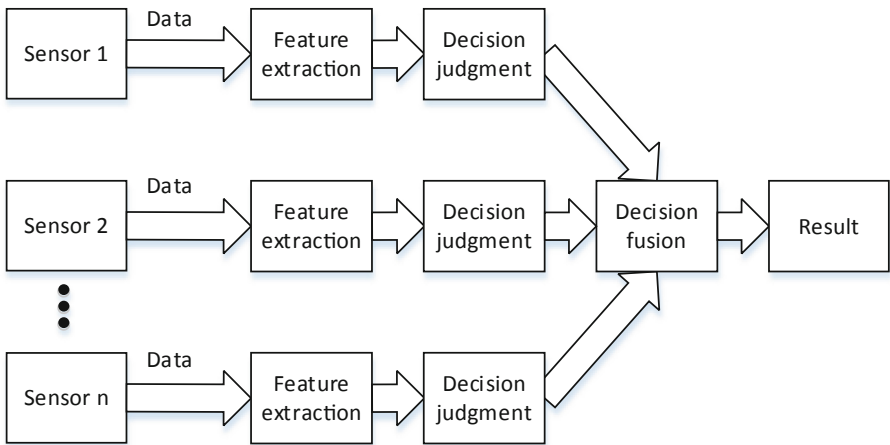


Fig. 2. The decision fusion structure

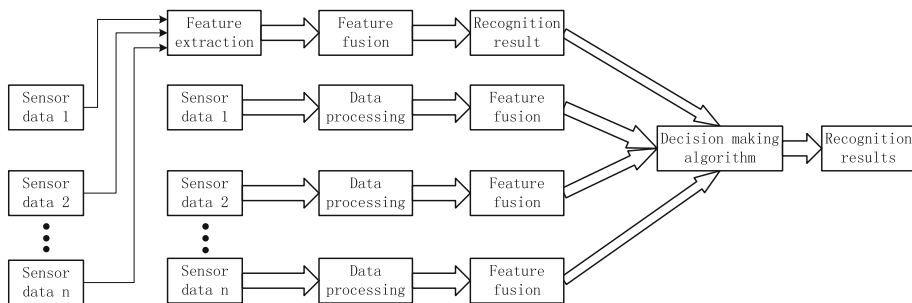


Fig. 3. The hybrid fusion structure

The DF-FDM combines feature fusion and decision fusion for improving the fusion performance. After feature level fusion, it fuses the results of individual decision judgment, which improves the robustness and flexibility of data fusion (Fig. 3).

2.2 Feature Fusion

Feature fusion fuses the image features and classifies objects using CNN models as shown in Fig. 4. An image is input into the CNN, and the obtained feature vectors are input into a neural network. And finally, it outputs recognition result. The neuron numbers in the input, hidden and output layer in neural network depend on the target number in dataset.

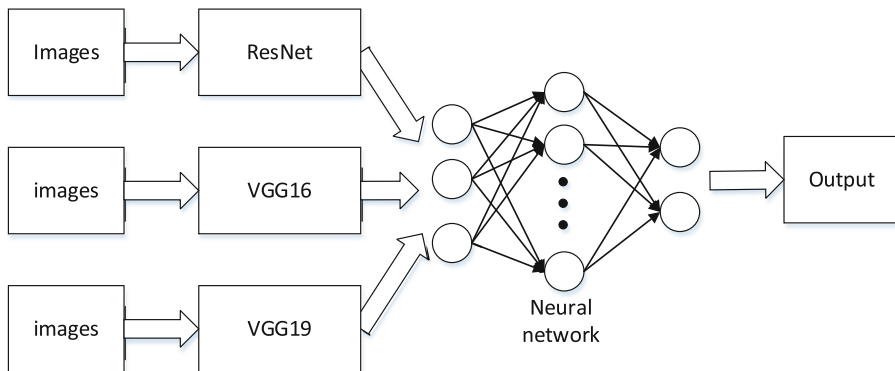


Fig. 4. The feature fusion model

We adopt BP Neural Network for the feature fusion model. A BP Neural Network consists of two parts. One is forward transmission and the other is reverse transmission. The forward transmission processes information layer by layer from the input to the

hidden layer and to the output layer. There is no cross-layer influence between layers. If the output of the output layer is far different from the expected value, it will carry out reverse transmission to feed back the error signal along the original route, and then gradually improve the weight of each layer of neurons, and finally minimize the error signal.

The BP network contains only one hidden layer with a nodes, and b nodes in the Input layer and c nodes in the output layer. We adopt the linear function as the transfer function between the output and hidden layer. A neuron state is set as X_i and its output as Y_i , and their relationship is as function (1).

$$Y_i = f(X_i) = X_i \quad (1)$$

Set $D_1, D_2 \dots, D_c$ as the input, and the corresponding output is as Eq. (2).

$$E_i = D_i, i = 1, 2, \dots, c \quad (2)$$

The input of node j for the hidden layer is as Eq. (3),

$$F_j = L_{j1} \cdot E_1 + L_{j2} \cdot E_2 + \dots + L_{jc} \cdot E_c + M_j \quad (3)$$

The output of node j for the hidden layer is as Eq. (4),

$$H_j = f(x_j), j = 1, 2, 3, \dots, a \quad (4)$$

The input of node j for the output layer is as Eq. (5),

$$k = \sum_{j=1}^a L_{1j}^2 H_j + M^2 \quad (5)$$

The output of node j for the output layer is as Eq. (6),

$$Y = f(k) = k \quad (6)$$

L_{ji}, L_{1j}^2 are the connection weights, M_j, M^2 are the offsets of constant parameters.

2.3 Decision Fusion

Figure 5 presents the decision fusion model. The input includes image, weight and volume data. The model trains CNNs for image data to obtain object recognition decisions, and uses prior knowledge base for weight and volume data for object judgements. The model fuses recognition and judgement results and obtain final recognition results.

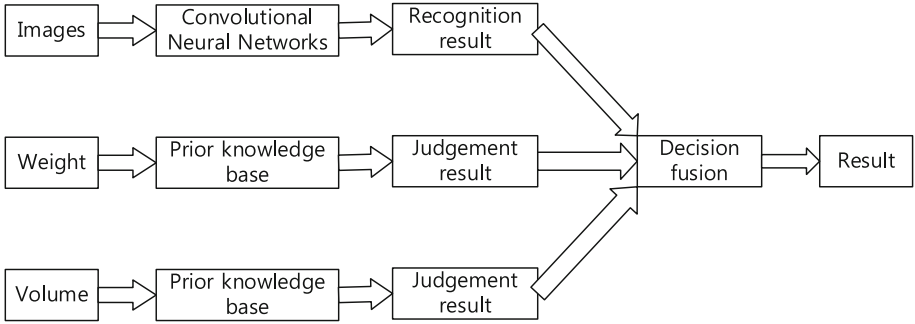


Fig. 5. The model of decision fusion

The decision fusion model applies the D-S evidence theory for the fusion algorithm. The measurement method of D-S evidence theory is trust function, which is obtained by constraining target probability so that it has a good capability to deal with ambiguous information. When the D-S evidence theory is used for target recognition, the allocation of basic credibility is difficult, which can be alleviated by the usage of a neural network. Through the training of the neural network, the basic credibility of each recognition target is allocated, and then D-S evidence theory is to obtain the fusion results.

Let V be the identification framework, function $m : 2^V \rightarrow [0, 1]$ meets the following conditions,

$$m(\phi) = 0, \sum_{A \subset V} m(A) = 1 \tag{7}$$

The basic probability of an impossible event is 0, m is the probability distribution function, and $m(A)$ is called the basic probability number of proposition A , which represents the accuracy trust of A . However, the total trust degree of A cannot be expressed by $m(A)$, we need to compute the sum of the basic probabilities for all subsets of A , we define the function $BEL : 2^V \rightarrow [0, 1]$

$$BEL(A) = \sum_{B \subset A} m(B) (\forall A \subset V) \tag{8}$$

We call function (8) as lower bound function, indicating the total trust of A , therefore you get $BEL(\phi) = 0, BEL(V) = 1$.

We define the likelihood function $PI : 2^V \rightarrow [0, 1]$ as

$$PI(A) = 1 - BEL(\bar{A}) = \sum_{B \cap A \neq \phi} m(B) \tag{9}$$

PI is called the likelihood function, also known as the upper bound function. \bar{A} confidence level is used to measure the information that A cannot represent. The likelihood function represents the confidence level that A is not false.

The combination rule of evidence theory is a method of combining multiple evidences. For the combination of the two evidence, assuming m_1 and m_2 as the two

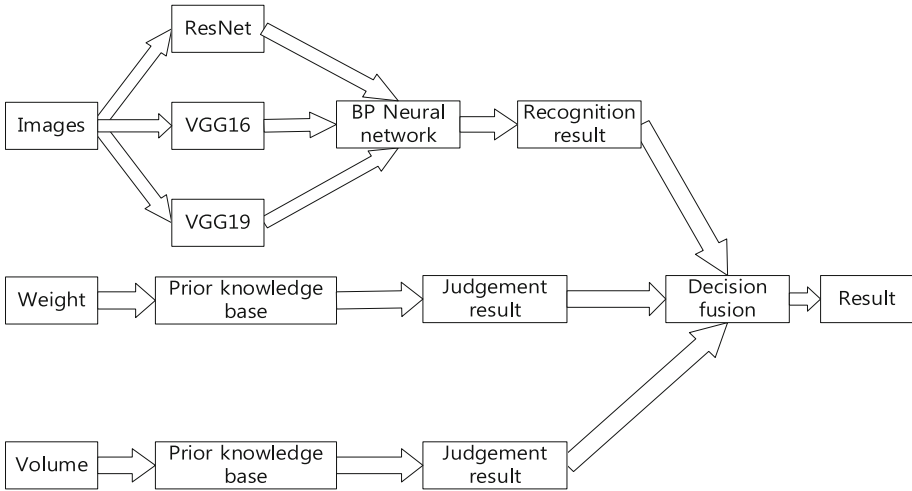


Fig. 6. The Feature and Decision-Data Fusion Model

independent basic probability on 2^V , then the combination of basic probability is $m = m_1 \oplus m_2$.

Let BEL_1 and BEL_2 be two trust functions, with m_1 and m_2 as their basic probabilities, and the focal elements A_1, \dots, A_k and B_1, \dots, B_r , Suppose

$$K_1 = \sum_{A_i \cap B_j \neq \phi} m_1(A_i)m_2(B_j) < 1 \tag{10}$$

So

$$m(C) = \begin{cases} \frac{\sum_{A_i \cap B_j = C} m_1(A_i)m_2(B_j)}{1 - K_1}, & \forall C \subset U \text{ 且 } C \neq \emptyset \\ 0, & C = \emptyset \end{cases} \tag{11}$$

In formula (10), if $K_1 \neq 1$, the basic probability distribution is determined by m ; If $K_1 = 1$, m_1 and m_2 cannot be combined. For the combination with more than two evidences, m_1, \dots, m_n represent the reliability distribution of n pieces of information. If they are independent, the reliability of the fused function $m = m_1 \oplus m_2 \oplus \dots \oplus m_n$ can be expressed as

$$m(A) = \frac{\sum \bigcap_{A_i=A} \prod_{i=1}^n m_i(A_i)}{1 - \sum \bigcap_{A_i=\phi} \prod_{i=1}^n m_i(A_i)} \tag{12}$$

2.4 Hybrid Fusion

The FD-DFM model combines feature fusion and decision fusion, taking into account the interconnection and feedback among different data levels. The feature fusion is used for image data to obtain fusion results. The prior knowledge base respectively is used

for multiple descriptive data to make classification judgment. Then, these results are fused by using the decision fusion algorithm into obtaining the final recognition results. Figure 6 presents the hybrid fusion model - FD-DFM.

3 Evaluation

3.1 Fruit Recognition

There are a number of approaches for object recognition, e.g., R-CNN [12], SPPNET [13], Fast R-CNN [14], Faster R-CNN [15], YOLO [16] and SSD [17]. We choose three SSD models for fruit recognition because of its high recognition efficiency.

We use the SSD for training, the images are input into the VGG16, VGG19, and ResNet models simultaneously. The three output vectors are jointed as the input of BP neural network, and finally the recognition result is obtained. The BP neural network consists of 30 neurons in the input layer, 20 neurons in the hidden layer, and 10 neurons in the output layer.

Combining the output of feature level fusion with the prior knowledge base, the FD-DFM applies the decision fusion algorithm for the final recognition, as shown in Fig. 7.

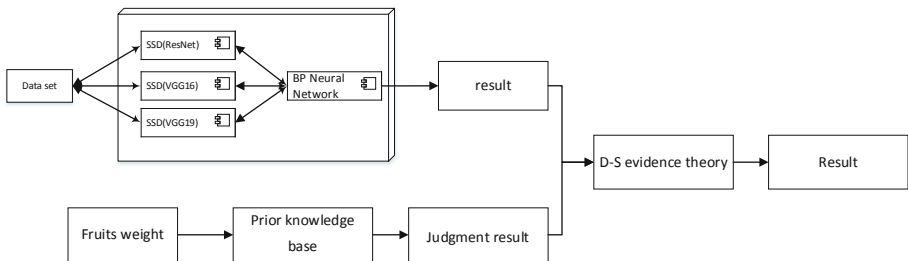


Fig. 7. The application of FD-DF Model for fruit recognition

The BP neural network is used to allocate the credibility of image data. The prior knowledge base is used to allocate the credibility of weight data. The knowledge base consists of fruit name, weight, and a list of similar fruits. By comparing the fruit weight, the fruit credibility within the certain weight range is evenly distributed. If the weight is only within the weight range of a certain fruit, then it belongs to that fruit with a credibility of 1, belongs to other categories with a credibility of 0.

3.2 Experiment

We evaluate the FD-DFM model and compare it with other 5 methods.

3.2.1 Test Bed Configuration

All experiments are conducted with the following software and hardware configuration (Table 1). The cluster consists of four 1070 GPUs with Jdk1.8, OpenCV2.4.9,

Hadoop2.6.4, HBase1.2.1, and Caffe. Jdk1.8, OpenCV2.4.9, and Caffe are installed in INVIDA TX1.

Table 1. Experimental configurations

Machine mode	Hardware configuration	Software configuration	Machine number
1070	NVIDIA 1070 i7 6700 k 16G, 500G SSD	JDK1.8, OpenCV2.4.9, Caffe, Hadoop2.6.4 + HBase1.2.1	4

3.2.2 The Dataset

The dataset consists of 60000 images. 48,000 images are used for training and 12,000 for testing. The light factor and the camera angle influence are considered in collecting this dataset. This dataset contains small amounts of unregistered fruits and vegetables such as canned and boxed goods for distraction. The light is controlled with both dark and bright setting when shooting images. Four different shooting angles are taken in each corner of refrigerator, and four data sets were produced from each angle. we choose 12,000 pictures for training and 3,000 pictures for testing from the four datasets. Figure 8 presents example images.



Fig. 8. Example: images

3.2.3 Experimental Analysis

The experiment uses ten kinds of fruits., The target recognition framework $V = \{O_1, O_2, O_3, O_4, O_5, O_6, O_7, O_8, O_9, O_{10}\}$, O_1 stands for watermelon, O_2 stands for pitaya, O_3 stands for apple, O_4 stands for yellow apple, O_5 stands for pear, O_6 stands for walnut, O_7 stands for mango, O_8 stands for lemon, O_9 stands for orange, O_{10} stands for tangerine. The experiment uses camera (CA) and weight sensor (WE) as sensors.

CA uses BP neural network to assign basic credibility. We assign the basic credibility by using average distribution, as shown in Table 2.

Table 2. The basic probability assignment for CA and WE

Sensor	Probability assignment										
	O_1	O_2	O_3	O_4	O_5	O_6	O_7	O_8	O_9	O_{10}	U
$m_{CA}(\cdot)$	0.00	0.00	0.00	0.02	0.01	0.00	0.05	0.03	0.70	0.13	0.06
$m_{WE}(\cdot)$	0.00	0.00	0.25	0.25	0.00	0.00	0.00	0.00	0.25	0.00	0.25

Then, according to Dempster’s rule of combination, we combine $m_{CA}(\cdot)$ and $m_{WE}(\cdot)$ to obtain the probability assignment for CA and WE as shown in Table 3.

Table 3. $m_{CA}(\cdot)$ and $m_{WE}(\cdot)$

$m_{WE}(\cdot)$	$m_{CA}(\cdot)$											
	$O_1(0.00)$	$O_2(0.00)$	$O_3(0.00)$	$O_4(0.02)$	$O_5(0.01)$	$O_6(0.00)$	$O_7(0.05)$	$O_8(0.03)$	$O_9(0.70)$	$O_{10}(0.13)$	U(0.06)	
$O_1(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_1(0.00)$
$O_2(0.00)$	$\emptyset(0.00)$	$O_2(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_2(0.00)$
$O_3(0.25)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_3(0.00)$	$\emptyset(0.005)$	$\emptyset(0.003)$	$\emptyset(0.00)$	$\emptyset(0.013)$	$\emptyset(0.008)$	$\emptyset(0.175)$	$\emptyset(0.033)$	$\emptyset(0.033)$	$O_3(0.015)$
$O_4(0.25)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_4(0.005)$	$\emptyset(0.003)$	$\emptyset(0.00)$	$\emptyset(0.013)$	$\emptyset(0.008)$	$\emptyset(0.175)$	$\emptyset(0.033)$	$\emptyset(0.033)$	$O_4(0.015)$
$O_5(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_5(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_5(0.00)$
$O_6(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_6(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_6(0.00)$
$O_7(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_7(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_7(0.00)$
$O_8(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_8(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_8(0.00)$
$O_9(0.25)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.005)$	$\emptyset(0.003)$	$\emptyset(0.00)$	$\emptyset(0.013)$	$\emptyset(0.008)$	$O_9(0.175)$	$\emptyset(0.033)$	$\emptyset(0.033)$	$O_9(0.015)$
$O_{10}(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$\emptyset(0.00)$	$O_{10}(0.00)$
U(0.25)	$O_1(0.00)$	$O_2(0.00)$	$O_3(0.00)$	$O_4(0.005)$	$O_5(0.003)$	$O_6(0.00)$	$O_7(0.013)$	$O_8(0.008)$	$O_9(0.175)$	$O_{10}(0.033)$	$\emptyset(0.033)$	U(0.015)

ϕ stands for empty set, and we can get K that measures the inconsistency between $m_{CA}(\cdot)$ and $m_{WE}(\cdot)$.

$$K = 0.005 + 0.003 + 0.013 + 0.008 + 0.175 + 0.033 + 0.003 + 0.013 + 0.008 + 0.175 + 0.033 + 0.005 + 0.003 + 0.013 + 0.008 + 0.033 = 0.531,$$

Then

$$\begin{aligned} m_{CA*WE}(O_1) &= 0, m_{CA*WE}(O_2) = 0, m_{CA*WE}(O_3) = 0.032, \\ m_{CA*WE}(O_4) &= 0.053, m_{CA*WE}(O_5) = 0, m_{CA*WE}(O_6) = 0, \\ m_{CA*WE}(O_7) &= 0, m_{CA*WE}(O_8) = 0, m_{CA*WE}(O_9) = 0.778, \\ m_{CA*WE}(O_{10}) &= 0, m_{CA*WE}(U) = 0.032 \end{aligned}$$

Table compared the FD-DFM fusion results with the feature fusion results. By the FD-DFM fusion, the basic probability for uncertainty is reduced to 0.032. The final decision result is orange, which is 7.8% points more accurate than the feature fusion. The FD-DFM reduced the probability of an orange being recognized as an tangerine to 0 (Table 4).

Table 4. Comparison between the FD-DFM and feature fusion

	O_1	O_2	O_3	O_4	O_5	O_6	O_7	O_8	O_9	O_{10}	U
$m_{CA}(\cdot)$	0.00	0.00	0.00	0.02	0.01	0.00	0.05	0.03	0.70	0.13	0.06
$m_{CA*WE}(\cdot)$	0.00	0.00	0.032	0.053	0.00	0.00	0.00	0.00	0.778	0.00	0.032

3.2.4 Accuracy Contrast

We test the ResNet, VGG16 and VGG19 models respectively, and then test the fusion model. We compare their recognition rate with weight data fusion. Table 5 presents the comparison results.

Table 5. Recognition rate with different models

The network structure	Accuracy
SSD(ResNet)	0.91
SSD(VGG16)	0.89
SSD(VGG19)	0.90
Feature fusion	0.92
FD-DFM fusion	0.97

Table 6 presents the recognition rate with different methods for different types of fruits. The rate by data fusion is higher than that by feature fusion, where the confusion probability is very high for fruits of orange, tangerine, pear and yellow apple. However, the probability of error recognition by data fusion decreases, especially for the fruit recognition of orange, tangerine, pear and yellow apple.

Table 6. Recognition rate and confusion matrix with different fusion models

Fruits/vegetables	Feature fusion		FD-DFM fusion	
	Recognition rate	High confusion type/probability	Recognition rate	High confusion type/probability
watermelon	93.0	cucumber 1.1	98.9	cucumber 0.1
pitaya	90.8	apple 0.9	97.8	apple 0.3
apple	92.0	pitaya 0.8	97.1	pitaya 0.4
yellow apple	90.3	pear 9.0	97.1	pear 0.9
pear	89.4	yellow apple 7.0	95.8	yellow apple 0.8
kiwifruit	90.6	potatoes 6.9	96.5	potatoes 1.1
mango	91.2	lemon 0.8	96.0	lemon 0.4
lemon	92.5	pear 1.0	97.6	pear 0.4
orange	87.8	tangerine 13.1	96.4	tangerine 1.0
tangerine	88.1	orange 14.1	96.1	orange 1.2
yam	91.3	potatoes 0.4	95.9	potatoes 0.1
towel gourd	92.1	watermelon 0.8	98.1	green peppers 0.1
cabbage	91.7	wax gourd slices 0.3	97.6	wax gourd slices 0.1
rapeseed	91.2	cucumber 0.4	97.8	cucumber 0.2
eggplant	92.5	cucumber 0.2	96.6	cucumber 0.1
carrot	88.5	tangerine 3.2	97.7	tangerine 0.5
corn	90.3	pear 0.9	96.4	pear 0.2
tomatoes	91.6	pitaya 1.2	97.2	pitaya 0.4
potatoes	90.2	Kiwifruit 7.3	96.1	Kiwifruit 0.9
broccoli	91.4	towel gourd 0.6	96.9	towel gourd 0.3
green peppers	92.3	watermelon 0.9	97.3	towel gourd 0.1
purple cabbage	91.9	eggplant 0.8	96.7	eggplant 0.3

4 Related Work

Kokar [5] et al. proposed data, feature, and decision fusion, and relational information fusion. This work provides a reference for the data fusion standardization. Goodman et al. [18] proposed the fusion concept from the point of view of mathematical logic, which combines the uncertainty of decision-making.

Steinberg et al. proposed the JDL model [3], which integrates objects, situations, influences, and processes on four abstraction layers in an incremental manner. It was not an extensible approach. James et al. [XX] proposed an improved JDL approach that supports distributed fusion to improve the fusion extensibility. But there are too many parameters to be adjusted.

Dasarathy et al. [19] proposed a decision fusion method, which regards the fusion from the perspective of software engineering. It was a data flow characterized by input and output, and has strict requirements on data sources and processing. This method cannot fully extract the characteristics of heterogeneous data in the decision fusion.

Smirnov et al. [20] proposed five classic data fusions, namely simple fusion, select fusion, expand fusion, absorb fusion and parallel fusion, starting from the fusion environment and purpose. However, this method is mainly for knowledge and information fusion and cannot be used to solve problems related to deep learning.

5 Conclusions and Future Work

This paper proposed a hybrid deep learning-based model for object recognition - FD-DFM. This method integrates feature fusion and decision fusion into neural networks with the D-S evidence theory. The method is evaluated with fruit recognition and the results shows it can significantly improve the fruit recognition accuracy, especially for the fruit and vegetable with similar color, shape, and texture.

In the future, we will apply the FD-DFM model into other scenarios, e.g., we will explore other approaches for the final fusion stage, e.g., using the graph convolutional network to further improve recognition accuracy. Another direction is that we will continue to optimize the model for embedded system applications.

Acknowledgement. This research is supported by the National Key R&D Program (2018YFE0116700), the Shandong Provincial Natural Science Foundation (ZR2019MF049, Parallel Data Driven Fault Prediction under Online-Offline Combined Cloud Computing Environment), and also supported by Fundamental Research Funds for the Central Universities.

References

1. Khaleghi, B., Khamis, A., Karray, F.O., Razavi, S.N.: Multisensor data fusion: a review of the state-of-the-art. *Inf. Fus.* **14**(1), 28–44 (2013)
2. Aziz, A.M.: A new multiple decisions fusion rule for targets detection in multiple sensors distributed detection systems with data fusion. *Inf. Fus.* **18**, 175–186 (2014)

3. Steinberg, A.N., Bowman, C.L., White, F.E.: Revisions to the JDL data fusion model. *Proc. SPIE - The Int. Soc. Optical Eng.* **37**(19), 430–441 (1999)
4. Llinas, J., Bowman, C., Rogova, G., et al.: Revisiting the JDL Data Fusion Model II. Svensson, P., Schubert, J. (eds.), pp. 1218–1230 (2014)
5. Kokar, M.M., Tomasik, J.A., Weyman, J.: Formalizing classes of information fusion systems. *Inf. Fus.* **5**(3), 189–202 (2004)
6. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. *Comput. Sci.* **33**(20), 296–310 (2015)
7. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 770–778 (2016)
8. Chen, Z., Li, W.: Multisensor feature fusion for bearing fault diagnosis using sparse autoencoder and deep belief network. *IEEE Trans. Instrum. Measur.* **66**(7), 1693–1702 (2017)
9. Chen, F.C., Jahanshahi, M.R.: NB-CNN: deep learning-based crack detection using convolutional neural network and Naïve Bayes data fusion. *IEEE Trans. Ind. Electron.* **65**(5), 4392–4400 (2017)
10. Ghamisi, P., Hofle, B., Zhu, X.X.: Hyperspectral and LiDAR data fusion using extinction profiles and deep convolutional neural network. *IEEE J. Select. Top. Appl. Earth Observations Remote Sens.* **10**(6), 3011–3024 (2017)
11. Luyang, J., Taiyong, W., Ming, Z., et al.: An adaptive multi-sensor data fusion method based on deep convolutional neural networks for fault diagnosis of planetary gearbox. *Sensors* **17**(2), 414 (2017)
12. Girshick, R., Donahue, J., Darrell, T., Malik, J.: Rich feature hierarchies for accurate object detection and semantic segmentation. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 580–587. IEEE Computer Society (2014)
13. Girshick, R.: Fast R-CNN. In: *IEEE International Conference on Computer Vision*, pp. 1440–1448. IEEE Computer Society (2015)
14. Ren, S., He, K., Girshick, R., Sun, J.: Faster R-CNN: towards real-time object detection with region proposal networks. *IEEE Trans. Pattern Anal. Mach. Intell.* **39**(6), 1137–1149 (2017)
15. Redmon, J., Divvala, S.K., Girshick, R.B., et al.: You only look once: unified, real-time object detection. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, June 27–30 2016, Washington: IEEE Computer Society*, pp. 779–788 (2016)
16. Liu, W., Anguelov, D., Erhan, D., et al.: SSD: single shot multibox detector. In: *LNCS 9905: Proceedings of the 14th European Conference on Computer Vision, Amsterdam, Oct 11–14 2016*, pp. 21–37. Springer, Berlin (2016). https://doi.org/10.1007/978-3-319-46448-0_2
17. Sa, L., Ge, Z.Y., Dayoub, F., et al.: DeepFruits: a fruit detection system using deep neural networks. *Sensors* **16**(8), 1222 (2016)
18. Goodman, I.R., Mahler, R.P., Nguyen, H.T.: Mathematics of data fusion. *Theor. Decis. Libr.* **37**(1), 137–153 (2010)
19. Dasarathy, B.V.: *Decision Fusion*. IEEE Computer Society Press, Florida (1993)
20. Smirnov, A., Pashkin, M., Chilov, N., et al.: Knowledge logistics in information grid environment. *Future Gener. Comput. Syst.* **20**(1), 61–79 (2004)



Feature Fusion Detection Network for Multi-scale Object Detection

Weishan Zhang¹(✉), Xia Liu¹, Liang Xu², Zhaotong Li¹, Hongwei Zhao¹,
and Jiehan Zhou³

¹ College of Computer Science and Technology, China University of Petroleum,
Qingdao, China

zhangws@upc.edu.cn

² School of Computer and Communication Engineering,
Beijing University of Science and Technology, Beijing, China

xuliang.upc.edu@gmail.com

³ Faculty of Information Technology and Electrical Engineering,
University of Oulu, Oulu, Finland

jiehan.zhou@oulu.fi

Abstract. Small-scale-object usually occupies a small area in an image. The existing object detection methods are performing well for small-scale object detection in real scenes. This paper proposes, a Feature Fusion Detection Network (FFDN), for multi-scale objects detections. Firstly, the FFDN applies three feature maps in the improved VGG16 (Visual Geometry Group Network 16) with a proposed resolution expansion module to achieve the same resolution of the three feature maps. Then the FFDN fuses these three feature maps by a lightweight feature fusion method. Finally, it generates the feature pyramid by the fused feature map to achieve multi-scale object detection. In addition, we design a default box matching concession method which enables to train the real targets, and increases the number of positive samples. The experiments show that FFDN has better performance compared with the existing neural networks. It improves the recall rate for small-scale objects detection and the accuracy for large-scale object detection.

Keywords: Multi-scale object detection · Resolution expansion module · Default box matching · Neural network

1 Introduction

Deep learning is widely used for image classification [1], object detection [2], semantic segmentation [3], and achieved fairly good results. However, it is still challenging for these existing methods for processing, the scale changes of the targeting objects.

Figure 1 shows how existing methods are used to multi-scale object detection. Figure 1(a) inputs images with different sizes into the convolution neural network to generate feature maps for different scales. This method is effective

but inefficient. Faster RCNN [4] and RFCN (Region-based Fully Convolutional Networks) [5] use only one top feature map to detect objects with different scales through default boxes with different sizes as shown in Fig. 1(b). But there are inconsistencies between fixed receiving domains and objects with different scales. SSD (Single Shot MultiBox Detector) [6] and MS-CNN (Multi-scale Deep Convolutional Neural Network) [7] detect objects with different scales by using the feature maps in different layers with convolutional neural networks as shown in Fig. 1(c). The shallow feature map has smaller receptive field and the deep feature has larger receptive field. However, shallow feature maps have less semantic information, which leads to unsatisfied detection accuracy for small objects. FPN (Feature Pyramid Networks) [8], ZIP (Zoom out-and-in network) [9] and DSSD (Deconvolutional Single Shot Detector) [10] adopt top-down structure to fuse all information of feature maps. As shown in Fig. 1(d), adding additional structure to construct feature pyramid will incur computational overhead and increase detection time. In addition, each layer of the newly generated feature pyramid only integrates the features of the high level layer, ignoring the features of the lower level.

In order to solve the above issue, Singh et al. [11] proposes a new training method: Scale Normalization for Image Pyramids (SNIP). In gradient echo, the

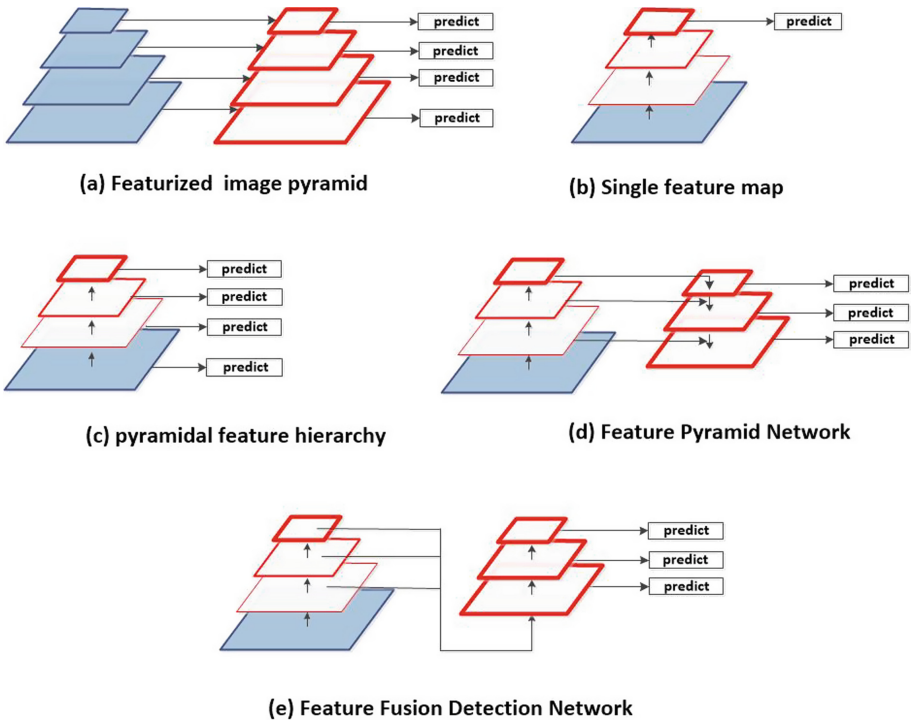


Fig. 1. Solutions to multi-scale objects detection.

gradient of ROI (region of interest) corresponding to the size of training set used in the pre-training model is only retrieved. In order to solve the problem of SNIP slow training speed, SNIPER [12] does not process all the pixels in the image pyramid, and selectively processes the context area around the annotated object by generating chips of multiple scales. However, these two methods sacrifice the detection speed. TridentNet (Scale-Aware Trident Networks) [13] achieves multi-scale object detection through the range of a receptive field. Specifically, three branches are used to realize the receptive field of multi-scale objects. The three branches share weights and dilation rate controls the size of the receptive field. ION (Inside-outside net) [14] uses hopping pooling to extract information at multiple layers, and then uses fused features to detect objects. HyperNet [15] integrates the depth, middle and shallow features of a image to detect objects. These methods mainly enhance the ability of feature expression through fusion to achieve multi-scale object detection. These methods' network structure is complex, although it improves the detection accuracy, but it can not meet the real-time requirements, and is difficult to apply to actual production deployment.

Henceforth, in this paper, we propose a Feature Fusion Detection Network (FFDN), to detect multi-scale objects. FFDN uses three feature maps in the improved VGG16 network with a newly proposed resolution expansion module to achieve the same resolution of the three feature maps. Then these three feature maps are fused by a lightweight feature fusion method. We make use of Conv4.3, Conv6.2 and Conv7.2 convolution layers of VGG16 neural network; the resolution expansion module is used to make the three feature maps the same resolution; then the transformed feature maps are fused, so that the fused feature maps contain both high-level semantic information and low-level detail information; finally, the fused feature maps generate feature pyramid to detecting multi-scale objects. In the training process, a default box matching concession method is designed to increase the number of positive samples, which enables the real targets being trained. This model improves recall rate of small-scale objects and precise location of large-scale objects.

The remainder of the paper is organized as follows: Sect. 2 presents the architectural design and details the implementation of FFDN. Section 3 presents the default box matching concession method. Section 4 evaluations the deployed FFDN solution. Section 5 gives the conclusion.

2 Feature Fusion Detection Network

Figure 2 presents the Feature Fusion Detection Network structure. The FFDN uses VGG16 as feature extraction network. It uses Conv4.3, Conv6.2 and Conv7.2 feature maps for feature fusion. It generates the feature pyramids from the fused feature maps for object detection with different scales. Finally, it uses Non-Maximum Suppression (NMS) algorithm to screen out duplicate default boxes and outputs the final detection results. Resolution expansion module includes resolution expansion layer and upper sampling layer. Resolution expansion layer enlarges the size of feature maps in Conv6.2 convolution layer and

reduces the number of channels without increasing computation. Upper sampling layer realizes the conversion from low resolution to high resolution by interpolation.

2.1 VGG16 Network

VGG16 network consists of multiple convolution layers and a pool layer. It uses 3×3 small convolution kernels and a 2×2 small pooling kernels. It consists of five groups of convolutions, each consisting of two or three convolution layers, and the pooling layer is used to reduce parameters. In addition, in each group of convolutions, the number of convolution kernels is fixed. The number of convolution kernels in each group is 64, 128, 256, 512 and 512 respectively. In order to improve feature extraction, the pooling layer and three full connection layers in VGG16 network are deleted, and two convolution blocks are added. Each convolution block has two convolution layers. The final size of the feature maps in the network is $10 \times 10 \times 512$.

2.2 Resolution Expansion Module

The resolution of feature map plays an important role in object detection. It is helpful for fusing different resolution feature maps in multi-scale object recognition. Before feature fusion, the size of feature map should be consistent. The resolution expansion module consists of two parts. One is the resolution expansion layer, the other is the upper sampling layer. For the upper sampling layer, the convolution kernel of 1×1 is used to reduce the number of channels from 1024 to 256, which is helpful to reduce the training parameters and the complexity of the model. Then the feature map is expanded from 10×10 to 38×38 by interpolation.

In order to obtain high-resolution feature maps without additional computational effort, we design a resolution expansion layer, which is efficient for image conversion with different resolutions and can be directly inserted into VGG16 model. Assume that the dimension of the input feature graph is: $H \times W \times C \times r^2$, where m is the up-sampling factor. The resolution expansion layer enlarges the width and height of the feature map by reducing the number of channels in the feature map, as defined in the following:

$$g(I^{LR}) = O^{SR} \quad (1)$$

Each specific conversion function is as follows:

$$g(I_w^{LR}) = O_{w*r}^{SR} \quad (2)$$

$$g(I_h^{LR}) = O_{h*r}^{SR} \quad (3)$$

$$g(I_c^{LR}) = O_{c/r^2}^{SR} \quad (4)$$

In the above formulas, O^{SR} is a feature map with high resolution and I^{LR} is a feature map with low resolution. w, h, c are the width, height, channel number

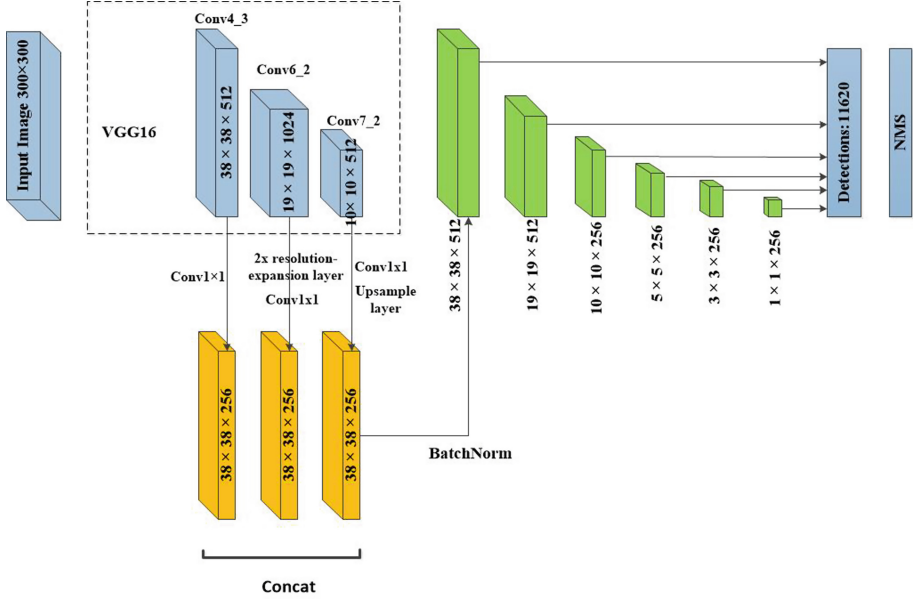


Fig. 2. The structure of FFDN.

of the input low-resolution images, $w \times r$, $h \times r$ and c/r^2 which are respectively the width, high and channel number of the transformed high-resolution images. Resolution expansion module effectively reduces the number of channels and enlarges the size of feature map. It does not introduce additional parameters, and it doesn't increase the amount of calculation either.

In the resolution expansion layer, Conv7.2 feature maps is $19 \times 19 \times 1024$, and the up-sampling factor $r = 2$. Therefore, the size of feature map is transformed from $19 \times 19 \times 1024$ to $38 \times 38 \times 256$. Then through the convolution kernel of 1×1 , the changed feature map is integrated and the feature map of $38 \times 38 \times 256$ is generated. After transformation, the three feature maps are fused in channel number dimension, and then the fused feature maps are regularized by BatchNorm [16] layer. The final size of feature map is $38 \times 38 \times 768$.

2.3 Feature Pyramid

The feature pyramid is generated after convolution operation on the feature map with the fusion size of $38 \times 38 \times 768$. FFDN then convolutes each layer of the feature pyramid using two convolution layers with a convolution kernel of 3×3 . One of the convolution layers outputs the class of default boxes as the prediction result of the category, the other outputs the location offset of default boxes. Then according to the class confidence ranking of default boxes, it removes the redundant boxes by the NMS algorithm and remains, the boxes most likely

to contain objects. The size and location of default boxes are adjusted according to the predicted offset, and finally generate the final detection results.

3 Default Box Matching Concession Method

During the training process, we usually choose the IOU (Intersection-Over-Union) of a default box and a real box as a deciding factor, if IOU is larger than the given threshold (usually 0.5), then the default box is used as a matching box for a real box. However, the size of the pre-set default box is difficult to match well with all the scales of object. If some scales of object do not match the default boxes, then these objects cannot not be fully trained, which results in unsatisfied detection results.

Therefore, we propose a default box matching concession method to solve the above problems. We set the IOU thresholds to 0.5 for defining positive and negative samples; positive samples are greater than or equal to 0.5, and negative samples are less than 0.5. For real boxes that do not match any default boxes, their IOU values and all default boxes are ranked in an ascending order, and it selects the first five default boxes as matching boxes of real boxes and inputs them as positive samples into the neural network for training. This method increases the number of positive samples in the input network, increasing the recall rate of object with this scale, and improves the detection accuracy.

4 Evaluation

In order to verify the effectiveness, this experiment uses two data sets, one is the data-set with safety helmet. There are two classes in the data-set: blue and red safety helmet. The other is the data-set with multi-scale tower crane. It divides 6000 images into training and test set with the ratio of 8:2.

It selects the dataset trained by VGG16 with ImageNet [1], as the initial model. The input image size is 300×300 . Due to the limitation of GPU memory, it sets `batch_size` as 24 to train on a GPU. The total number of training is 100 epochs, and the initial learning rate is 10^{-4} . The learning rates of the 30th epoch and the 60th epoch are reduced by 10 times [9], and the weight decay is set to 0.0001.

4.1 Ablation Experiment

This method is evaluated on the test set, and the mAP (mean Average Precision) score [17] is used as the metric to evaluate detection performance. In order to verify the effectiveness, we perform ablation experiments on the test set with blue helmet. The results are summarized in Table 1.

In the experiment, SSD and FFDN select VGG16 trained with ImageNet dataset as the feature extraction model. Line 1 and 2 in Table 1 show that the fusion of the three feature maps improves the detection accuracy of blue helmet,

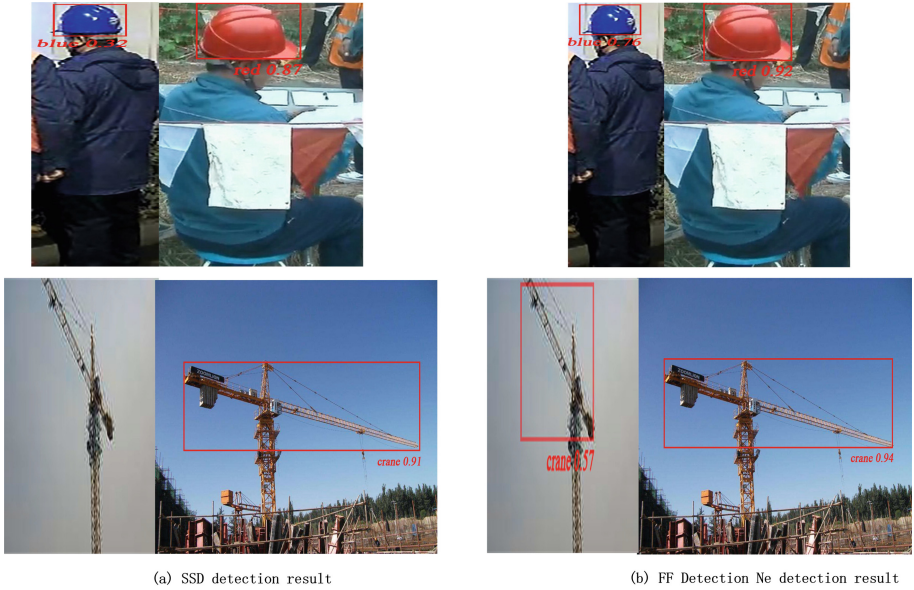


Fig. 3. Detection result by SSD and FFDN. (Color figure online)

and the mAP improves by nearly 1%. We think that feature pyramids generated on the basis of fused feature maps, make feature maps at all levels contain semantic information and detailed information. In Table 1, the method “FFDN without resolution expansion layer” uses linear interpolation method to sample small resolution feature maps, FFDN uses resolution expansion layer to sample 19×19 feature maps, and other feature maps are sampled by linear interpolation method. mAP increased from 86.3% to 86.7%. Table 1 shows that the mAP of detector is increased by 0.5% after introducing the Default Box Matching Concession Method. It enables previously untrained objects to be trained and improves recall rates for objects with certain scales.

Table 1. Ablation experiments on the dataset with bluehat.

Method	mAP
SSD	85.4
FFDN without resolution expansion layer	86.3
FFDN	86.7
FFDN with default box matching concession method	87.2

4.2 Detection Result Analysis

In order to test the speed of FFDN, we count the detection time of the network in the test set with tower crane, and then calculated the number of frames per second (fps). We set `batch_size` to 1 and test the speed on a machine with a GPU of 1080Ti. Table 2 shows the test results represented with mAP.

SSD does not fuse the features in high and low levels, and only uses a single layer of different levels to detect. It shows that FFDN improves the detection comparing with SSD. FFDN uses the fused feature map to generate feature pyramids, which promotes the low-level feature map to the high-level feature map with detailed information. Among them, the detection accuracy of tower crane has been improved by 2.2%. In addition, although Faster RCNN uses RPN network (Region Proposal Network) to select default boxes, it only uses one feature map at the top, while FFDN uses multiple feature maps, which improves the detection effectiveness of objects with different scales. FFDN improves the precision 1.1%, 0.3% and 1.3% respectively comparing with Faster RCNN. FFDN performs the best detection precision among the three methods.

It should be noted that Faster RCNN sizes the image size to 600×800 . Table 2 shows that FFDN could balances precision and speed. Although its detection speed is lower than that of SSD, its precision is improved on the three datasets. Faster RCNN firstly generates default boxes from RPN network, then classifies and regresses them. FFDN uses convolution operation to classify and regress directly. It achieves better detection results and higher recognition speed than Faster RCNN.

Table 2. Testing results and speed.

Methods	Input size	Bluehat (mAP)	Redhat (mAP)	Crane (mAP)	Recall	Speed (fps)
Faster RCNN	600×800	86.1	88.2	85.6	84.2	9.3
FFDN	300×300	87.2	88.5	86.9	85.7	20.3
SSD	300×300	85.4	87.9	84.7	82.3	22.0

Figure 3 presents detection results. Because SSD only uses single feature map for prediction, and low-level feature map lacks semantic information, high-level feature map lacks detail information. For small-scale tower crane, there is a phenomenon of omission of detection for SSD, and FFDN detects it with the score of 0.57. For medium-scale blue safety helmet, SSD detection result is 0.32 and FFDN's result is 0.75. Although detected, the SSD's confidence is low. For large-scale red safety helmet and large-scale crane, the FFDN improves the confidence 0.05, 0.03 respectively. Because of effective feature fusion, FFDN improves the recall rate of small-scale objects, the confidence and locations of medium and large-scale objects are more accurate.

5 Conclusion

This paper proposes a feature fusion detection network (FFDN) to make the multi-scale object detection. The method firstly extracts objects' features using the improved VGG16 network. It transforms the low-resolution feature map of VGG16 into high-resolution feature map for fusion by using a resolution expansion module, and then generates the feature pyramid by the fused feature map. Finally, it uses the feature map in the pyramid to detect objects. In addition, in order to avoid the problem that some objects can not match default boxes in the training process, we design a default box matching concession method to increase the number of positive samples. The experimental results show that FFDN outperforms SSD and Faster RCNN in object detection with multi-scales, among which its improvement for small-scale objects detection is more obvious. The detection efficiency can also meet the real-time performance and balance detection accuracy and speed.

Acknowledgments. This research is supported by the National Key R&D Program (2018YFE0116700), the Shandong Provincial Natural Science Foundation (ZR2019MF049, Parallel Data Driven Fault Prediction under Online-Offline Combined Cloud Computing Environment), and also supported by Fundamental Research Funds for the Central Universities.

References

1. Krizhevsky, A., Sutskever, I., Hinton, G.E.: ImageNet classification with deep convolutional neural networks. In: *Advances in Neural Information Processing Systems*, pp. 1097–1105 (2012)
2. Girshick, R., Donahue, J., Darrell, T., et al.: Rich feature hierarchies for accurate object detection and semantic segmentation. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 580–587 (2017)
3. Long, J., Shelhamer, E., Darrell, T.: Fully convolutional networks for semantic segmentation. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 3431–3440 (2017)
4. Ren, S., He, K., Girshick, R., et al.: Faster R-CNN: towards real-time object detection with regional proposal networks. In: *Advances in Neural Information Processing Systems*, pp. 91–99 (2015)
5. Dai, J., Li, Y., He, K., et al.: R-FCN: object detection via region-based fully convolutional networks. In: *Advances in Neural Information Processing Systems*, pp. 379–387 (2016)
6. Liu, W., et al.: SSD: single shot multibox detector. In: Leibe, B., Matas, J., Sebe, N., Welling, M. (eds.) *ECCV 2016*. LNCS, vol. 9905, pp. 21–37. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-46448-0_2
7. Cai, Z., Fan, Q., Feris, R.S., Vasconcelos, N.: A unified multi-scale deep convolutional neural network for fast object detection. In: Leibe, B., Matas, J., Sebe, N., Welling, M. (eds.) *ECCV 2016*. LNCS, vol. 9908, pp. 354–370. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-46493-0_22
8. Lin, T.Y., Dollr, P., Girshick, R., et al.: Feature pyramid networks for object detection. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2117–2125 (2017)

9. Li, H., Liu, Y., Ouyang, W., et al.: Zoom out-and-in network with recursive training for object proposal. arXiv preprint [arXiv:1702.05711](https://arxiv.org/abs/1702.05711) (2017)
10. Fu, C.Y., Liu, W., Ranga, A., et al.: DSSD: deconvolutional single shot detector. arXiv preprint [arXiv:1701.06659](https://arxiv.org/abs/1701.06659) (2017)
11. Singh, B., Davis, L.S.: An analysis of scale invariance in object detection snip. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 3578–3587 (2018)
12. Singh, B., Najibi, M., Davis, L.S.: SNIPER: efficient multi-scale training. In: Advances in Neural Information Processing Systems, pp. 9310–9320 (2018)
13. Li, Y., Chen, Y., Wang, N., et al.: Scale-aware trident networks for object detection. arXiv preprint [arXiv:1901.01892](https://arxiv.org/abs/1901.01892) (2019)
14. Bell, S., Lawrence Zitnick, C., Bala, K., et al.: Inside-outside net: detecting objects in context with skip pooling and recurrent neural networks. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2874–2883 (2016)
15. Kong, T., Yao, A., Chen, Y., et al.: HyperNet: towards accurate region proposal generation and joint object detection. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 845–853 (2017)
16. Ioffe, S., Szegedy, C.: Batch normalization: accelerating deep network training by reducing internal covariate shift. arXiv preprint [arXiv:1502.03167](https://arxiv.org/abs/1502.03167) (2015)
17. Chen, X., Fang, H., Lin, T.Y., et al.: Microsoft COCO captions: data collection and evaluation server. arXiv preprint [arXiv:1504.00325](https://arxiv.org/abs/1504.00325) (2015)



Post Profiles Research Based on Electric Power Major

Wei Dai¹(✉), Tao Xu², Jun Zhao², Rong Sun¹, Xin-dong Zhao¹,
Yueran Wen³(✉), Hongfei Yuan⁴, Shangxiu Song⁵,
and Haoyu Zong⁵(✉)

¹ Jiangsu Electric Power Company Research Institute, Nanjing 211103, China
15295520592@139.com

² Jiangsu Electric Power Company, Nanjing 210000, China

³ School of Labor and Human Resources, Renmin University of China,
No. 59 Zhong Guan Cun Avenue, Hai Dian District, Beijing, China
wenyueran@vip.sina.com

⁴ Job Reading (Beijing) Technology Co., Ltd., No. 3 Suzhou Street,
Haidian District, Beijing, China

⁵ School of Computer and Communication Engineering,
University of Science and Technology Beijing (USTB), Beijing 100083, China
15200428420@163.com

Abstract. In the era of big data, how to effectively use information resources under the condition of information overload has been the focus of academia and industry. As an important data analysis method, user profile technology is widely used in the field of big data, including the field of recommendation system. Based on the background of electric power post training, this paper constructs the post knowledge thesaurus of electric power industry, uses the word segmentation tool-Jieba to segment the job description, and processes the text after the word segmentation combined with Term Frequency–Inverse Document Frequency (TF-IDF) algorithm. Then, the post profiles at all levels are displayed by Wordcloud visualization tool. Finally, the effectiveness of our method is proved by experiments. This work provides a basis for the intelligent recommendation of the best learning materials in various positions and auxiliary online examination technology for employees in the future.

Keywords: Post profile · Recommendation system · Electric power · Intelligent learning · Knowledge extraction

1 Introduction

In the era of knowledge and intelligence, the impact on the traditional business model of enterprise training is becoming more and more serious. At present, there are many widespread problems in the training of electric power field, for example, the wide sources of learning resources lead to the difficulty of management, the ineffectiveness of traditional study arrangement and manual examination, the resource construction is time-consuming and labor-intensive but the effect is not obvious. Nowadays, most of the electric power learning resources lack of internal implicit knowledge mining, and

the professional knowledge required by various professional posts is constantly updated and changing, but lack of timely and effective adjustment and supplement, which can't meet the individual and accurate learning needs of employees in different professional posts [1]. The recommendation system based on profile technology can effectively solve this problem. On the one hand, the system can establish post profiles by analyzing job attributes, on the other hand, it can integrate massive heterogeneous power knowledge resources, so as to provide personalized knowledge guidance for power employees.

In view of the existing enterprise training and employee learning mode of electric power has been unable to meet the needs of enterprise and employee development, it is necessary to use artificial intelligence technology to study the massive heterogeneous resources scattered in the field of electric power. Therefore, this paper starts from solving these problems, combined with the characteristics of knowledge in the field of power, applies user profile technology in the field of recommendation, by analyzing the descriptive files and related attributes of various positions in the power industry, the profile of each position is established, which provides a basis for the implementation of content-based intelligent learning recommendation method and auxiliary online examination technology in the future. Experiments show that our method builds the post profile model is accurate and has certain application value.

The rest of the paper is organized as follow: Sect. 2 is for the related work. In Sect. 3, we described the detail of the method we used. The experimental results and analysis are discussed in Sect. 4, followed by the conclusion and future work in Sect. 5.

2 Related Work

At present, the research in this field is mainly focused on user profiles and recommendation systems, while the research on post profiles is relatively little. User Profile, top proposed by Alan Cooper, is a target user model based on a series of real data [2]. It depicts the same kind of users in different dimensions, aiming at fully displaying the user's information panorama through massive user behavior data mining. In this paper [3], authors use an ontology-based system for job recommendation. This has been used to model the user profile and provide more personalized job listings to the user. After detailed domain analysis, the relevant classes were identified and the attributes, relations were defined. Such a system introduces personalized recommendation in job recruitment domain, by recommending jobs that are likely to be of interest to candidates.

In [4], authors introduce MineraSkill methodology that deals with methods to infer the desired profile of a candidate for a job vacancy. In the end, vacancies were mined in the Information Technology area, through the analysis of relevance of keywords using TF-IDF and through association rules generated by the Apriori algorithm. However, more experiments are needed to verify whether the ontology model has a good effect in practical application.

Recommendation systems are used to analyze user profiles, content items and their relationships, and try to predict future user behavior. Recommendation systems are

mainly divided into three types [5]: collaborative-based filtering (CF) [6–10], content-based filtering (CBF) [11] and hybrid filtering [12–16]. User profile technology provides the basis of user-project association degree calculation for content-based recommendation algorithms and provides the basis of user similarity for recommendation algorithm based on collaborative filtering. Amit et al. [17] proposes the design aspects of Analytical Recommendation System that represents attributes for designations, skills and job profile of employees for an organization based on career history that serves as data set for user-based collaborative filtering, hence recommendations can be provided for Employees and Organization. In this paper [18], authors have proposed a novel framework that employs text extraction techniques for generating personalized skill graph representations of candidate profile. An evaluation of our current skill extraction model with an industrial scale dataset yielded a precision and recall of 80.54% and 86.44% respectively. However, they didn't consider dynamically adjusting the profiles according to the job requirements and the skill level of the workers.

Post profile is an effective tool to sketch the target post and contact the demands and design direction of trainees. Each post in the power industry has different characteristics. Post profile is to use structured data or unstructured data to present the attributes of the post in the form of data, it can perfectly express the full information of a post and label it, so we propose to design a more suitable professional post profile model for the power industry.

3 Profile Construction

3.1 Source of Data

The profiles work is the basis of recommendation. Post profiles need to be fully combined with the characteristics of positions in the field of electric power. Through the analysis of the profiles of all levels of posts, the key knowledge points of the workers in each position will be helpful to solve the cold start problem of the recommendation system, it's the basis of content-based recommendation.

The information on our post profile is provided by Jiangsu Electric Power Company Research Institute, including training textbooks, technical specifications and standards for the power industry and three posts description, respectively, relaying worker (500 kV), relaying worker (220 kV) [19–21], distribution circuit worker. Relaying worker are technical application professionals who engaged in operation, commissioning and installation of relay protection and automation devices in power plants and power systems. The distribution circuit worker is responsible for line operation and maintenance, erecting and maintaining overhead power lines and other line equipment and distribution equipment. The post description file contains level, core work, description of core work, task items, evaluation points, etc. It covers the daily work content of the post and the specific requirements of various operations. However, the skill description of relaying worker (500 kV) and relaying worker (220 kV) is basically similar. Therefore, we selected the two positions for the research on profiles work: relaying worker and distribution circuit worker. Each position is divided into five levels: primary worker, intermediate worker, senior worker, technician and senior technician.

3.2 Experimental Procedure

Most of the massive post description resources have little effect on the construction of post profile, so we need to extract the most critical and general words from these texts to help the overall description of post. The profile uses keyword extraction algorithm which is based on TF-IDF [22], and realizes the profiles of posts at all levels by extracting keywords from descriptive texts of post skills.

The basic process of post profile construction is as follows (see Fig. 1):

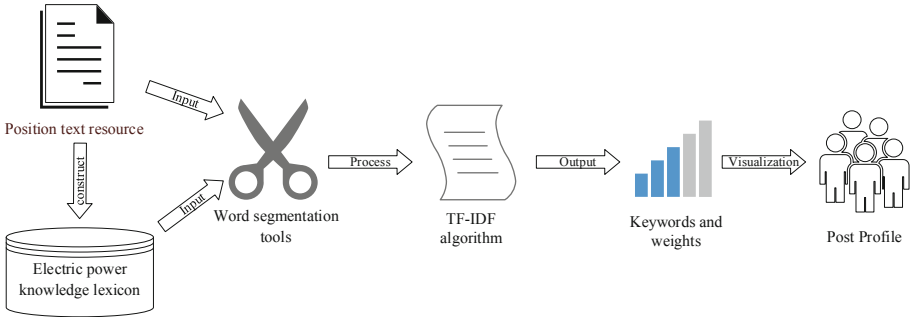


Fig. 1. Flow chart of post profile construction

1. Manual construction of electric power knowledge lexicon based on existing job description. In order to ensure the accuracy of text segmentation in the next step, professionals in the field of electric power are required to help build the power knowledge lexicon.
2. Word segmentation tools (such as Jieba) are used to segment job description texts at all levels. The top step of word segmentation is to load the customized lexicon and stop the lexicon.
3. TF-IDF algorithm is used to process the text after segmentation and calculate the weight of each word. TF-IDF is a statistical method used to assess the importance of a word to a document set or one of the documents in a corpus. The main idea of TF-IDF is that if a word appears frequently in an article and rarely in other articles, it can be regarded as the key word of the article.

The formula for calculating TF-IDF of a word in a text:

$$TF - IDF = TF * IDF$$

TF is word frequency, referring to the frequency of the word appearing in the article; IDF is inverse document frequency, which measures the frequency of the word appearing in all articles. Formula for calculating TF:

$$TF_{i,j} = \frac{n_{i,j}}{\sum_k n_{k,j}}$$

Among them, $n_{i,j}$ is the number of occurrences of the word in the document d_j , and denominator is the total number of occurrences of all words in the document d_j . The formula for calculating IDF:

$$IDF_j = \log \frac{|D|}{|\{j : t_i \in d_j\}| + 1}$$

Among them, $|D|$ is the total number of files in the corpus. $|\{j : t_i \in d_j\}|$ denotes the number of files containing the word t_i (i.e., the number of files containing $n_{i,j} \neq 0$). If the word is not in the corpus, it will cause the denominator to be zero, so in general, $|\{j : t_i \in d_j\}| + 1$ is used.

4. Visualize the keywords and weights acquired in the previous step by using the data visualization tool Wordcloud, and visually display the profiles of each post. The `generated_from_frequencies` method of Wordcloud can transform the weights of words obtained from the above step into two-dimensional images of images, which are composed of many words and become word clouds, in which the font size of words represent the weights of the words. Word clouds graphic vividly present the profile of the post.

4 Results and Discussions

According to the profiles process described above, the profiles of posts at all levels are carried out. There are 10 posts in two types of work. The profiles results are described below.

4.1 Relaying Worker

In order to ensure the safe, stable and reliable operation of the Grid, relay protection devices need to be adjusted according to the changes of operation mode, and relaying workers are mainly responsible for this part of work.

Primary Workers. The core work of primary relaying workers is to install and connect the vertical screen of relaying, and to check the sampling and setting value of relaying and self-safety devices.

Figure 2 show its profile (relaying post profiles temporarily remove the key word “relaying”). The size of the keyword font in the profiles represents the weight of the word in the profiles of the post. It can be seen that relaying primary workers need to focus on learning knowledge points: protection cabinet, secondary circuit, micro-computer calibrator, multimeter, substation, safety helmet and so on. The following Table 1 gives the weights of keywords in this post profile.

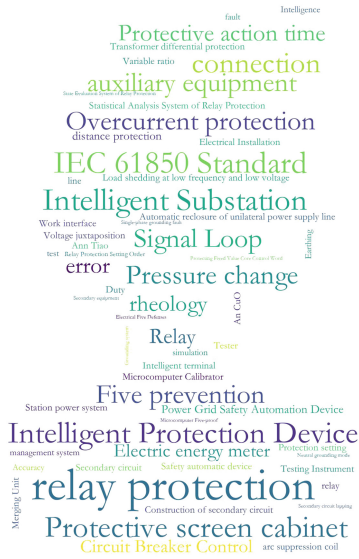


Fig. 3. The profile of relaying worker (intermediate worker).

Table 2. The top 10 keywords and their weights in the intermediate worker profile of relaying

Keywords	Weights
Relay protection	0.548387871112162
Intelligent substation	0.215401216268468
IEC 61850 Standard	0.215401216268468
Intelligent protection device	0.215401216268468
Protective screen cabinet	0.215401216268468
Connection	0.197409705816216
Signal loop	0.161550912201351
Overcurrent protection	0.161550912201351
Pressure change	0.161550912201351
Auxiliary equipment	0.161550912201351

Senior Worker. The core work of relaying senior workers is: the acceptance of protective devices below 110 kV; the acceptance of auxiliary equipment below 110 kV; the functional debugging of intelligent substation devices; the use of relaying-related equipment; the construction of secondary circuit; the debugging of relaying and self-safety devices. It can be seen that relaying senior workers need to focus on learning knowledge points (see Fig. 4): 110 kV and below (familiar with equipment under the voltage level), secondary circuit, security measures, etc. The following Table 3 gives the weights of keywords in this post profile.

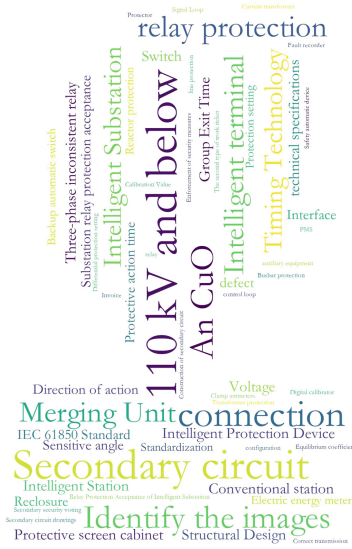


Fig. 4. The profile of relaying worker (senior worker).

Table 3. The top 10 keywords and their weights in the senior worker profile of relaying

Keywords	Weights
110 kV and below	0.405775398270757
Secondary circuit	0.374561906096083
Connection	0.286063672919060
Safety measures (An CuO)	0.218494445222715
Identify the images	0.200554548772323
Relay protection	0.173380641899216
Merging unit	0.156067460873368
Intelligent terminal	0.156067460873368
Intelligent substation	0.124853968698694
Timing Technology	0.124853968698694

Technician. The core work of relaying technicians is: simple defect treatment of relaying and self-protection device; use of other related equipment and functions; design of software and hardware of intelligent substation, implementation of security measures; use of relaying related equipment; debugging and installation of single secondary circuit; single defect treatment of relaying and self-protection device; accident analysis and defect treatment of secondary equipment. It can be seen that relaying technicians need to focus on learning knowledge points (see Fig. 5): defect handling, switch, secondary circuit, safety measures, protection action time, line protection and so on. The following Table 4 gives the weights of keywords in this post profile.

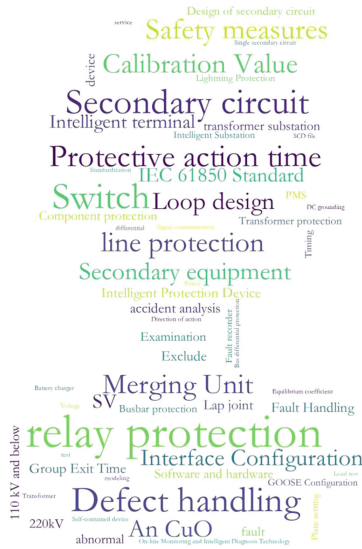


Fig. 5. The profile of relaying worker (technician).

Table 4. The top 10 keywords and their weights in the technician profile of relaying

Keywords	Weights
Relay protection	0.257844150542473
Switch	0.135047104035842
Defect handling	0.128545887127956
Secondary circuit	0.128545887127956
Protective action time	0.128545887127956
Safety measures	0.114858084162365
Line protection	0.107121572606630
Merging unit	0.107121572606630
Calibration value	0.107121572606630
Secondary equipment	0.085697258085305

Senior Technician. Core work of senior technicians: design of relaying and self-safety device; acceptance of Intelligent Substation; relevant secondary circuit debugging and maintenance; relay and self-safety device related defect treatment; comprehensive accident analysis and secondary equipment defect treatment. It can be seen that relaying senior technicians need to focus on learning knowledge points (see Fig. 6): intelligent substation, secondary circuit, intelligent terminal, fault handling, message, merging unit, etc. The following Table 5 gives the weights of keywords in this post profile.

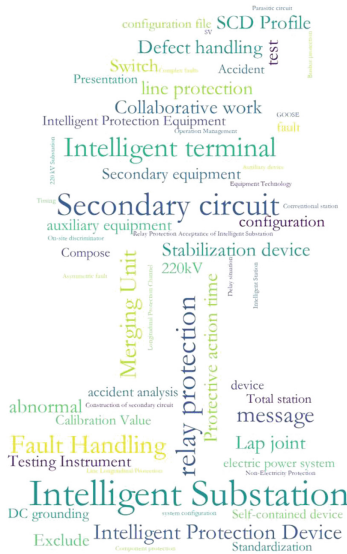


Fig. 6. The profile of relaying worker (senior technician).

Table 5. The top 10 keywords and their weights in the senior technician profile of relaying

Keywords	Weights
Intelligent substation	0.409209645576039
Secondary circuit	0.292292603982885
Relay protection	0.243538334403667
Intelligent terminal	0.233834083186308
Fault handling	0.204604822788019
Merging unit	0.175375562389731
Message	0.170143167124694
Intelligent protection device	0.146146301991442
Abnormal	0.117280659913936
Stabilization device	0.116917041593154

4.2 Distribution Circuit Worker

Distribution network is the link between transmission network and power users. Fault location of distribution network is the basic work to improve the reliability of demand-side power supply, the central technical link to realize the automation of distribution network, and one of the important tasks to ensure the safe and stable operation of the whole power system.

Intermediate Workers. The core work of intermediate workers in distribution circuit is: application of general information system for distribution circuit workers; general inspection and operation of distribution circuit and equipment; general maintenance and overhaul of distribution circuit and equipment; and general emergency repair of distribution circuit and equipment. It can be seen that the distribution circuit intermediate workers need to focus on learning the knowledge points (see Fig. 8): distribution transformer, distribution station room, information system, operation and maintenance, lines, fault repair, patrol and so on. The following Table 7 gives the weights of keywords in this post profile.

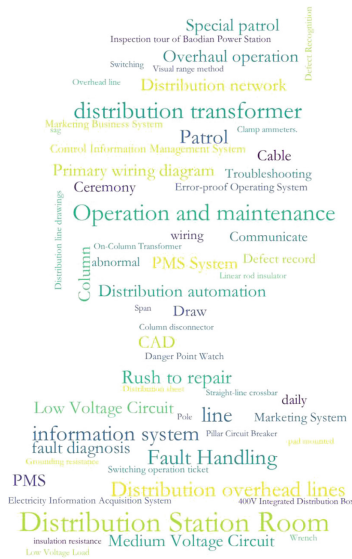


Fig. 8. The profile of distribution circuit worker (intermediate worker).

Table 7. The top 10 keywords and their weights in the intermediate worker profile of circuit

Keywords	Weights
Distribution station room	0.445519285822360
Distribution transformer	0.297012857214906
Operation and maintenance	0.297012857214906
Line	0.232471450086956
Information system	0.227688924312546
Distribution overhead lines	0.222759642911180
Troubleshooting	0.222759642911180
Fault handling	0.222759642911180
Patrol	0.208681228358509
Rush to repair	0.179854330619813

Senior Worker. The core tasks of senior workers in distribution circuit are: application and data audit of conventional distribution information system; inspection and operation of conventional distribution circuit and equipment; maintenance of conventional distribution circuit and equipment; emergency disposal of conventional distribution circuit and equipment. It can be seen that the knowledge points that senior workers of distribution circuit need to focus on are (see Fig. 9): conventional distribution lines, distribution station rooms, troubleshooting, switching, distribution overhead lines, patrols, etc. The following Table 8 gives the weights of keywords in this post profile.



Fig. 9. The profile of distribution circuit worker (senior worker).

Table 8. The top 10 keywords and their weights in the senior worker profile of circuit

Keywords	Weights
Conventional distribution lines	0.838931052835087
Distribution station room	0.559287368556725
Troubleshooting	0.419465526417543
Switching	0.349554605347953
Distribution overhead lines	0.349554605347953
Routine inspection	0.279643684278362
Three measures	0.209732763208771
Defect	0.176118498356491
Patrol	0.147358235814561
Marketing business system	0.139821842139181

Technician. The core tasks of distribution circuit technicians are: analysis of complex information data of distribution circuit workers; inspection of complex distribution circuit and equipment; maintenance and repair of complex distribution circuit and equipment; emergency repair of complex distribution circuit and equipment. It can be seen that distribution circuit technicians need to focus on learning knowledge points (see Fig. 10): distribution circuit network, distribution station room, equipment maintenance, PMS system, fault diagnosis, distribution overhead lines, major defects and so on. The following Table 9 gives the weights of keywords in this post profile.

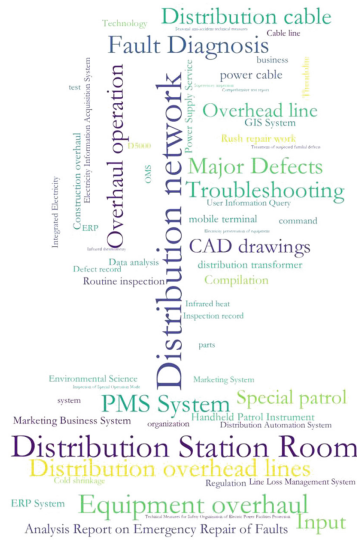


Fig. 10. The profile of distribution circuit worker (technician).

Table 9. The top 10 keywords and their weights in the technician profile of circuit

Keywords	Weights
Distribution network	0.657512212659499
Distribution station room	0.478190700115999
Equipment overhaul	0.358643025086999
PMS system	0.298869187572500
Distribution overhead lines	0.298869187572500
Fault diagnosis	0.298869187572500
Major defects	0.239095350057999
Overhaul operation	0.239095350057999
Distribution cable	0.239095350057999
Troubleshooting	0.239095350057999

Senior Technician. The core work of senior technicians in distribution circuit is: comprehensive analysis of difficult information data of distribution circuit workers; analysis and treatment of difficult problems in operation of distribution circuit; analysis and treatment of difficult problems in emergency repair of distribution circuit; analysis and treatment of difficult problems in maintenance of distribution circuit; analysis and treatment of difficult problems in distribution line engineering. It can be seen that the knowledge points that senior technicians of distribution circuit need to focus on are (see Fig. 11): difficult problems, distribution station rooms, troubleshooting, distribution transformers, key technical issues, critical defect, etc. The following Table 10 gives the weights of keywords in this post profile.

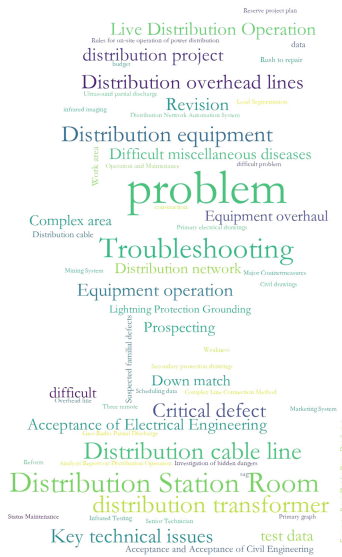


Fig. 11. The profile of distribution circuit worker (senior technician)

Table 10. The top 10 keywords and their weights in the senior technician profile of circuit

Keywords	Weights
Problem	1.919341081366420
Distribution station room	0.436305383317518
Troubleshooting	0.436305383317518
Distribution transformer	0.305413768322262
Distribution cable line	0.305413768322262
Distribution equipment	0.261783229990510
Critical defect	0.218152691658759
Distribution overhead lines	0.218152691658759
Key technical issues	0.218152691658759
Distribution project	0.174522153327007

4.3 Comparative Analysis of Results

Combining Tables 1, 2, 3, 4 and 5 and Fig. 12 (In the bar chart, five levels are represented by blue, yellow, green, red and black bars, among which with stripes are higher frequency words in different levels, abscissa represents keywords and ordinate represents weight), we can find that: 1. Relay protection and secondary circuit have appeared many times in the four levels of positions (relaying worker), and their importance ranks in the top six, which is in line with the core content of the post; 2. Comparing the top ten keywords of each level, half of the keywords don't appear in other levels of work. Such as the most weighted words of senior workers are 110 kV and below protection devices. This word has not appeared in other levels of jobs, because the work is a special requirement of senior workers, and it also shows our method has a clear distinction between different levels of work. 3. For lower-level workers, their work is mainly the basic operation of wiring, overhaul and debugging, while for higher-level technicians, their work is mainly to solve complex problems such as troubleshooting, diagnosis and accident analysis, which also meets the responsibilities of different levels within the post.

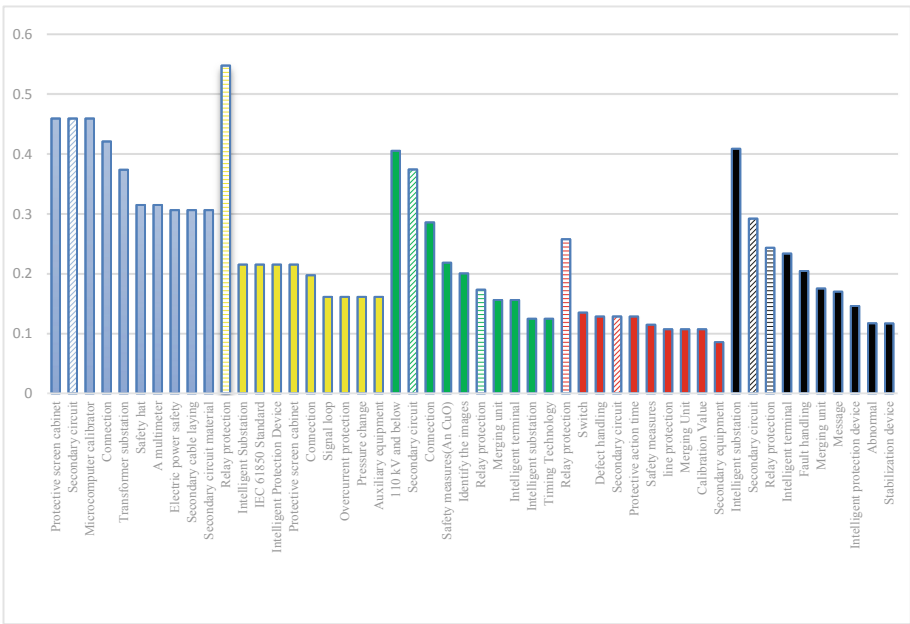


Fig. 12. Comparison of relaying workers at different levels (Color figure online)

Combining Tables 6, 7, 8, 9 and 10 and Fig. 13 (In the bar chart, five levels are represented by blue, yellow, green, red and black bars, among which with stripes are higher frequency words in different levels, abscissa represents keywords and ordinate represents weight), we can find that: 1. Distribution station room, distribution overhead

line and troubleshooting are the most frequent words. Except for primary workers, the top ten keywords of each level of work include these words, which is consistent with the work content of distribution circuit workers; 2. Except for primary workers, the most weighted word in every level of work have higher weight than other words, which is highlighting the core work content of different levels of workers; 3. Comparisons show that low-level workers are mainly engaged in the basic jobs with relatively low requirements such as wiring, while higher-level workers are mainly dealing with faults, problems, defects and other difficult work, such as with the largest weight word of the senior technicians is “problem”, the proportion of 1.9, far higher than other words, which is also in line with the actual work.

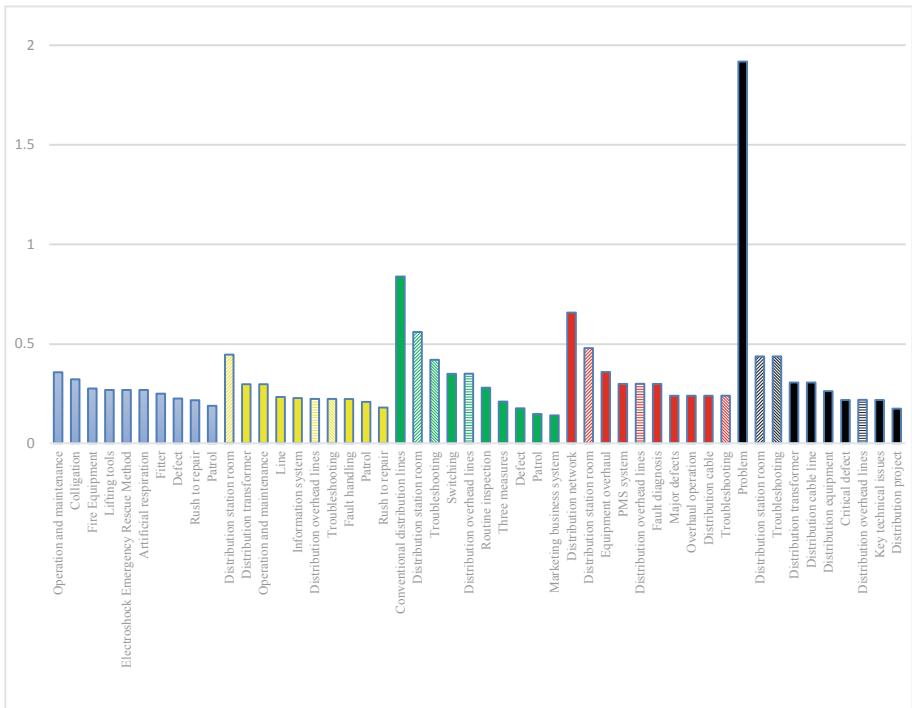


Fig. 13. Comparison of distribution circuit worker at different levels (Color figure online)

Then compare the same level work of two jobs horizontally: 1. For example (see Fig. 14), the top ten keywords weights are not very different, which also covers a wide range of work done by the primary workers, but the difficulty of operation is relatively easy to match; 2. But for the senior technicians of two posts (see Fig. 15), the largest weight of keywords is obviously higher than other words, which is because senior technicians need to be more prominent in their core work, so as to solve the more complex problems in this direction; 3. In addition, the same level of two types work content keywords are very different, which also shows that our method is better for differentiating different types of work performance.

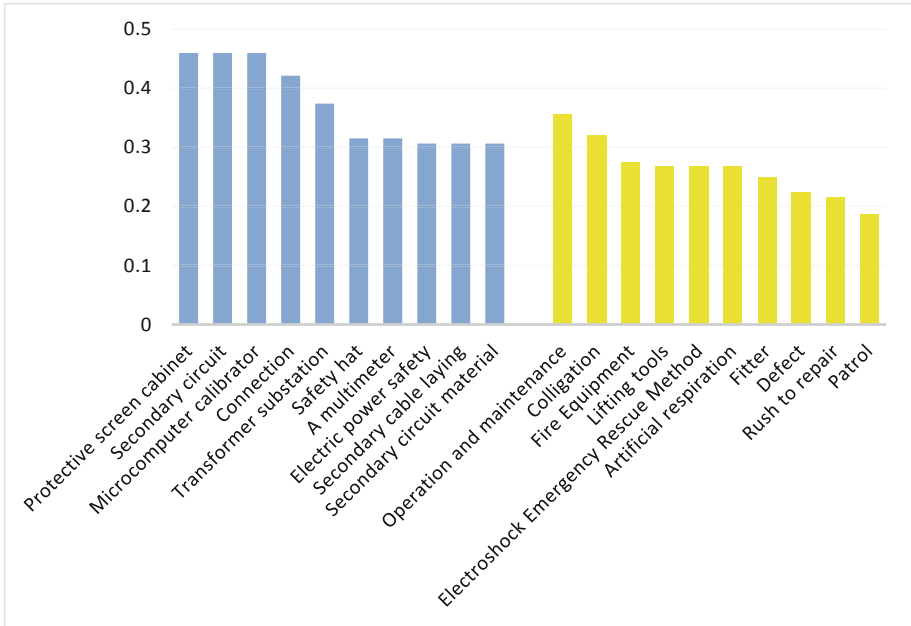


Fig. 14. Comparison of different types of work at the same level (primary worker)

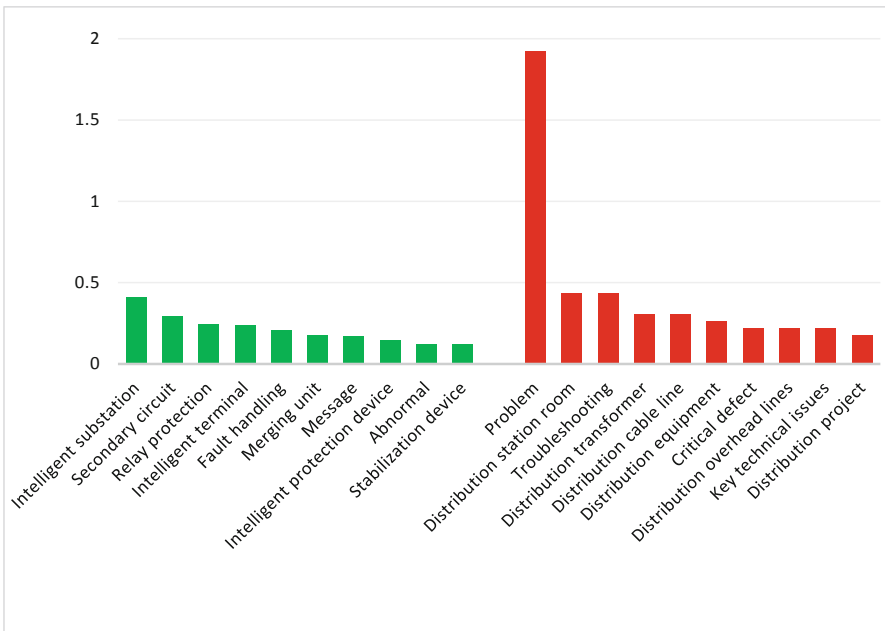


Fig. 15. Comparison of different types of work at the same level (senior technician)

5 Conclusion and Future Work

This paper mainly introduces the construction process of post profiles. Firstly, Term Frequency–Inverse Document Frequency (TF-IDF) algorithm is used to extract the key words of post description files. Then, in order to present the extraction effect of key words, Wordcloud can be used for visual analysis. Through the post profile, it is easy to figure out the key points to be learned for the post, which provides convenience for the implementation of content-based recommendation algorithm later.

In the future, we will conduct more full and comprehensive profile analysis of more posts in the power industry, and conduct more in-depth research on intelligent learning recommendation and auxiliary online examination system design based on the post profile.

Acknowledgment. The authors would like to acknowledge the support provided by the Jiangsu Electric Power Company Technology Project (NO. J2019023).

References

1. Liang, R., Meng, X., Zhou, L., Peng, N.: Status quo and prospect of distribution network fault location. *Electric Power Eng. Technol.* **37**(6), 20–27 (2018). (in Chinese)
2. Park, W., Kim, W., Kang, S., Lee, H., Kim, Y.-K.: Personalized digital e-library service using users' profile information. In: Gonzalo, J., Thanos, C., Verdejo, M.F., Carrasco, R.C. (eds.) *ECDL 2006. LNCS*, vol. 4172, pp. 528–531. Springer, Heidelberg (2006). https://doi.org/10.1007/11863878_60
3. Rimitha, S.R., Abburu, V., Kiranmai, A., Chandrasekaran, K.: Ontologies to model user profiles in personalized job recommendation. In: 2018 IEEE Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Mangalore (Mangaluru), India, pp. 98–103 (2018)
4. Dayane, C.M.F.C., Ronaldo, C.M.C., et al: Data mining on LinkedIn data to define professional profile via MinerSkill methodology. In: 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, pp. 1–6 (2017)
5. Ibrahim, M.E., Yang, Y., Ndzi, D., et al.: Ontology-based personalized course recommendation framework. *IEEE Access* **7**, 5180–5199 (2018)
6. Linden, G., Smith, B., York, J.: Amazon.com recommendations: item-to-item collaborative filtering. *IEEE Internet Comput.* **7**(1), 76–80 (2003)
7. Yang, W., Wang, Z., You, M.: An improved collaborative filtering method for recommendations' generation (2004)
8. Sarwar, B., Karypis, G., Konstan, J., et al.: Item-based collaborative filtering recommendation algorithms. In: Proceedings of the 10th International Conference on World Wide Web, pp. 285–295 (2001)
9. Lee, Y.: Recommendation system using collaborative filtering. M.S. thesis, Dept. Comput. Sci., San Jose State Univ., San Jose, CA, USA, vol. 49 (2015)
10. Jin, X., Mobasher, B.: Using semantic similarity to enhance item-based collaborative filtering. In: Proceedings of the 2nd IASTED International Conference on Information and Knowledge Sharing, pp. 1–6 (2003)

11. Pazzani, M.J., Billsus, D.: Content-based recommendation systems. In: Brusilovsky, P., Kobsa, A., Nejdl, W. (eds.) *The Adaptive Web*. LNCS, vol. 4321, pp. 325–341. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72079-9_10
12. Tarus, J.K., Niu, Z., Mustafa, G.: Knowledge-based recommendation: a review of ontology-based recommender systems for e-learning. *Artif. Intell. Rev.* **50**(1), 21–48 (2017)
13. Chang, P.C., Lin, C.H., Chen, M.H.: A hybrid course recommendation system by integrating collaborative filtering and artificial immune systems. *Algorithms* **9**(3), 47 (2016)
14. Zhang, H., Yang, H., Huang, T., et al.: DBNCF: personalized courses recommendation system based on DBN in MOOC environment. In: *2017 International Symposium on Educational Technology (ISET)*. IEEE (2017)
15. Adomavicius, G., Tuzhilin, A.: Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions. *IEEE Trans. Knowl. Data Eng.* **17**(6), 734–749 (2005)
16. Bobadilla, J., Ortega, F., Hernando, A., Gutiérrez, A.: Recommender systems survey. *Knowl. Syst.* **46**, 109–132 (2013)
17. Amit, S., Sherwein, V., Vijaya, S.D.: Analytical recommendation model using directed graphs for employee and organization. In: *2018 8th International Conference on Intelligent Systems, Modelling and Simulation (ISMS)*, Kuala Lumpur, Malaysia, pp. 84–89 (2018)
18. Akshay, G., Vinay, K.R.K., Karthikeyan, P.: Generating unified candidate skill graph for career path recommendation. In: *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, Singapore, Singapore, pp. 328–333 (2018)
19. Song, S., Qiao, X., Bu, Q., Song, L., Gao, L.: Research on the technical scheme of outdoor-layout relay protection in smart substation. *Electric Power Eng. Technol.* **37**(02), 83–88 (2018). (in Chinese)
20. Hou, X., Wang, B., Liu, W., Zhou, J.: Approach of relay protection setting remote operation based on operating files. *Electric Power Eng. Technol.* **37**(01), 147–152 (2018). (in Chinese)
21. Zou, D., Chen, G., Xu, X., Zhao, Y.: Architecture design of automatic voltage control system for active distribution network. *Electric Power Eng. Technol.* **38**(04), 42–47 (2019). (in Chinese)
22. Thomas, R., Jun, W.: TF-IDF uncovered: a study of theories and probabilities. In: *Proceedings of the 31st Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR 2008)*, pp. 435–442. ACM, New York (2008)



Safety Analysis of Communication-Based Train Control System by STPA and Colored Petri Net

Qian Xu and Junting Lin^(✉)

Lanzhou Jiaotong University, Lanzhou, Gansu, China
linjt@mail.lzjtu.cn

Abstract. The conventional safety analysis methods were caught in a dilemma with analyzing the functions and the close component interactions of the complicated system. On the contrary, the System Theory Process Analysis (STPA) regards the system as a hierarchical control structure instead of the separate components, which helps to explore the control flaws. Thus, it provides an optimized solution for the safety analysis of Communication based Train Control (CBTC) systems that are commonly-used in urban railway transit. Colored Petri Net (CPN), a widely-used formal language, can avoid the potential ambiguity caused by the block diagram of the classic STPA and make models executable and more rigorous. The main contributions of the paper are carried out. Firstly, the general process of the integrated method and its formal definition are clarified. Secondly, the block diagram is put forward to build the three-layer CPN models of CBTC. Then the models are checked by ASK-CTL (Computer Tree Logic) queries. In addition, the XML document from CPN is utilized to achieve the automatic search for the hazard and the reachable path to reveal the unsafe control behaviors, the refined safety constraints and control flaws. For the purpose of the feasibility and the superiority of the proposed method, the results is compared to the Fault Tree in terms of “train overspeed” hazard and 20 flaws in the paper are more than 11 from the reference.

Keywords: Colored Petri Net · Control flaws · Hazard identification · Hierarchical control structure · System Theory Process Analysis

1 Introduction

Communication-based Train Control (CBTC) system is prevalent in the modern urban rail transit, which is no longer a simple combination of various signal facilities but a complete and hierarchical distributed signaling system embodies the functions like the safety protection, the speed control and the information feedback. The functional modules of CBTC system interact independently and simultaneously to form a complex network where a large number of concurrent, conflicts and competitive behaviors take place. Scientific safety analysis methods for the increasingly complex system is significant to ensure the operational safety.

Preliminary Hazard Analysis (PHA) is a basic method to identify the hazards of the systems, which was recommended in ref. [1]. However, it might not be adequate to handle the hazard analysis for great complex systems according to ref. [2]. Ref. [3] recorded the special safety study with HAZOP (Hazard and operability analysis) to identify the potential hazards arising from the operational scenarios in the ETCS-2. However, due to the lack of a prescribed way to present systems, the system representation models to be analyzed in HAZOP process are different.

Leveson proposed the System-Theoretic Process Analysis (STPA) [4] based on her former theory named as STAMP (Systems-Theoretic Accident Model and Processes) [5]. STPA became a new concern of the efficient hazard identification approach for complicated system. However, the inadequate expressive ability in the general form of the control structure is obvious. The analytical process and outcomes are almost textual description, which is lack of readability and portability. In ref. [6], formal method is used to extend the classic STPA. The extended UML model is established and verified by PHAVer. The reachable set is used to analyze the model to identify the factors causing inadequate control. However, the analysts should be familiar with the system and have rich practical experience. In ref. [7], it presents a method for combining STPA and the model checking by UPPAAL, where a robotic flight simulator is presented as a case study. The STPA hazard identification based on formalization model (BFM-STPA) is proposed in ref. [8], which combines STPA with Colored Petri net (CPN) to establish the control structure models in China Train Control System-Level 3 (CTCS-3) and the identified hazards is generated into hazard logs. Temporary Speed Restriction (TSR) issued scenario is the case study in ref. [8]. But once the model is more detailed and complex, state space explosion occurs that the reachability from the state space reachability graph(SSG) may be invalid. In addition, the model in ref. [8] simply follows the TSR information flow, making it less possible to be reused for other motivations.

Inspired by ref. [7, 8], STPA with the formal method can provide an unambiguous representation of the system under analysis and the hazards can be identified by STPA. The tack is gaining acceptance. Colored Petri Net, a mature formal method in the industrial field, is an advanced Petri net with classification, hierarchy and data structure. It possesses an intuitive graphical representation with the mathematical definitions and detailed grammatical semantics by “coloring” the elements of the same features. CPN-Tools developed by the University of Aarhus (Denmark), a tool for editing, simulation, and analysis of colored Petri nets, is integrated with Meta Language (ML), ASK-CTL (Computer Tree Logic) toolkit, monitor and state space calculator to provide a more user-friendly interface and more convenient operation. Above all, STPA with CPN can be a potential approach in safety analysis of CBTC.

The rest parts of the paper are organized as follows. In Sect. 2, the preliminary theory about STPA are explained and how CPN incorporated into the classic STPA is introduced. Additionally, the integrated method’s formal definition by referring the definition CPN is illustrated. Section 3 is in accordance with Sect. 2 and the specific implementation is set. Afterwards, the content follows the guideline to define the system-level hazards and safety constraints, build the block diagram and three-layer CPN models. Due to the focus on the hazard identification of Movement Authority (MA), the subpage Zone Controller (ZC) and the process to generate MA are presented.

Under the guide of the top model, we can also do other further research. Then the model checking by ASK-CTL queries are performed to verify the model's accuracy. Furthermore, by analyzing the MA sequence by XML document, the unsafe control behaviors and the corresponding refined safety constraints are obtained. Finally, the control flaws are produced for further system design.

2 Preliminary Theory of the Integrated Method

This section clarifies the general process of the STPA with CPN and it is on account of the classic STPA theory. It's stressed out that the difference of CPN model is used to construct a hierarchical control structure. The key norms are throughout the paper, like "hazards", "safety constraints", "the hierarchical control structure", "the unsafe control behavior", "the control flow", etc. Moreover, the formal definition of the integrated method is updated by the reference of CPN to depict the mathematical semantics.

2.1 General Procedure of the STPA with CPN

Step 1: System-level hazards and safety constraints should be determined at first. Safety constraints are the safeguards against hazards. In the system design cycle, safety constraints will be refined gradually as well as the sub-constraints will be assigned to the components of the system.

Step 2: A hierarchical control structure diagram is built. In the integrated method, the traditional non-executable block diagram is transformed into executable CPN. The differences are depicted in Fig. 1. The system is regarded as a hierarchical control structure and each layer imposes a safety constraint on its lower layer, that is, the behavior of the lower layer is controlled by high-level constraints. In the classic STPA, the model covers the control structure block diagram, the process model and the control algorithm for describing the control behaviors while the new model contains the top model(*CBTC Hazard Identification page*), the controller model (*Zone Controller page*) and the process model(*MA calculation page*) as Fig. 2 shown. It's noteworthy that the Fig. 2. is also one of the model in Sect. 3.

Step 3: Unsafe control behaviors that led to the hazard are recognized by the cause of hazards and the concrete safety constraints are further developed. The ultimate goal of the safety analysis is to identify the potential hazards so the corresponding measures against hazards shall be taken. The unsafe control behaviors have the four categories:

- (1) The control behaviors required by the safety constraints haven't been implemented or fail to be kept;
- (2) The improper control commands may cause the hazards;
- (3) Issuing the control commands is too late, too early or disordered;
- (4) The control command is finished too fast or too slow.

The above classification is only for reference during the analysis period. Before an accident occurs, the goal of safety analysis is to analyze the hazards cause and to prevent the unexpected occurrence. Therefore, it is necessary to refine the safety constraints to make the system more secure.

Step 4: System’s control flows (the root cause of the hazard) shall be obtained, which are mainly classified into the control logic algorithm flows, the process model flows, the controller cooperation flows, the sensor flows, the actuator flows, and the feedback mechanism flows. The system design’s optimization is bottom on the control flows.

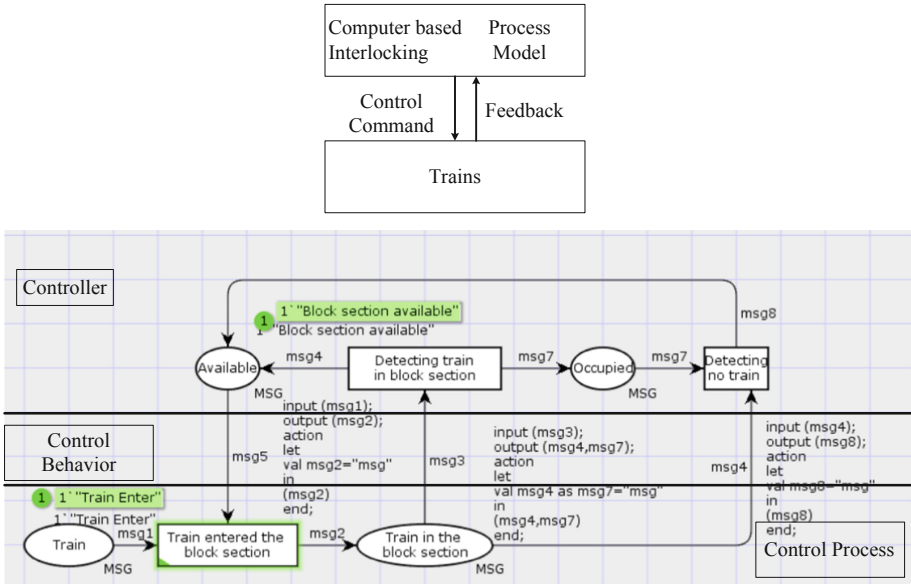


Fig. 1. Control Structure (Above: non-executable block diagram; Below: executable CPN)

- ▼CBTC Hazard Identification
 - ▼Automatic Train Supervision
 - Draft TSR to be Verified
 - ▼Data Storage Unit
 - Issue TSR
 - ▼Vehicle on Board Control
 - Information Transmission Process
 - ▼Computer Based Interlocking
 - Route Build Process
 - ▼Driver
 - Driver Operation Process
 - ▼Zone Controller
 - MA Calculation

Fig. 2. Declarations of the top model, the controller model and the process model

2.2 Formal Definition of the Hierarchical Control Structure

CPN models are formal in the sense that the modelling language has a mathematical definition of syntax and semantics, which can be processed by a software and system properties can be automatically verified. For example, it verifies that the desired properties have been fulfilled and the undesired properties have been avoided. The formal definition is the basis for the analysis of the various behavior properties. Without the mathematical definition, the sound and powerful CPN wouldn't be developed. Inspired by the CPN formal definition in ref. [9], the model in Sect. 2.2 shall be redefined.

Definition 1. Anon-hierarchical Colored Petri Net is a nine-tuple:

$$CPN = (P, T, A, \sum, V, C, G, E, I) \tag{1}$$

- (1) P is a finite set of places;
- (2) T is a finite set of transitions and $P \cap T = \phi$;
- (3) $A \in P \cap T = P \cap A = \phi$ is a finite set of directed arcs;
- (4) \sum is a finite set of non-empty color sets;
- (5) V is a finite set of typed variables that $Type[v] \in \sum$ for all variables $v \in V$;
- (6) C: $P \rightarrow \sum$ is a color set function that assigns a color set to each place;
- (7) G: $A \rightarrow EXPR_V$ is a guard function that assigns a guard to each transition t such that $Type[E(a)] = C(p)_{MS}$;
- (8) E: $A \rightarrow EXPR_V$ is an arc expression function that assigns an arc expression to each arc a such that $Type[E(a)] = C(p)_{MS}$, where p is the place connected to the arc a; I : $P \rightarrow EXPR_\phi$ is an initialization function that assigns an initialization expression to each place p such that $Type[E(a)] = C(p)_{MS}$.

Definition 2. Hierarchical control structure model is a 9-tuple,

$$I = (PG, \sum P, T, A, N, G, F_S, F_E) \tag{2}$$

- (1) PG is referred to the system operating model page, the controller model page and the process model page;
- (2) \sum includes the state and message type;
- (3) $P = (P_M, P_C, P_P)$, P_M, P_C, P_P is the place in the operating/controller/process model page, respectively;
- (4) $T = T_1 \cup T_2$, the state changes is T_1 and substitution transition is T_2 ;
- (5) A is the directed arc;
- (6) N: $A \rightarrow P \times T \cup T \times P$, N is the node function;
- (7) F_S is the function of message transmission and state changes; F_E is the message of arc transmission and expression function of state changes.

3 Construction of CPN Models: An Application in CBTC

Figure 3 is the more specific implementation of the mentioned process in Sect. 2. From Step 1 to Step 2, when the structure diagram is transformed into CPN, the mature experience from the general model checking and formal verification can be utilized via CPN-Tools. For example, the ASK-CTL queries and state space calculation as shown in Step 3. CPN have a powerful ability to describe the asynchronous concurrent systems while ASK-CTL can verify the model and system accuracy. Model checking is an exhaustive search of the state space. Once the state space is too large to exceed the memory space, it will cause the model and all efforts in vain. The hierarchical colored Petri net can reduce the complexity by the “substitution”, which effectively reduce the possibility of a state space explosion. In the most crucial Step 4, the reachability tool is developed by C# programming language, which was inspired by how to generate the test case automatically from formal models in ref. [10].

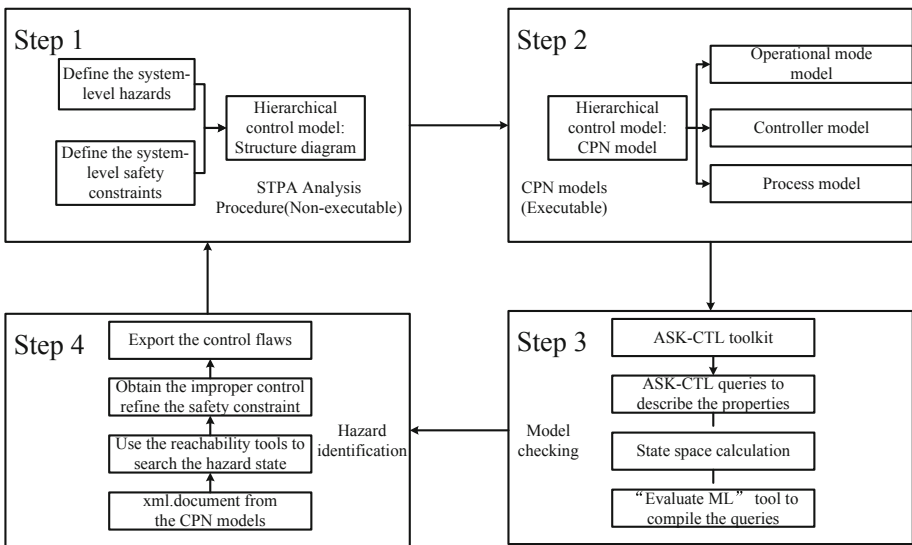


Fig. 3. Implementation procedure of the safety analysis method by STPA and CPN

The case study is about how to construct the sound CPN models of CBTC. Therefore, the following parts are closely prone to the Fig. 3 guideline.

3.1 Define the System-Level Hazard and Safety Constraint

Accidents in railway system mainly consist of “rear end collision”, “head on collision”, “flank collision”, “train to structure collision” and “derailments”, which can be summarized as the accidents caused by the trains overspeeding or overtaking the required distance. Therefore, the system-level hazards are the phenomena of trains exceeding or distance overtaking occur. Accordingly, the safety constraints are how CBTC prevents the trains from exceeding or overtaking as shown in Table 1.

Table 1. System-level hazards and corresponding safety constraints

Hazards	Safety constraints
Trains’ speed has over the speed limited	Overspeeding shall not occurs
Trains’ moving distance has over MA	Over that distance shall be avoided

3.2 Hierarchical Control Model: Structure Diagram and CPN

After familiar with the system structure and functions by ref. [10], a block diagram of hierarchical control structure is established in Fig. 4. The process model shall describe the state of the controller while the variables shall illustrate the message interaction between the components. Models’ structure and variables are necessity for analyzing the causes of the systems’ unsafe control behaviors.

TSR (Temporary Speed Restriction) and Movement Authority (MA) are the most crucial outcomes. “How far and how fast to go” is also determined by MA in the common occasions and is influenced by TSR in the emergency occasions, such as unsolved accidents occur ahead the line. MA is generated by ZC and then is sent to the appointed train while TSR is generated by ATS and is sent to ZC to change the expected MA.

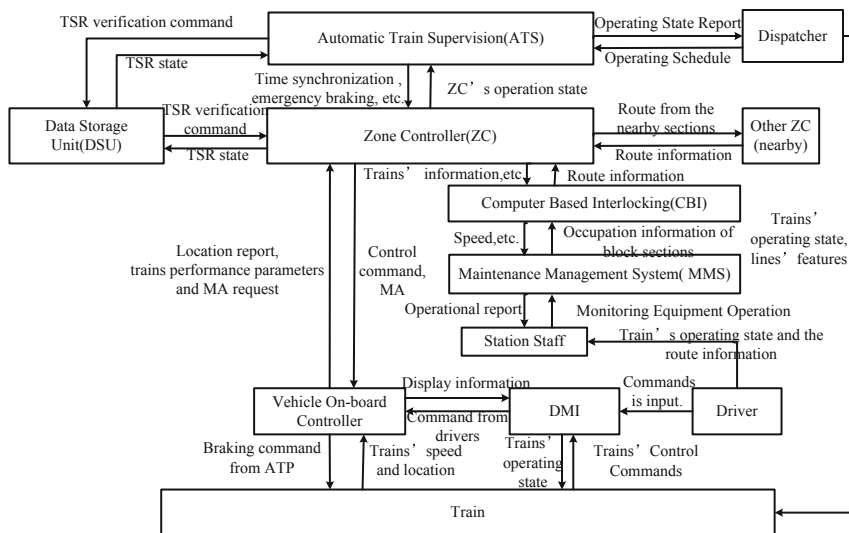


Fig. 4. Structure diagram of CBTC

The hierarchical control structure in Fig. 4 is transformed into CPN models in Fig. 5. The CPN sub-models are used to depict the dynamic behaviors of the system and the specific internal interactions of components. Hierarchical control structures of CPN models conform to the STPA theory. Table 2 illustrates how to transform STPA elements into CPN. Layering can effectively avoid the possibility of state space explosion.

Table 2. Transformation Rules

STPA elements	CPN elements	STPA elements	CPN elements
Control elements	Place	Actuator	Transition/Substitution
Control commands	Arc inscription	Controller	Transition/Substitution
Feedback information	Arc inscription	Decision-making input	Original token

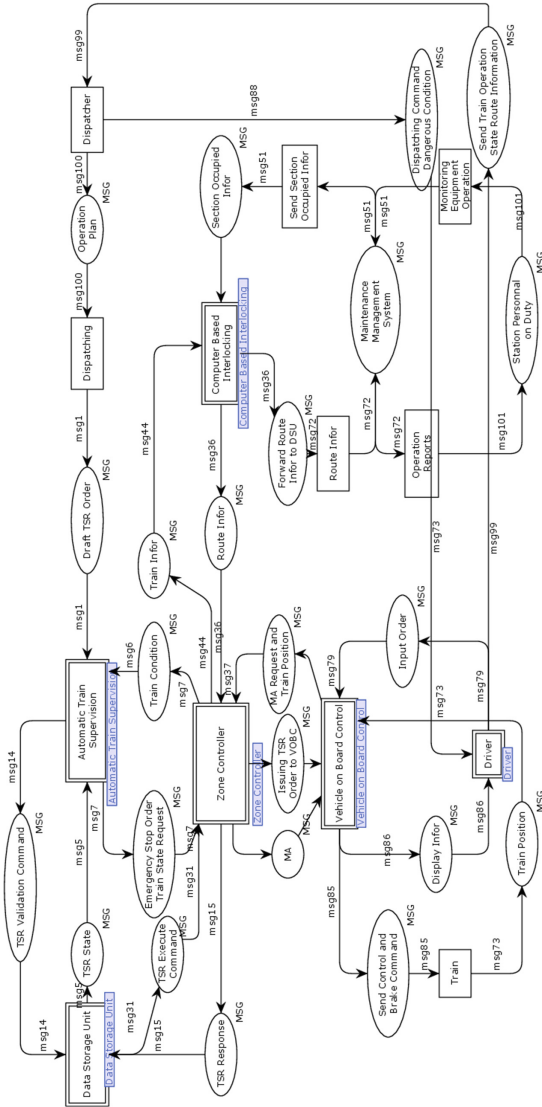


Fig. 5. Top CPN model

The top-down approach is adopted to construct CPN models. The top model describing the system overall structure shall be set up at first. Consequently, the sub-function models of the system are raised, respectively. It's apparent that the top-down modeling idea is closer to the modeler's thinking, therefore, it is more suitable for the functional requirements of CBTC that's why we have taken it. The hierarchical control structure model of CPN is divided into three layers.

- (1) System operating mode model. All controllers in the system should be included as much as possible.

The top model in Fig. 5 includes six controllers, which are the crucial subsystems of CBTC: Automatic Train Supervision (ATS), Zone Controller (ZC), Data Storage Unit (DSU), Computer Based Interlocking (CBI), Vehicle on Board Control (VOBC), Driver according to ref. [11]. Each controller is set to a substitution for further description of the controller process.

CBI is the basis of CBTC operation implementing the safety interlock relations between the switch, the route and the signal. It sends the relevant interlock status to ZC to ensure that the train won't intrude into the unlocked switch or the unavailable lines.

ZC forms an online train operation sequence by receiving the train position report. ZC matches the train position with the line occupancy condition and performs occupancy indication on the line track section of each train safety occupied position. As mentioned, MA is generated by ZC, which is calculated by the train location, the occupancy of the section on the line ahead and the status of the obstacles.

The on-board ATP subsystem or Vehicle on-board control (VOBC) receives the MA from ZC. Emergency Brake Intervention (EBI) is calculated. The real-time difference value between the actual train speed and the EBI speed is monitored. Once the train overspeeds, EBI will be triggered immediately to ensure the train braked safely.

- (2) Controller model.

All controllers are passing the various variables, because they have to constantly interact with the control commands and feedback when the system is operating. ZC is the most crucial ground system and generates the MA. Due to limited space, only the controller model of ZC is presented in Fig. 6.

The essential paths are drawn from Fig. 6:

- ① ZC-CBI (How ZC sends the train information for CBI):
Transition *ZC Host* → Place *Forward Train Infor* → Transition *Send Train Infor* → Place *Train Infor* (the output *Train Infor* actually is the input information for CBI)
- ② CBI-ZC-VOBC (How ZC generate MA):
Input is from the three source: Place *Route Infor*, Place *Emergency stop order and train state request*, Place *MA request and train position* → Transition *Get Relevant Infor* → Place *Send to ZC via wireless communication* → ZC Host
After the process of ZC, the MA is generated with the path: Transition *ZC host* → Place *MA calculation with route information* → Transition *MA calculation* → Place *MA*

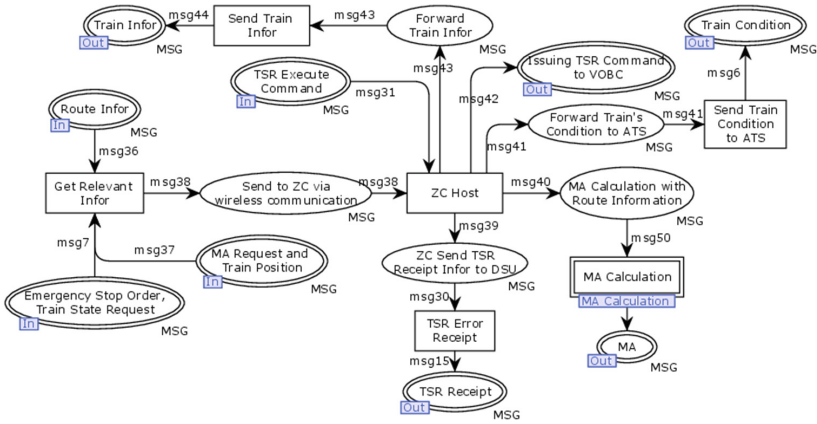


Fig. 6. Controller model of ZC

- ③ ATS-ZC-VOBC (how ZC issue TSR):
Place *TSR execute command* (from ATS) → Transition *ZC Host* → Place *Issuing TSR order to VOBC*. ZC plays a role in transferring TSR from ATS to VOBC (msg31) and making commands implemented (msg42).
- ④ ZC—ATS (Train condition):
Transition *ZC Host* → Place *Forward Train Condition to ATS* → Transition *Send Train Condition to ATS* → Place *Train condition*

(3) Process model.

Figure 7 is used to describe the execution process of the controller (ZC) and the information interaction. The corresponding input information of the controller and the entire processing of the control command execution shall be clarified.

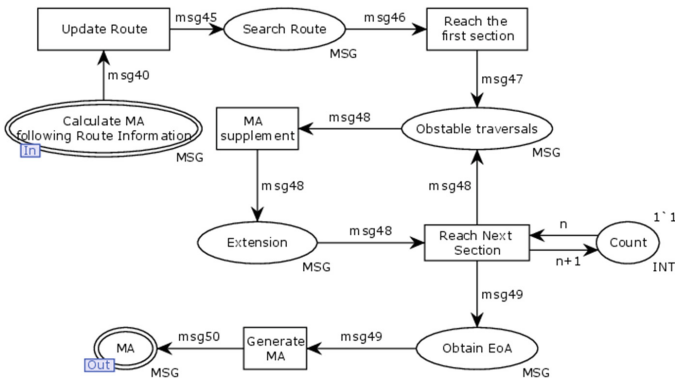


Fig. 7. Process model

Obstacle shall be traversed from far to near to determine the nearest obstacle as the End of Authority (EoA). Additionally, the end of the route is obtained from CBI. Once the current state of the fixed obstacle is consistent with the expected path, the MA extends; otherwise it will be the last obstacle. According to the different scenarios and preliminary calculation of the EoA minimum and taking the safety distance into consideration, the final EoA is obtained. MA is generated in ZC and then transferred to VOBC by wireless network.

The existing train-ground data communication system (DCS) is WLAN (Wireless Local Area Network). Currently, LTE-M (4G for metro) is gradually applied in the new or upgraded lines and is expected to the comprehensive platform for CBTC, PIS (Passenger Information System), CCTV (Closed Circuit Television) transaction, etc. Because the signaling system in railway field is safety-critical system. Once the accident happens, it brings out the inestimable loss for human health and wealth. So the communication mechanism shall not keep in pace with the advanced technique in public network. Instead, the advanced technique needs to be enough mature that can be used in railway field, for example, GSM-R (2G for railway) still the mechanism for CTCS-3 used by China's high-speed railway.

The controller needs to have a good command of the process before implementing the control measures, and that command is named "process model". The control actions of the controller are generated according to the control algorithm and the process model. Only by fully understanding the controller's control algorithm and process model, the analyst can seize the generation principle of the control action and then the accident in the system can be obtained. Therefore, we ought to make efforts to construct the accurate models by model checking to refine the model.

3.3 Model Checking with ASK-CTL Queries

The use of temporal logic for starting and checking verification questions is referred to as model checking, which automatically verifies the consistency of the system model of the formal language description and the systematic nature of the natural language description via a finite state space search. The method has been successfully applied in the related fields, for example the safety communication protocol [11], the development of a practical system [12]. "Evaluate ML" tool and the ASK-CTL queries are required.

(1) Home Properties.

A home marking M_{home} is a marking which can be reached from any reachable marking, which means that it is impossible to have an occurrence sequence starting from M_0 which cannot be extended to reach M_{home} . In other words, we cannot do what will make it impossible to reach M_{home} afterwards according to ref. [9]. From Table 3, the returned results indicate that the "initial marking" of the system is not home, which is satisfied with our expectation. Since the CPN model of the paper is not cyclically executed, "initial marking" will not return to the original state.

Table 3. Verification procedure of “Home Properties”

Queries to verify “Home Properties” and results
<pre>fun IsInitialMarking n=(n=InitNode); val myASKCTLformula=INV(POS(NF("initial marking", IsInitialMarking))); eval_node myASKCTLformula InitNode;</pre>
<p>Results:</p> <pre>val IsInitialMarking=fn: Node->bool val myASKCTLformula =NOT(EXIST_UNTIL(TT,NOT(EXIST_UNTIL(TT,NF("initial marking", fn))))): A val it=false: bool</pre>

The models’ accuracy requires that there is no deadlock and live-lock as far as possible, because the two outcomes may make the system unable to perform the sequence of system behaviors properly.

(2) Self-loop terminal (live-lock)

The live-lock check is to find whether there is a self-looping terminal. We find out from Table 4 that there is no loop terminal proving the system can’t fall into livelock. But there are many dead markings.

Table 4. Verification procedure of “Self-loop terminal”

Queries to verify “Self-loop terminal” and results
<pre>fun SelfLoopTerminal n=(OutNodes(n)=[n]) fun InValidTerminal()=PredNodes(EntireGraph,fn n=>(SelfLoopTerminal n),NoLimit); let val fid=TextIO.openOut"verification results.txt" val _=if InValidTerminal()=[] then TextIO.output(fid,"There is no loop terminal!\n") else TextIO.output(fid,"List of self loop terminals:\n") val _= EvalNodes(InValidTerminal(),fn n=>INT.output(fid,n)) val _= TextIO.output(fid,"List of dead markings:\n") val _=EvalNodes(ListDeadMarkings(),fn n=>INT.output(fid,n)) val _=TextIO.output(fid,"\nNumber of dead markings:") val _=INT.output(fid,length(ListDeadMarkings())) in TextIO.closeOut(fid) end</pre>
<p>Results: There is no loop terminal! List of dead markings: 26494 26493 26492 26491 26490Number of dead markings: 8859</p>

(3) Deadlock marking (dead-lock)

The deadlock analysis process needs to find the deadlock marking of the model.

Table 5. Verification procedure of “deadlock marking”

Queries to verify “dead marking” and results
<pre> fun ValidTerminal n=(Mark.Data_Storage_Unit`TSR_Execute_Command 1 n=["TSR Execute Command"] andalso Mark.Automatic_Train_Supervision`Generate_Command_Text 1 n=["Input Related Parameters"] andalso Mark.Zone_Controller`MA 1 n=["MA"] andalso Mark.Vehide_Based_Train_Control`VOBC_Receive_Relevant_Info 1 n=["VOBC Receive Relevant Info"] andalso Mark.Computer_Based Interlocking`Route_Info 1 n=["Route Info"] andalso Mark.Driver's_Operaciones_Process`Driver_Has_Good_Mental_State 1 n=["Driver Has Good Mental State"]) fun InValidTerminal()=PredNodes(ListDeadMarkings(),fn n=>not(ValidTerminal n),NoLimit); let val file_id=TextIO.openOut"DeadlockMarking.txt" val = if InValidTerminal()=[] then TextIO.output(file_id, "No deadlock markings!\n") else TextIO.output(file_id, "List of deadlock marking:\n") val _=EvalNodes(InValidTerminal(),fn=>INT.output(file_id,n)) in TextIO.closeOut(file_id) end; </pre>
<p>Results: No deadlock markings!</p>

There is no deadlock markings in Table 5, which proves the dead markings in Table 4 didn’t cause serious impact on the model thus they are reasonable.

- (1) Deadlock marking is the reflection of deadlock. In the execution of two or more processes (or threads), a phenomenon of waiting for each other due to competition for resources will not be able to advance without external force.
- (2) Dead marking is the reflection of livelock. Thread 1 and thread 2 can use resources, but they choose the other side to use first causing neither of them can utilize. Threads are always running in vain but the task that the thread itself has to complete has been unable to progress.

3.4 Case Study: Hazard Identification of MA Calculation Scenes

In Sect. 3.2, the Zone Controller (ZC) model has been established to perform Movement Authority (MA) calculation. Relevant method can be found in [13, 14]. Here the process model is stressed out and the hazard sequence abstracted from XML.document is shown in Table 6.

Table 6. Hazard sequence of MA calculation via ZC

Nodes’ ID and explanation
ID1412661512(Calculate MA following Route Information)→
ID 1412669220(Update Route)→ID1412672834(Search Route→
ID1412678007(Reach First Section)→ID 1412681801(Obstacle Traversal)
→ID1412685667(MA supplement) →ID 141268821(Extension) →
ID1412692822(Reach Next Section) →ID1412703616(Obtain EoA)
→ID1412707887(Generate Error MA) →ID1412661506(Error MA)

According to the STPA theory and the hazard sequence information, the possible unsafe control behaviors we have obtained are illustrated in Table 7.

Table 7. Unsafe control behavior of MA calculation via ZC

Command behavior	Provide MA	Provide the shorter MA
“Not Provided” causes hazards	① ZC failed to provide MA to VOBC	④ It is necessary to shorten MA, however, ZC failed to provide the shortened MA to VOBC; ⑤ When an emergency occurs, ZC failed to provide the shortened MA to VOBC;
“Provided” causes hazards	② ZC provide the wrong MA to VOBC	⑥ ZC provided the wrong MA to extend into a train occupation section.
“Error moment or sequence” contributes to the hazards	③ ZC didn’t provide the MA to VOBC timely	⑦ When it is necessary to shorten MA, ZC didn’t provide the shortened MA to VOBC timely;
“Too fast or too short” cause hazards		

Moreover, the refined safety constraint (RSC) are formulated depicted in Table 8 in accordance with the above unsafe control behavior (UCB).

Table 8. RSC with corresponding UCB

RSC Type	Refined safety constraint
MA is requested by VOBC	① ZC shall provide the accurate MA for VOBC ② ZC shall provide the MA for VOBC timely ③ ZC shall provide the emergency stop command
The shorten MA is requested by VOBC	④ ZC shall provide the shorten MA ⑤ ZC shall provide the accurate shorten MA ⑥ ZC shall provide the shorten MA timely

3.5 Control Flows’ Identification of MA

Control Flaws (CF) in the system lead to the emergence of unsafe control behaviors. In other words, the root cause of the system’s hazards are that there are control flow. Hence, according to the unsafe control behavior in Sect. 3.3, the control flaws are investigated as shown in Table 9. In the process of the system design, these control flows shall be paid more attention.

Table 9. Control flow

Types	Control flow
Wireless communication unit (WCU)	① WCU falls into a failure, causing the MA cannot to VOBC; ② It takes too much time for information transmission; ③ Altered MA cannot be sent to the ZC due to WCU failure; ④ The emergency stop message can't be sent to VOBC;
CBI	⑤ The route information for MA generate is improper; ⑥ Line information is not updated in time; ⑦ The shortened route information is not provided to the ZC;
ZC	⑧ ZC's Control algorithm has flaws, producing improper Mas; ⑨ There are errors in the End of Authority (EoA); ⑩ The processing of ZC is too long; ⑪ Because of the control algorithm's error, the system may mistakenly think that it's unnecessary to shorten the MA; ⑫ The emergency condition is taken for normal;
Track circuit	⑬ The track circuit sends incorrect train occupancy information;
VOBC	⑭ VOBC sends the wrong position information to the ZC; ⑮ The train data parameters stored in the VOBC are improper; ⑯ There are errors in the balise information encoding, and the VOBC host parses the wrong train position information; ⑰ VOBC parses out the wrong occupied occupancy information from track circuit; ⑱ VOBC didn't get the newest MA timely; ⑲ There are errors in VOBC's control algorithm.
Driver	⑳ The driver didn't have high safety sense.

The paper compares the analysis results of system-level dangerous train overspeed with the results of fault tree analysis in [14]. The fault tree analysis of train overspeed is qualitatively analyzed by finding the minimum cut set, and the nine minimum cut sets of the train overspeed fault tree are obtained. The resulting risk causes are mainly classified into hardware faults and system errors, line data errors, system internal communication interruptions and communication problems between systems. By contrastive analysis, the new method adopted in this paper is more comprehensive. 20 hazard sources have been identified, which are more than 11 in literature [14]. Besides, it can effectively analyze the hazard related to human factors and most of the hazard sources derived from fault tree analysis only focus on component failure and take the system safety as the reliability of the component.

4 Conclusion

In order to provide a formal and unambiguous representation of the CBTC and identify the hazards by STPA, an integrated method of System Theory Process Analysis with Colored Petri Net is proposed in the paper. The three-layer CPN models help to

substitute the original control structure block diagram in STPA, largely enriching the systematic features that could be modeled before. The application of the method is used to find the potential hazards about MA generation. So the Zone Controller and the process model of MA generation are presented. Afterwards, the ASK-CTL queries are utilized to check the model's accuracy from the "home property", "self-loop terminal" and "deadlock", which prove that the model is correct for further research [15–20]. Then, the hazard sequence is obtained. Unsafe control behaviors of MA calculation can be concluded. Aiming at unsafe control behaviors, the corresponding refined safety constraints are put forward. Lastly, the control flows are found out, which warns the developers and the solution administrators to notice these vulnerability. It can be concluded that the CPN control structure models are able to identify both technical flaws and organizational vulnerabilities. In the future work, it should be emphasized that the CPN models have to involve as many details of system as possible on the basis of the analysis requirement.

Acknowledgement. This work was supported by National Natural Science Foundation of China (No. 61661026, 61841303) and Scientific Research Project of Gansu University of Educational Department (No. 2018A-028).

References

1. CENELEC 50126, Railway Applications: Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) (2017)
2. Ericson, C.A.: Hazard Analysis Techniques for System Safety. Wiley Interscience (2005)
3. ESROG (ERTMS Safety Requirements and Objectives Group), ERTMS Scope, Boundary and Hazards, ESROG-SBH-01, Issue 1 Draft 3 (2000)
4. Leveson, N.: Engineering a Safer World: Systems Thinking Applied to Safety Engineering Systems). MIT Press, Cambridge (2011)
5. Leveson, N.: A New Accident Model for Engineering Safer Systems. *Saf. Sci.* **42**(4), 237–270 (2004)
6. Liu, J., Tang, T.: Functional safety analysis method of CTCS-3 level system based on STPA. *China Railw.* **35**(5), 86–95 (2014). (in Chinese)
7. Dakwat, A.L., Villani, E.: System safety assessment based on STPA and model checking. *Saf. Sci.* **109**, 130–143 (2018)
8. Wang, R., Zheng, W., Liang, C., Tang, T.: An integrated hazard identification method based on the hierarchical Colored Petri Net. *Saf. Sci.* **88**, 166–179 (2016)
9. Jensen, K., Kristensen, L.M.: Coloured Petri Nets — Modeling and Validation of Concurrent Systems. Springer, Heidelberg (2009). <https://doi.org/10.1007/b95112>
10. Gao, C.: Communication Based Train Control System. China Railway Publishing House, Beijing (2018). (in Chinese)
11. Chen, L., Tang, T., Zhao, X., Schnieder, E.: Verification of the safety communication protocol in train control system using Colored Petri Net. *Reliab. Eng. Syst. Saf.* **100**, 8–10 (2012)
12. Song, H., Liu, J., Schnieder, E.: Validation, verification and evaluation of a train to train distance measurement system by means of Colored Petri Nets. *Reliab. Eng. Syst. Saf.* **164**, 10–23 (2017)

13. Song, H., Tang, T., Li, K.: Reachability analysis of timed automata based on XML in RBC subsystem. *Railw. Comput. Appl.* **23**(6), 10–15 (2014). (in Chinese)
14. Lv, J., Zhu, X.: Model-based test case automatic generation of CTCS-3 train control system. *Southwest Jiaotong Univ. J.* **50**(5), 917–927 (2015). (in Chinese)
15. T/CAMET 040104-2018: Urban Rail Transit Interoperability Communication-based Train Control (I-CBTC) system Part4: Hazard Specification. China Railway Publishing House, Beijing (2018). (in Chinese)
16. Song, H., Liu, H., Schnieder, E.: A Train-centric communication-based new movement authority proposal for ETCS-2. *IEEE Trans. Intell. Transp. Syst.* **20**(6), 2328–2338 (2019)
17. Chen, M., Bao, Y.: Survey on formal method of trustworthy construction for communication-based train control systems. *J. Softw.* **28**(5), 1183–1203 (2017). (in Chinese)
18. Wu, D., Schnieder, E.: Scenario-based system design with colored Petri nets: an application to train control systems. *Softw. Syst. Model.* **17**(1), 295–317 (2018)
19. Zhu, L., Yao, D., Zhao, H.: Reliability analysis of next-generation CBTC data communication systems. *IEEE Trans. Veh. Technol.* **68**(3), 2024–2034 (2019)
20. Song, H., Schnieder, E.: Development and validation of a distance measurement system in metro lines. *IEEE Trans. Intell. Transp. Syst.* **20**(2), 441–456 (2019)



Location and Fusion Algorithm of High-Rise Building Rescue Drill Scene Based on Binocular Vision

Jia Ma and Zhiguo Shi^(✉)

University of Science and Technology Beijing, Beijing 100083, China
szg@ustb.edu.cn

Abstract. In the emergency rescue exercise of high-rise buildings, mastering the accurate position of the participants is an important means for coaches to arrange tactics, evaluate the efficiency of rescue aid, evaluate the effect and ensure the safety of the participants. Video location is a more accurate positioning method, using personnel detection, personnel tracking can lock the position of personnel in the monitoring, but once occlusive, personnel can not be detected, will cause the loss of personnel identity information, another problem is that the current technology is difficult to stably identify the identity of personnel through signs. Therefore, this paper studies the fusion algorithm based on the characteristics that the most widely used WiFi fingerprint location can provide rough position information and personnel identity information. The detection with identity information is obtained by matching the personnel information provided by the WiFi fingerprint location system with the detected personnel in the video. At the same time, the location result of WiFi fingerprint can provide reference position when occlusive for a long time. Aiming at the characteristics of fixed number of participants and fixed identity information in emergency rescue exercise, this paper proposes a personnel tracking algorithm based on appearance and motion characteristics. This algorithm reduces the incidence of identity exchange problem when the personnel are very close, and records the representation information of the participants for a long time, which can make the personnel can be rerecognized after a long period of disappearance, and avoid the problem of matching error caused by multiple matching of WiFi fingerprint information and video location information.

Keywords: Location · Binocular vision · Person detection · Tracking algorithm

1 Introduction

In the emergency rescue, the rescue of high-rise buildings is the most typical. In recent years, with the increase of high-rise buildings, high-rise building accidents bring more and more challenges to rescue, especially high-rise building fires, high-rise building post-earthquake rescue. In the environment of such emergency rescue drill, the high-precision position information of the personnel is required to be used as the reference

basis for the tactical arrangement, the evaluation of the drill effect, and the risk assessment.

At present, multi-use wireless communication mode, including RFID, WiFi Fingerprint, Bluetooth, Ultra-Wideband, etc. [2–4], can be used to meet the indoor positioning needs of most public places. Ultra-Wideband and Bluetooth are the most accurate methods, while RFID and WiFi Fingerprints [5] are the second. However, Ultra-Wideband positioning needs expensive devices, Bluetooth needs to replace Bluetooth label batteries regularly, and the maintenance cost is very high. WiFi, as the most commonly used wireless signal in daily life, has wide coverage and cheap equipment layout, but if used as an emergency rescue exercise, it is not accurate enough.

With the development of artificial intelligence technology, target recognition for image has been widely used. Image recognition technology can be used to calibrate the position of people in the graph directly, so as to carry out accurate positioning. However, image recognition is difficult to accurately identify people in a wide range of areas, so the calibrated personnel position can not correspond to the actual personnel identity. In this paper, a fixed scene target location method based on multi-view video image is proposed. Later, the research status, the transformation from image coordinates to real coordinates, how to obtain the identity of the detected target, and how to achieve stable video location will be carried out.

2 Related Work

2.1 Indoor Positioning Theory Based on WiFi

WiFi is one of the most common wireless signals in daily life. It generally follows IEEE 802.11b/g/n protocol and works at a frequency of 2.4 GHz. Each WiFi signal is sent by a wireless ap (access point), often a wireless router. Each wireless ap has its own unique global code, that is, mac address, and generally these ap do not move frequently. WiFi fingerprint location is a convenient and accurate indoor location method.

Using WiFi fingerprinting method to locate is divided into two stages, the first stage is the collection of WiFi fingerprints in a certain area. The so-called WiFi fingerprint refers to a set of key value pairs composed of a group of RSSI from AP and the corresponding real coordinates collected by the terminal at a certain point. This associates the signal strength with the location. The collected fingerprint information is then stored in the database, and each set of fingerprints is unique. In general, the points we collect are not random, and the coordinate system is built with a certain point as the origin, so that the coordinates of each point can be obtained. With the increase of the density of acquisition points, the accuracy of positioning will also increase accordingly, but there will also be certain upper limit. When RSSI near several points are very similar or even overlapping, the increase of acquisition points will not increase the accuracy.

In the process of collecting RSSI, the signal strength of each ap is time-varying, but the whole fluctuates around a range, and we need to collect and average it many times at one point as the estimated value of RSSI at a certain point.

The second phase is the positioning phase. Locate the terminal to a certain location in the area. The RSSI, of ap collected by the terminal is compared with the WiFi fingerprint in the database at the same time to find the closest several fingerprints. Here are two ways, one is the minimum distance, including the Euclidean distance, the Manhattan distance, the Mahalanobis distance, or the maximum similarity, including the cosine similarity, the Spearman similarity, and so on. The most commonly used cosine similarity is used in this paper.

2.2 Pedestrian Detection Method

At present, pedestrian detection methods are mainly divided into three categories, one is based on motion detection, the second is mainly based on machine learning, and the third is deep learning. Among them, based on motion detection such as Gaussian mixture model, frame difference method, vibe algorithm [6, 7] and so on, the idea of these background modeling algorithms is to get a background model through the previous frame learning, and then compare the current frame with the background model to get the moving target. These algorithms are simple to implement and fast to implement, but these algorithms only use pixel-level information and do not make use of the high-level semantics of the image, so the following problems exist: they can only detect moving targets; they are greatly affected by light; if multiple target adhesions can not be dealt with; they are vulnerable to bad weather and so on. The machine learning algorithm and the depth learning algorithm improve the above problems from the advanced semantics of the image.

Navneet Dalal proposed a pedestrian detection algorithm based on hog SVM on 2005 CVPR [8]. HOG (directional gradient histogram) feature is a feature operator used for object detection in computer vision and image processing. HOG uses the gradient histogram of the local region to form the feature by calculating and counting the gradient histogram of the local region, which makes use of the orientation and intensity information of the edge. The method of HOG is to calculate the gradient of fixed size picture, then divide the picture into grid points, then calculate the gradient orientation and intensity of each grid point, then form the gradient direction distribution histogram of all pixels in the grid, and finally summarize the whole histogram feature. This feature describes the shape and appearance information of pedestrians, and is insensitive to light changes and small spatial translation.

In view of the fact that HOG features only focus on edge and shape information, and it is difficult to deal with occlusion and sensitive forehead problems, some researchers have proposed the integral channel feature (ICF) [9]. The integral channel features include 10 channels: gradient histogram in 6 directions, 3 luv color channels, and a gradient amplitude. By combining ICF with AdaBoost, the author carries out cascade classification training. Instead of zooming the picture to a fixed size, he designed several common scale classifiers. For pedestrians of other sizes, the prediction results of typical classifiers were used to approximate the difference, and the accuracy was higher than that of direct image scaling.

In order to solve the problem of occlusion, a method (DMP) [10] for the detection of parts is proposed, and the human body is divided into the parts such as the head, the trunk, the limbs and other components. These parts are detected respectively, and the detected results are combined. DMP includes two parts: root model and component model. The root model (Root-Filter) is mainly aimed at the potential region of the object to obtain the position of the possible object, but whether there is really the desired object needs to be further confirmed after the calculation combined with the component model (Part-Filter). In addition, DMP algorithm also uses Latent-SVM classifiers with strong discrimination ability, which makes it achieve good results in human body detection.

Methods such as Faster-RCNN, SSD, Yolo, FPN [11, 12], etc., in the field of depth learning can be used to detect pedestrians, whose accuracy is significantly higher than the SVM and Adaboost classifier. But because the scene illumination in the training set is monotonous, the target in the figure is relatively sparse, and the problem of occlusion and lighting in the pedestrian detection can not be well processed. The Liliang zhang's team improved [13] the Faster-RCNN, only reserved the RPN network for candidate area extraction, and changed the classification network into a random forest, which improved the problem that the CNN network is too sparse for small target extraction features. In addition DMP method is also used, so they get a good effect.

The Institute of Artificial Intelligence of the Origin of the United Arab Emirates (UAE) proposed a detection idea without anchor frame [14], which directly convolution the picture without sliding window to predict the center point and scale of the target. They achieved a very good results.

2.3 Multi-target Tracking Based on Personnel Detection

Personnel tracking algorithm is an effective means to improve the efficiency of personnel detection and reduce the false detection rate in video. In this paper, multi-target tracking is mainly studied, occlusion is still one of the difficulties to be solved in this field. At present, the method of deep learning has gradually surpassed the probability method and machine learning method in this field, and has become the mainstream of research.

Bergmann et al. proposed to convert the target detector into a tracker, and use rerecognition and motion prediction to complete the tracking task. In this method, the boundary box regression of the object detector is used to predict the new position of the object in the next frame, and the new position of the object in the next frame is extended by simple re-recognition and camera motion compensation [15]. Due to the limited effect of pedestrian recognition in scenes with a large number of people, the tracking effect of this model in more complex scenes is poor.

On the basis of sort algorithm, Nicolai et al. proposed that Deep Sort, applies the idea of Cascade Matching to the matching of multi-target tracking, which effectively reduces the probability of target identity switching when occlusion occurs [16]. Although this method also uses the advanced semantics of the image and the motion information of the target, the image feature extraction network is too simple, resulting in the extracted features sometimes can not be used to determine whether the detection

target is the object you want to track. This paper will improve this method based on the existing scenarios.

SenseTime Technology proposes a multi-target tracking framework which can capture long-term and short-term clues. The switching perception separator in data association is used to improve the robustness of identity switching matching in multi-target tracking. At the same time, a simple but effective method is introduced to retrieve potential classifiers [17].

In addition, Milan et al. proposed a novel multi-class multi-target tracking (MCMOT) framework, which combines detection response and variable point detection (CPD) algorithm to carry out infinite multi-target tracking. The effect of this framework is better than that of the most advanced video tracking technology [18]. Lee uses CNN-based target detector and KLT (Lucas-Kanede Tracker)-based motion detector to calculate the likelihood probability of the foreground as the detection response of different categories of targets [19].

2.4 Projection of Image Coordinates to World Coordinates

In order to locate the target in the image, it is necessary to convert the image coordinates of pedestrians in the image to the real coordinates. In this paper, the stereo matching algorithm of binocular camera is used to solve this problem.

In general, the binocular camera is a wide-angle lens, the imaging is distorted, and the imaging surface of the two cameras may not be coplanar, which causes interference to the subsequent stereo matching. The camera needs to be calibrated before the stereo matching algorithm is carried out. The calibration is divided into two parts, namely the calibration of the single camera and the calibration of the double camera [20].

In this paper, Zhang Zhengyou calibration algorithm is used to calibrate a single camera: multiple groups of chessboard lattice maps are taken, corner detection and sub-pixel information extraction are carried out by OpenCV library function. Using this information, the internal parameter matrix M and distortion matrix J of the camera, as well as the rotation matrix R and the shift matrix T of each image can be obtained. Through multiple iterations, more accurate M and J can be obtained, and they can be input into the corresponding camera correction function as parameters, and the calibration of the single camera can be completed.

Binocular calibration is based on the calibration of monocular camera. In addition to obtaining the internal parameter matrix and distortion coefficient matrix, the additional parameters that need to be calibrated are eigenmatrix E , basic matrix F , rotation matrix R and shift matrix T . The R and T of the binocular camera can be calculated by the following formula:

$$\begin{cases} R = R_r R_l^T \\ T = T_r - R_r R_l^T T_l \end{cases} \quad (1)$$

R_r and R_l are the rotation matrices of the right camera and the left camera, respectively, and T_r and T_l are the translation matrices of the right camera and the left camera, respectively.

The intrinsic matrix E and the basic matrix F of the corresponding binocular camera can be obtained by bringing the inner parameter matrix M and the distortion matrix J of the single camera and the whole rotation matrix R and the translation matrix R into the library function, and then the E and F are brought into the library function to realize the calibration of the binocular camera.

There is the following relationship between image coordinates and world coordinates:

$$Z_w = \frac{bf_x}{d} \quad (2)$$

$$X_w = \frac{b(u-u_0)}{d} \quad (3)$$

$$Y_w = \frac{b(v-v_0)}{d} \quad (4)$$

Where (Z_w, X_w, Y_w) represents the world coordinates of a certain point, (u, v) represents its image coordinates. b represents the distance between the two cameras' center of light, and d represents parallax. Among them, b can be obtained by measurement, and the parallax d can be obtained by *SGBM* algorithm, so that the image coordinates of people in video can be transformed into the real world coordinates.

3 Rescue Scene Location Algorithm Based on WiFi Location and Video Image Location

3.1 The Overall Framework of Video Image Location Algorithm

The video image, as the carrier of the target, carries the identity information and the position information of the target, in particular the position information which has a considerable accuracy. However, when there are many people in the image, the method of target recognition cannot accurately distinguish the different people's identity, and the simple position information is not worth. So that We use the combination of WiFi fingerprint and video image location for fusion localization. The WiFi fingerprint positioning devices are easy to be arranged, and can provide the characteristics of the double information of the person's identity and position, but the accuracy of the location information provided is not high. If we combine the WiFi fingerprint positioning with the video image location, give full play to the image positioning accuracy and the characteristic that the WiFi fingerprint positioning has the identity information, the indoor positioning accuracy of the two technologies will be further improved [21, 22].

The following steps are required for the location of people in a video image:

- (1) Detection: obtain size and position of all personnel in a frame, which is represented by a box;
- (2) Obtaining the pixel coordinates which around feet of each identified pedestrian;
- (3) Convert the coordinates of pixels in the image to the coordinates in the real world.

After these three steps, you can get the actual location of everyone in the video (Fig. 1).

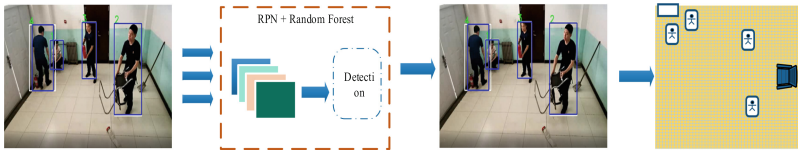


Fig. 1. Flow chart of video image location

While identifying and obtaining pedestrian location, a timestamp is recorded, and the positioning results of WiFi fingerprints for indoor personnel are obtained from the database. The video location results and WiFi location results are matched one by one according to the similarity of them, so that the pedestrians in the video can obtain the identity information in the WiFi fingerprint location results.

In the practical application, due to the existence of the reasons such as occlusion and light change, the detection link of the pedestrian often has missed detection and false detection, resulting in the failure of the association between the video positioning information and the WiFi fingerprint positioning information. To this end, the above problems will be improved by using the target tracking algorithm (Fig. 2).

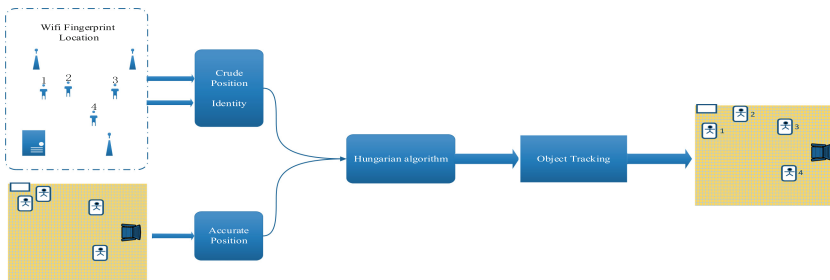


Fig. 2. Block diagram of WiFi fingerprint and video stream fusion localization algorithm

3.2 Fusion of Multi-target Position Information

The position coordinates of the target in reality can be obtained by using WiFi fingerprint, and the coordinates of the target in reality can be obtained by video image. However, the target obtained by image is only location information, there is no identity information, the information obtained by WiFi has both location information and identity information, but the location information is not accurate. If the two can be correlated with each other, a fusion positioning system with both identity information and accurate location information can be generated.

For the multi-objective association problem of matching multi-person WiFi information and image information in a fixed scene, it can be regarded as an assignment problem, that is, assuming that there are m tasks, m personnel, each person gets a task, and solve the problem of minimizing. In this problem, WiFi produces n personnel information, and the image recognizes the corresponding n personnel information, but in practical application, sometimes the image will produce missed detection or false detection, resulting in the resulting personnel information greater than or less than n , which is beyond the scope of the traditional assignment problem.

The Hungarian method is a very good method for the traditional assignment problem. Its basic idea is to change the original value coefficient matrix into a new value matrix with many 0 elements through certain operations, while maintaining the optimal solution of the original problem. In this paper, we use the extended Hungarian algorithm to increase the number of virtual elements to supplement the number of people when the information generated by the video image is not enough to solve the problem that the information generated by the video image may be different from that of the WiFi information.

In the video image detection, it is assumed that n detection results are obtained, and it is recorded as follows:

$$IP_i = x_i, y_i; i = 1, 2, \dots, n \tag{5}$$

At the same time, WiFi also located m test results, which are as follows:

$$RP_j = x_j, y_j, z_j; j = 1, 2, \dots, m \tag{6}$$

The matrix P is constructed, and its dimension is $n \times m$, matrix represents the Euclidean distance between the WiFi detection results and the video image detection results.

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nm} \end{pmatrix} \tag{7}$$

Among them, the calculation formula of each element is obtained by the following formula:

$$p_{ij} = IP_i - RP_j \tag{8}$$

In the actual calculation, use the matrix of $L_{d \times d}$, $d = \max(n, m)$. For elements with dimensions greater than n rows and m columns in L are set to 0, and the other elements are the same as in matrix P . After the coefficient matrix is constructed, it can be solved according to the Hungarian algorithm. The results of the solution can be divided into the following cases:

For each pair that matches successfully (IP_i, RP_j), the result of IP_i is used as the final location result, and the identity information carried by RP_j is used as the final fusion identity information.

For the matching result, RP_j has no matching object, that is, $n < m$, then the positioning result of RP_j is used as the positioning result of the target.

If IP does not have a matching object in the matching result, it is considered to be an image recognition error, because WiFi location contains all the personnel information, and more personnel information appears, it is an error. Ignore IP that does not match.

After this calculation, we can get m location results with identity:

$$P_j = \begin{cases} (x_i, y_i, z_j) & \text{If } IP_i \text{ matches } RP_j \text{ successfully} \\ (x_j, y_j, z_j) & \text{If } IP_i \text{ matches } RP_j \text{ unsuccessfully} \end{cases} \quad j = 1, 2..m \quad (9)$$

Through the above steps, the position information of all the people in one frame is obtained, and the continuous target movement information can be obtained by frame detection. However, due to the inaccurate location of WiFi and the instability of video detection, the matching error occurs, which affects the stability of matching.

3.3 Information Fusion Location Algorithm Based on Target Tracking

In the process of video detection, due to the existence of occlusion, people out of the camera field of view and other problems, resulting in unstable video pedestrian recognition, which leads to unstable matching between video and WiFi positioning, this paper proposes a combination of target tracking and WiFi positioning algorithm to improve this problem.

The tracking algorithm is divided into the following phases and Fig. 3 shows the flow chart:

- (1) Creation and trajectory prediction for target.
- (2) Matching between detection results and tracking targets.
- (3) using cascade matching to solve the problem of target identity exchange when occlusion occurs.
- (4) IOU matching is used again for detection objects and tracking targets that do not match successfully after cascade matching.

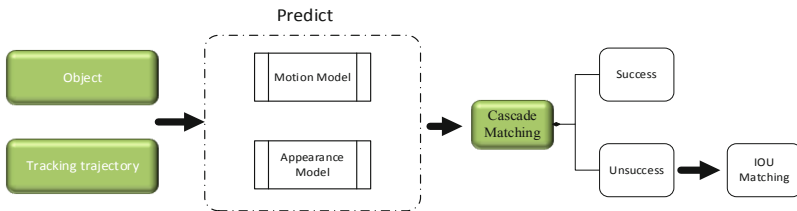


Fig. 3. The algorithm flow chart of target tracking.

First of all, introduce the measurement method of association. We detect a frame in the video, and the detected target is selected by using the anchor box (bounding box), and the format of the description anchor box is $(u, v, r, h, \dot{x}, \dot{y}, \dot{r}, \dot{h})$. (u, v, r, h) indicates the position and size of the anchor frame, $(\dot{x}, \dot{y}, \dot{r}, \dot{h})$ is the coordinate of the center of the anchor frame, \dot{r} is the ratio of the length to width of the anchor frame, and \dot{h} is the left length of the anchor frame. $(\dot{x}, \dot{y}, \dot{r}, \dot{h})$ represents the velocity information of each variable in (u, v, r, h) described in the image. We first use Kalman filter algorithm to predict the position of the detected anchor frame, where the pedestrian motion model is assumed to be uniform motion and the observation model is a linear model. The following experiments prove the rationality of the hypothesis. Here, the prediction results are recorded as $d_j = (u, v, r, h)$. Once the target is lost for a long time, this paper sets to more than 20 frames (the setting of this parameter is related to the number of frames taken by the camera and the movement speed of the actual scene), and the WiFi fingerprint system shows that the missing tracker is still in this room, then the positioning result of WiFi fingerprint is used as the basis of the prediction.

The newly detected target is recorded as $d_i = (u, v, r, h)$, and we want the newly detected target to match the predicted result based on the last detection in order to give the newly detected target identity information. The traditional methods to measure the two objectives are Euclidean distance, Pap distance, cosine similarity and Mahalanobis distance. Because of the perspective distortion in the image, the size of the object will change with the far and near angle. Therefore, the metric size of the anchor frame at different distances from the camera is different, and the influence of different metric scales can be effectively eliminated by using the Mahalanobis distance.

$$d_{i,j}^1 = (d_j - d_i)^T S^{-1} (d_j - d_i) \quad i = 1, 2, \dots, n, \quad j = 1, 2, \dots, m \quad (10)$$

Where d_j represents the No. j tracking target determined after the last detection, d_i represents the No. i detection target of the current frame, and $d_{i,j}^1$ represents the Mahalanobis distance between the anchor frame of the previous frame detected target and the current frame detection target.

In addition to the motion model-based metrics, the appearance information contained in the image is also measured. The new Dense block structure is used for the extraction of the appearance model. The structure has the characteristics of less parameters and strong expression. Here the last classification layer is replaced by a convolution layer of $1 * 1$ instead of the full connection, so that the feature vector of the target is obtained. The network structure is as shown in the following table (Table 1):

The network is pre-trained on the large pedestrian detection data set *Person Re – Identification* and contains a total of 1 million parameters. The network runs at 30 ms on NVIDIA GTX1080, meeting the speed requirements of real-time processing.

The appearance extraction network extracts the detected person and outputs a feature vector of a 49-dimension. We compare this feature vector with the feature

Table 1. CNN network structure used in appearance extraction

Name	Patch size/stride	Output size
Conv 1	7 * 7/2	112 × 112
Pooling	3 * 3 max pool/2	56 × 56
Dense block (1)	$\begin{pmatrix} 1 * 1\text{conv} \\ 3 * 3\text{conv} \end{pmatrix} \times 6$	56 × 56
Translation layer (1)	1 * 1conv 2 * 2 averagepool/2	56 × 56 28 × 28
Dense block (2)	$\begin{pmatrix} 1 * 1\text{conv} \\ 3 * 3\text{conv} \end{pmatrix} \times 12$	28 × 28
Translation layer (2)	1 * 1conv 2 * 2 averagepool/2	28 × 28 14 × 14
Dense block (3)	$\begin{pmatrix} 1 * 1\text{conv} \\ 3 * 3\text{conv} \end{pmatrix} \times 24$	64 × 32 × 16
Translation layer (3)	1 * 1conv 2 * 2 averagepool/2	14 × 14 7 × 7
Dense block (4)	$\begin{pmatrix} 1 * 1\text{conv} \\ 3 * 3\text{conv} \end{pmatrix} \times 16$	7 × 7
Conv 2	1 * 1 conv	49 × 1

vector corresponding to the tracking target in the previous frame, and then judge whether they are the same target. The measure method here adopts the cosine similarity, and the calculation formula is as follows:

$$d_{i,j}^2 = \min \left(1 - r_j^T r_k^{(i)} \mid r_k^{(i)} \in R_i \right) \tag{11}$$

Where r_j is the feature vector of the newly detected target, and $r_k^{(i)}$ is the set of k frame eigenvectors of the No. i tracking object in the past. R_i is a collection of all trace objects in the past.

$$R_i = \left\{ r_k^{(i)} \right\}_{K=1}^{L_K} \tag{12}$$

The matching result $d_{i,j}^1$ based on motion information is merged with the matching result $d_{i,j}^2$ based on appearance information, and a new matching result is obtained. The fusion expression is as follows:

$$c_{(i,j)} = \mu d_{i,j}^1 + (1 - \mu) d_{i,j}^2 \tag{13}$$

The following rules are used to detect whether an object becomes a tracking object:

- (1) the appearance of n trackers is detected and recorded by multiple frames before the positioning begins.

- (2) the target is not detected in 100 consecutive frames, and according to the WiFi information, it is determined that the target leaves the current monitoring area to stop matching the tracking target until the WiFi positioning information returns to the current scene.

In the process of target tracking, occlusion will inevitably occur, assuming that when a tracking target a is obscured by target b, it will not be detected by the detector. Because the predicted value of a and b is very close, it is very likely that the detection value of b will be matched with a, resulting in the matching exchange phenomenon (ID switch). For this reason, the cascade matching method is used to match here.

The pseudo code for cascade matching is as follows:

Cascade Matching

Enter: the serial number of the tracking target $T = \{1,2 \dots N\}$, The serial number of the detection target. $D = 1,2 \dots M$

1. Calculation cost matrix $C = [c_{i,j}]$
2. Set up a set M to represent the matched tracking target and the detected target, and initialize it.
3. Create a collection u to indicate that there is no matching successful collection in the detection target and initialize it
4. For n in $(1, \dots Age_{max})$:
5. {
6. Select $T_n (T_n \in T, n \in Age)$ according to the countdown of the order of disappearing tracking targets
7. $x_{i,j} \leftarrow \min_cost_matching\{C, T_n, U\}$
8. $M \leftarrow M \cup \{(i,j) | b_{i,j} \cdot x_{i,j} > 0\}$
9. *end For*
10. return M, U

Algorithm 1. The cascade matching algorithm

After cascade matching, we obtain tracking and detection targets M and U that have been matched successfully and not matched successfully. The U and $(T - T_n)$ are processed by sort mechanism standard. Calculate the IOU between them and using Hungarian algorithm to match. The following results were obtained:

$$P_{IOU} = \begin{cases} (T_i, D_j) \\ T_i \\ D_j \end{cases} \quad i, j = 1, 2..N \tag{14}$$

Among them, P_{IOU} is the result of IOU matching, (T_i, D_j) indicates the successfully matched tracking target and detected target, T_i indicates that there are unmatched tracking targets, and D_j indicates that there are only detected targets in the matching results, most of which are due to false detection.

Because the number of tracking targets can be determined according to the WiFi fingerprint system, it belongs to constant, but the detected people may be occlusive and

disappear, so some tracking may not be able to match the corresponding detection targets after this step. For how to deal with this kind of target will be explained later.

Finally, the Kalman prediction matrix is updated to delete the tracking target that is not in this scene (according to the scene information provided by WiFi fingerprint system). It is expressed as follows:

$$T_{new} = M_T + P_T^{IOU} - WiFi_{state=0} \tag{15}$$

T_{new} represents updated tracking, M_T indicates the tracking of successful matching after cascade matching, P_T^{IOU} indicates the tracking of successfully matching after cascade matching, and $WiFi_{state=0}$ indicates that the personnel information of this scene does not exist in the WiFi fingerprint system.

In addition, we need to update ID (label) of the tracking target and then the tracking of one frame is completed. The beginning of the next frame is still the prediction of the existing target by Kalman filter.

The target tracking can lock the position of the target in the image stably for a period of time, and the position information of the personnel can be accurately determined by the transformation of image coordinates to world coordinates. Two information will be fused below.

Firstly, still using the target position information fusion algorithm proposed in 3.2 to match the detected target of video with the target detected by WiFi fingerprint. The matching results are as follows:

$$P_{matching} = \begin{cases} (x_i, y_i, z_i) & \text{If } IP_i \text{ matches } RP_j \text{ successfully} \\ (x_i, y_i, z_i) & \text{If } IP_i \text{ matches } RP_j \text{ unsuccessfully} \end{cases} \quad j = 1, 2..N$$

Where (x_j, y_j) represents the result of the video localization, (x_j, y_j) represents the result of the WiFi fingerprint positioning, and z_j is the person information carried by the WiFi fingerprint system. At this time, the target in the video has the identity information of the personnel in the WiFi fingerprint system. Next, go to the section that follows the location:

$$P_i^{result} = \begin{cases} P_{track}S_{t-1} = 1, S_t = 1; \\ P_{kalman}S_{t-3} = 1, S_t = 0; \\ P_{WiFi}S_{t-3} = 0, S_t = 0; \\ P_{track}S_{t-1} = 0, S_t = 1; \end{cases} \quad i = 1, 2, \dots, N \tag{16}$$

Among them, P_i^{result} is the result of tracking and positioning, P_{kalman} is the predicted position obtained by Kalman filter according to the previous frame positioning results, and P_{WiFi} is the result of WiFi fingerprint location. In the process of tracking and positioning, occlusion may occur, so that the target can not be detected. Here, S_{t-1} is used to represent the tracking state of target I at the previous time, S_{t-3} represents the tracking state of the first three frames, and S_t represents the tracking state of the current time.

That is to say, in the process of target tracking, if the tracking results are converted to the world coordinates, the accurate position of the target in the room can be easily

obtained. Once the tracking fails in a certain frame, the target information will not be obtained in the video, we will use the Kalman filter to predict the position based information of the previous frame, and the predicted position will be used as the detection result of the lost frame. Because the number of frames taken by the general video surveillance does not exceed 30 frames per second, and the position change of the normal operating personnel usually does not change obviously within 0.1 s, the predicted results are used as the positioning results within 3 frames. If the target is lost for a long time, the prediction results can no longer meet the positioning accuracy, and then switch to the WiFi fingerprint system, using the results of WiFi fingerprint location as the detection value of the current position of the target. Once the target reappears, a new round of identity matching will be carried out on the lost target, the actual identity of the target will be given to the target, and the process of positioning will continue to be followed.

In addition, the problem of identity information exchange is inevitable in the course of target tracking, so that a monitoring threshold is needed between the result of the video positioning of each frame and the positioning result of the WiFi fingerprint. Once the difference between the positioning distance between the two is greater than the threshold value, we will re-matching the target with the problem, and adopt the position of the WiFi fingerprint positioning as predict results before the matching is completed. The setting is as follows:

$$P_i^{result} = \begin{cases} P_i^{result} (P_i^{result} - p_i^{WiFi}) > gate \\ p_i^{WiFi} (P_i^{result} - p_i^{WiFi}) > gate \end{cases} \quad i = 1, 2, \dots, N \quad (17)$$

The p_i^{WiFi} means the location information of the WiFi fingerprint location of the No. i person, left $(P_i^{result} - p_i^{WiFi})$ representing the difference between the image location and the WiFi fingerprint, and the $gate$ represents a threshold value that determines whether a identity needs to be rematched.

4 Experimental Verification

4.1 Experimental Method and Environment Configuration

The experimental system is divided into two parts, one is the location system of WiFi fingerprint: four routers are set up in the four corners of the room, the mobile phone is used as the location label to detect the intensity of WiFi signal, collecting information of signal strength with interval of 1 m, the collected data is stored in the database, and using the Hungarian algorithm to establish the WiFi fingerprint.

The other part is the image acquisition and processing system, which uses a fixed camera to collect the images of personnel in the area, and sends the images to the computer for pedestrian detection, tracking processing and matching processing. The camera adopts wide-angle lens, the computer is configured as i7-6600k, and the video card is GTX1080.

4.2 Experimental Analysis and Related Algorithms

According to the above algorithm flow, we first test the part of personnel detection and tracking, and the test data is a video shot in a fixed space. The main test content is that when the rescue exercise of high-rise building is carried out, the rescue staff produce the influence of various posture and occlusion on the performance of the algorithm. The main concern is the problem of identity exchange (id switch), and the other is the problem of the loss caused by the occlusion.

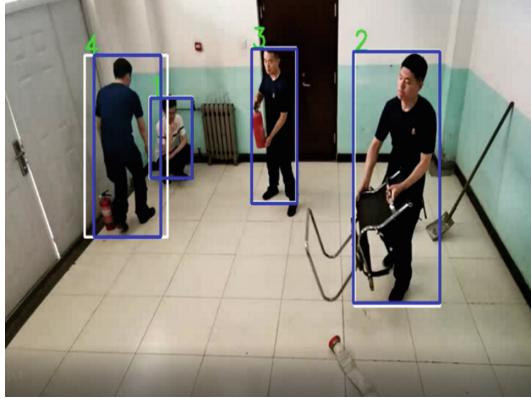


Fig. 4. Results of frame 30 processing

Figure 4 above shows the tracking results of frame 30, with four people in the image, using the label on the anchor box to distinguish the identity information of the four people, the target of No. 1 is the trapped person, and the rest is the rescue personnel. When the algorithm runs, it is good for the recognition of people of all kinds of posture.

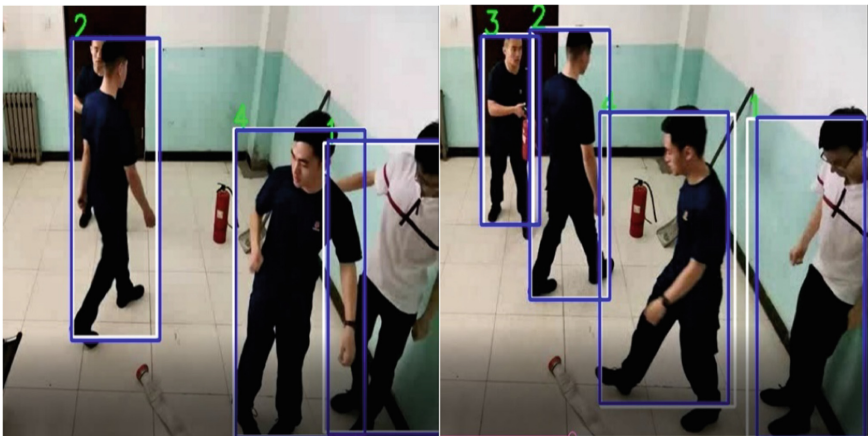


Fig. 5. Results of 90-frame and 95-frame processing when transient occlusion occurs

Figure 5(a) is the detection result of frame 90. It can be found that due to occlusion, the detection box can not select the whole pedestrian accurately. (b) is the result of frame 95 processing. After a brief 0.3 s reappearance of the tracking object, the missing information is quickly retraced.

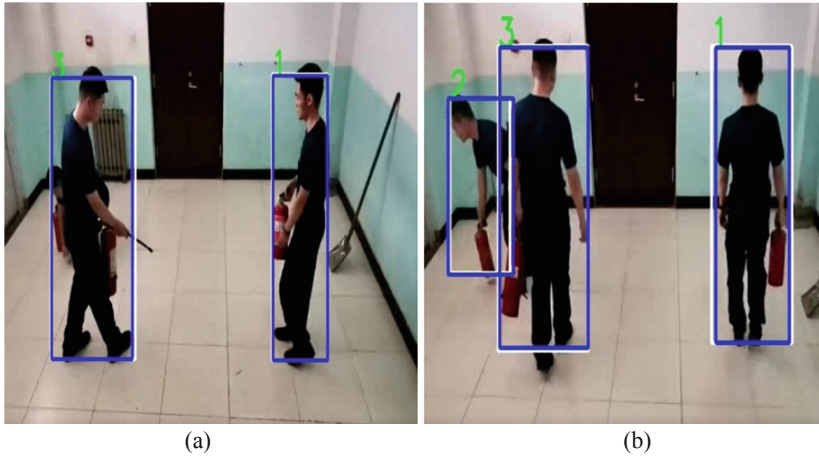


Fig. 6. A case where a long period of severe occlusion takes place

In order to verify the influence of long time occlusion on tracking, we also test the special scene. Ask three rescuers deliberately block each other in the scene. Figure 6(a) shows that person 2 is blocked by person 3, it can be seen that person 2 is almost completely disappeared and cannot be detected. About 3 s after frame 112, person 2 got up and was normally traced. About 3 s after frame 112, personnel 2 got up and was normally traced. It shows that the algorithm has certain ability to deal with the long-term loss of tracking objects in this scene.

In order to show the change of the position of the personnel clearly, the paper chooses the two-person position data to draw the graph. Figure 7 is a graph of the location of the WiFi fingerprint of the two people in the room. In the smaller indoor space, the accuracy of WiFi fingerprint location is not high, we can see that on the one hand, the path in the image is tortuous, on the other hand, the accumulation of sampling points will occur in the place where the inflection point is slow.

Figure 8 is the fusion location result. It can be seen that the curve is smooth, in accordance with the law of motion, and there is no jump phenomenon, which shows that the algorithm has a great improvement on the indoor location results of WiFi fingerprints.

4.3 Algorithm Availability and Performance Analysis

The fusion localization algorithm proposed in this paper is online mode, which is divided into four stages: personnel detection in video, fusion of personnel information

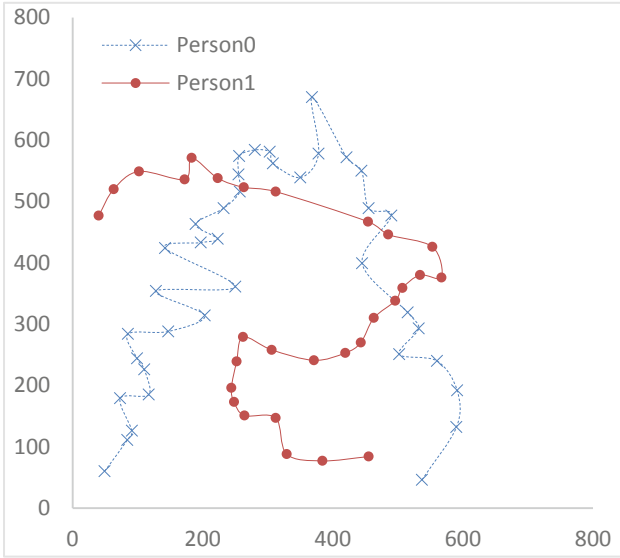


Fig. 7. Results of WiFi fingerprint location

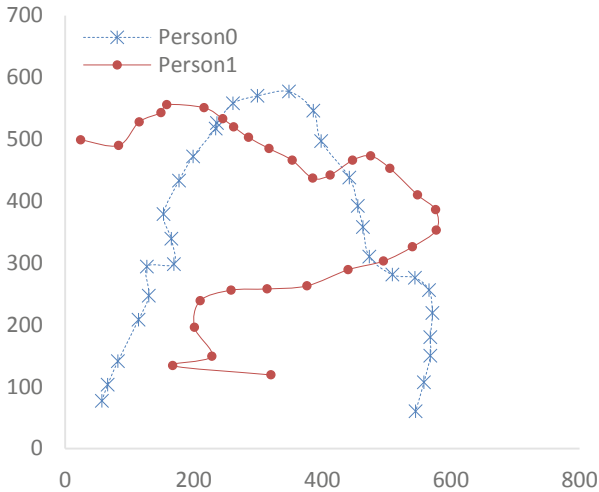


Fig. 8. Results of fusion positioning

and WiFi fingerprint information, video detection and tracking, and WiFi correction of lost targets. Under the experimental conditions, the comprehensive detection speed can reach 20 frames per second. Because the personnel move slowly indoors, in practice, the camera frame rate is adjusted to 15 frames per second, so that the detection speed is basically synchronized with the monitoring video speed. However, too high video frame rate will lead to the lag of detection results and can not achieve online positioning.

The positioning continuity has been analyzed in the above experiment. In addition to the random motion, the paper also carries out the specified route movement to study the accuracy of the positioning, and the following data is obtained through the experiment (Table 2):

Table 2. Error of regular route positioning

Target state	Unobstructed persons	Obstructed person
Average error (m)	0.16 + 10.0	0.25 + 15.0

It can be found that the positioning accuracy of occlusive personnel is much larger than that of unocclusive people, mainly because the positioning accuracy of WiFi fingerprint is lower, once the target is lost for a long time, WiFi fingerprint tracking will be switched, covering for a long time during testing, indirectly simulating the situation when the number of occlusive people is large, in addition, tens of pixels offset may occur when occlusive occurs, and the farther away from the camera. The more serious the deviation, the more serious the deviation.

In this paper, the performance of tracking algorithm in this scene is tested for a long time. The experimental data are 20 m² indoor, 5 segments of video moving around by 4 people, each video length of 1 min, video playback speed of 20 frames per second, a total of 1200 frames per video, a total of 6000 frames and 240000 anchor frames. The comparison with the algorithm in general scenario is as follows (Fig. 9):

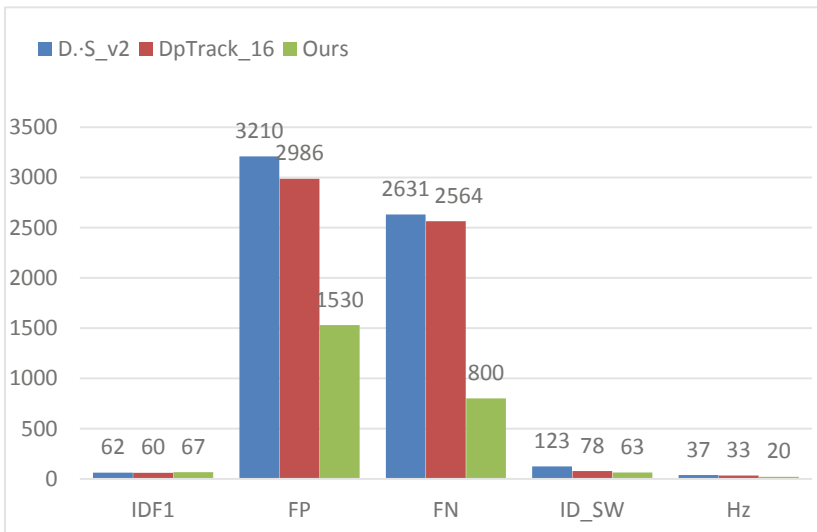


Fig. 9. Performance comparison diagram of personnel tracking algorithm

It can be seen from the above table that the fusion algorithm has good tracking performance in this scene, especially on MT and ML, mainly because of the fixed number of scenes. Once the detected target and the existing tracking do not meet the threshold of motion matching or representation matching, these unmatched targets will be removed from the threshold limit, and according to the distance value between the detected target and the tracking target to run secondary matching. The idea of cascade matching also greatly reduces the probability of target identity exchange. Because the number of people in the overall monitoring is not large, so the omission of tracking is not much, FN gets a good value, but the smooth wall occasionally appears the shadow of people, resulting in new tracking, which brings instability to the tracking part (Table 3).

Table 3. Index comparison results of personnel tracking algorithm

Name	MOTA	IDF1	MT	ML	FP	FN	ID_SW	Hz
D. • S_v2	73.6	62	54%	30%	3210	2631	123	37
DpTrack_16	70.3	60	61%	19%	2986	2564	78	33
Ours	90.5	67	82%	10%	1530	800	63	20

5 Conclusion

Based on the common WiFi equipment and monitoring system, this paper combines the personnel information carried by WiFi fingerprint location with the high precision of image positioning, and the proposed fusion location algorithm can greatly improve the effect of WiFi fingerprint location under the condition of low cost, and meet the needs of high precision positioning of participants in the scene of emergency rescue exercise. Although multi-camera can be used to avoid occlusion to the greatest extent, it is difficult to avoid the problem of poor light in practical applications, especially in darker rooms, the problem of video missed inspectors will be particularly prominent, which also limits the application of this algorithm in more scenes. In the next step of this paper, the research direction of pure image location without WiFi fingerprint will be studied, and the tracking and location of people will be completed by using the advanced semantic features of the characters in the image.

Acknowledgement. This study was supported by State's Key Project of Research and Development Plan (No. 2018YFC0810601, No. 2016YFC0901303). The work was conducted at University of Science and Technology Beijing.

References

1. Wenjuan, L.: The 13th five-year plan for the construction of emergency response system will establish a unified framework of emergency management standard system. *Stand. Eng. Constr.* **2**(5), 99–110 (2017)
2. Polito, S., Biondo, D.: Performance evaluation of active RFID location systems based on RF power measures. In: *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications* (2007)

3. Cruz, O., Ramos, E., Ramírez, M.: 3D indoor location and navigation system based on Bluetooth. In: International Conference on Electrical Communications & Computers (2011)
4. Yu, K., Montillet, J.P., Rabbachin, A.: UWB location and tracking for wireless embedded networks. *Signal Process.* **86**(9), 2153–2171 (2006)
5. Zheng, Y., Wu, C., Liu, Y.: Locating in fingerprint space: wireless indoor localization with little human intervention. In: International Conference on Mobile Computing & Networking (2012)
6. Barnich, O., Van Droogenbroeck, M.: ViBe: a universal background subtraction algorithm for video sequences. *IEEE Trans. Image Process.* **20**(6), 1709–1724 (2011)
7. Hofmann, M., Tiefenbacher, P., Rigoll, G.: Background segmentation with feedback: the pixel-based adaptive segmenter. In: Computer Vision & Pattern Recognition Workshops (2012)
8. Dalal, N., Triggs, B.: Histograms of oriented gradients for human detection. In: IEEE Computer Society Conference on Computer Vision & Pattern Recognition (2005)
9. Vidhyalakshmi, M.K., Poovammal, E.: A survey on face detection and person re-identification. **1**, 283–292 (2016)
10. Leibe, B., Seemann, E., Schiele, B.: Pedestrian detection in crowded scenes. In: IEEE Computer Society Conference on Computer Vision & Pattern Recognition (2005)
11. Li, J., Liang, X., Shen, S.M.: Scale-aware fast R-CNN for pedestrian detection. *IEEE Trans. Multimed.* **PP**(99), 1 (2015)
12. Zhang, L., Lin, L., Liang, X., He, K.: Is faster R-CNN doing well for pedestrian detection? In: Leibe, B., Matas, J., Sebe, N., Welling, M. (eds.) ECCV 2016. LNCS, vol. 9906, pp. 443–457. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-46475-6_28
13. Mao, J., Xiao, T., Jiang, Y.: What can help pedestrian detection? In: Computer Vision & Pattern Recognition (2017)
14. Liu, W., Liao, S., Ren, W.: High-level semantic feature detection: a new perspective for pedestrian detection. [arXiv:1904.02948](https://arxiv.org/abs/1904.02948) [cs.CV]
15. Feng, W., Hu, Z., Wu, W.: Multi-object tracking with multiple cues and switcher-aware classification. [arXiv:1901.06129](https://arxiv.org/abs/1901.06129) [cs.CV]
16. Bergmann, P., Meinhardt, T., Leal-Taixe, L.: Tracking without bells and whistles. [arXiv:1903.05625](https://arxiv.org/abs/1903.05625) [cs.CV]
17. Wojke, N., Bewley, A., Paulus, D.: Simple online and realtime tracking with a deep association metric. [arXiv:1703.07402](https://arxiv.org/abs/1703.07402) [cs.CV]
18. Lee, B., Erdenee, E., Jin, S., Nam, M.Y., Jung, Y.G., Rhee, P.K.: Multi-class multi-object tracking using changing point detection. In: Hua, G., Jégou, H. (eds.) ECCV 2016. LNCS, vol. 9914, pp. 68–83. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-48881-3_6
19. Sawhney, H.S., Kumar, R.: True multi-image alignment and its application to mosaicing and lens distortion correction. In: Conference on Computer Vision & Pattern Recognition (1997)
20. Yoneyama, S., Kikuta, H.: Lens distortion correction for digital image correlation by measuring rigid body displacement. *Opt. Eng.* **45**(2), 409–411 (2006)
21. Miyaki, T., Yamasaki, T., Aizawa, K.: Visual tracking of pedestrians jointly using Wi-Fi location system on distributed camera network. In: 2007 IEEE International Conference on Multimedia and Expo, pp. 1762–1765. IEEE (2007)
22. Rafiee, M.: Improving indoor security surveillance by fusing data from BIM, UWB and Video. Concordia University (2014)



Wear Debris Classification and Quantity and Size Calculation Using Convolutional Neural Network

Hongbing Wang¹, Fei Yuan^{2,3}(✉), Liyuan Gao¹, Rong Huang¹,
and Weishen Wang¹

¹ School of Computer and Communication Engineering,
University of Science and Technology Beijing, Beijing 100083, China

² School of Metallurgical and Ecological Engineering,
University of Science and Technology Beijing, Beijing 100083, China
yuanfei@ustb.edu.cn

³ State Key Laboratory of Advanced Metallurgy,
University of Science and Technology Beijing, Beijing 100083, China

Abstract. The steel production equipment faults are mostly caused by wear faults, and the classification of wear debris in its lubrication system can monitor the wear status of the machine. The traditional methods of wear debris image classification mostly use digital image processing technology by extracting color, shape, texture and other multi-dimensional features of wear debris. It is so difficult to extract suitable multi-dimensional features that the classification accuracy is always kept at a low level. Convolutional Neural Network can directly take the image pixels as input, and extract features automatically, avoiding the poor applicability of manual extraction methods and complicated image pre-processing. An improved lightweight convolutional neural network for wear debris image classification named UstbNet is proposed in this paper. Data augmentation, number and size adjustment of convolution kernels, batch normalization and loss function optimization are used to speed up the model convergence and improve the classification accuracy. The classification accuracy of UstbNet model reaches 96%. After the step of determining the existence of wear debris, we use Faster RCNN to detect the quantity and size of wear debris and further improve it. Grabcut is applied to segment wear debris image based on detected region proposals.

Keywords: Convolutional Neural Network · Wear debris · Classification · Faster RCNN · Grabcut

1 Introduction

Wear debris are the friction particles suspended in the oil of lubrication system, produced by internal friction pair wear of equipment [1]. They carry a great deal of information about the running status of a machine. The state of wear debris can reveal the wear degree and wear mechanism, providing an important reference to improve the working condition of machines such as rolling mill, aircraft engines and marine engines

The original version of this chapter was revised: The values in Table 10 have been modified. The correction to this chapter is available at https://doi.org/10.1007/978-981-15-1922-2_42

[2]. The wear status of a machine can be checked by extracting wear debris information, and different types of wear debris correspond to different faults. In the metallurgical rolling production process, mill gears as a carrier of power and torque transmission, have a direct impact on the normal operation of mechanical systems and rolled steel [3–6]. Abrasion is the main cause of machine failure, and the equipment wear curve is shown in Fig. 1. Common types of wear debris in lubricating oil are shown in Fig. 2. The wear debris generated in the oil film bearing and the corresponding failure are shown in Table 1. The classification of wear debris can reflect the wear condition of the oil film bearing, so as to maintain the oil film bearing in time.

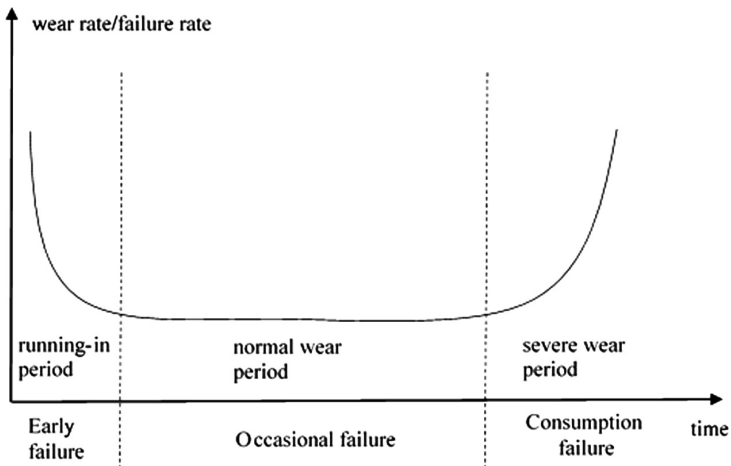


Fig. 1. Equipment wear curve

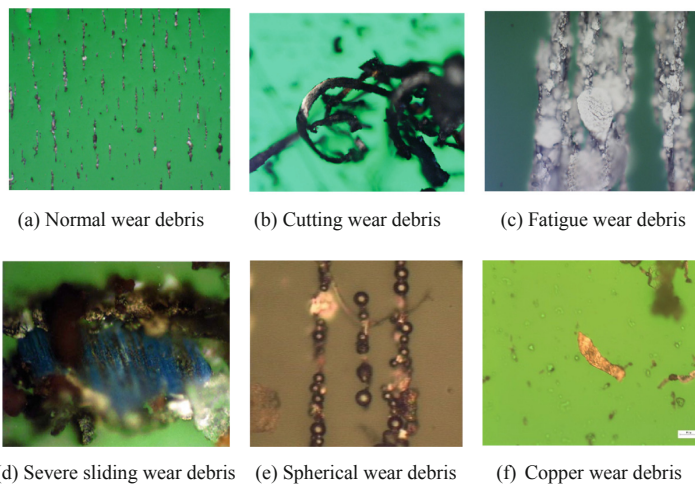


Fig. 2. Typical wear debris

Table 1. Wear debris and their faults in the oil film bearing

Wear debris type	Fault form
Cutting and Black oxide wear debris	Surface friction of bolster bearing
Cutting wear debris of non-ferrous metals	Surface friction of oil film bearing
Fatigue wear debris	Shedding of bushing surface
Severe sliding wear debris	Insufficient lubrication

Wear debris analysis and identification are mainly accomplished by domain experts at early stage, with high cost and a lot of time. In recent years, the rapid development of computer and artificial intelligence have promoted the automatic analysis and recognition of wear debris [7]. Thomas and Stachowiak analyzed the variable scale and fractal features of wear debris [8, 9]. Their researches focus on the digitalization of wear debris features. Roylance pioneered the computer wear debris pattern recognition research direction. He tried to use the grayscale value of different metal wear debris to identify the components, but the classification result is not good [10]. Xu and Luxmoore developed a neural network and expert system integrated interactive automatic identification system for wear debris, but the input features of neural network need to be extracted manually [11]. Zuo compared the application of BP (Back Propagation) neural network, fuzzy BP and gray fixed weight clustering in the recognition of wear debris [12]. Li took ELM (Extreme Learning Machine) as classifier, the shape, color and texture feature of wear debris as input [13]. However, the feature extraction is done manually and the wear debris image needs to be preprocessed.

Many image classification algorithms have been proposed [14–18]. However, the classification of wear debris must be based on multi-dimensional features. Most of the above studies focus on only a few features of color, shape or texture, and the low classification accuracy could be achieved [19–22]. The multi-dimensional feature extraction is difficult by using various conventional and single models. Convolutional Neural Network (CNN) can learn the features from bottom to top automatically from massive images, and lead the result of image classification close to human level. CNN has been proved to be very effective for general object classification tasks [23–28]. In this paper, we construct an improved lightweight CNN for wear debris image classification named UstbNet and get better result for wear debris detection through the improved Faster RCNN.

The remainder of the paper is organized as follows. In Sect. 2, a new CNN we develop for classifying wear debris images is presented and experimental results are shown and discussed. Wear debris quantity and size are analyzed in Sect. 3. We introduce the application of the classification model UstbNet in steel production equipment in Sect. 4 and a conclusion is presented in Sect. 5.

2 Wear Debris Image Classification

2.1 Convolutional Neural Network Structure

CNN is a multi-layer neural network, it has a high degree of invariance to image distortion, and can take massive images as input directly to produce many features. The typical CNN mainly includes input layer, convolutional (conv) layer, pooling layer, norm layer, full connected layer, logistic regression layer and output layer. CNN reduces the dimensionality of image features by weight sharing, local perception and subsampling, so that the network can be trained and complexity is reduced.

The usual CNN include Cifar10, AlexNet and GoogleNet. Cifar10 is a simple network designed for databases based on 10 categories. AlexNet and GoogleNet have all achieved high classification accuracy on large dataset ImageNet, but their network structures are complex, and these networks require a lot of time to train the model.

In this paper, we proposed an improved lightweight CNN named UstbNet. Data augmentation, number and size adjustment of convolution kernels, batch normalization and loss function optimization are used to speed up the model convergence and improve the classification accuracy. The model used for training consists of nine layers, out of which six are conv layers and three are fully connected layers, as depicted in Fig. 3. The kernel size and kernel number of each conv layer and the number of neurons in fully-connected layer are listed in the following Table 2.

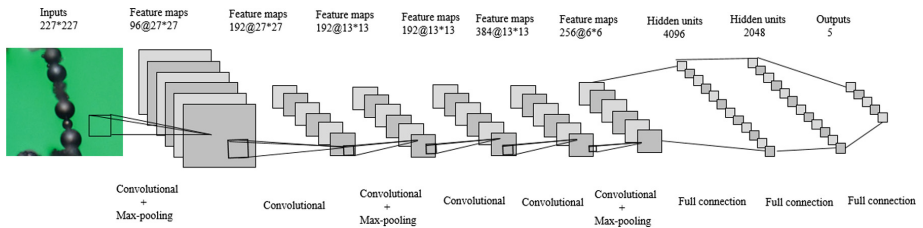


Fig. 3. Convolutional neural network UstbNet

Table 2. UstbNet network parameter description

Layer	Kernel size	Kernel/Neuron number	Stride
Conv1 + Relu	11	96	4
Pool + BachNorm+Scale	3	–	2
Conv2	3	192	1
Conv3 + Relu	3	192	1
BachNorm+Scale + Pool	3	–	2
Conv4 + Relu	3	192	1
Conv5 + Relu	3	384	1
Conv6 + Relu	3	256	1
Pool	3	–	2
FC1	–	4096	–
FC2	–	2048	–
FC3(Output)	–	5	–

2.2 Experimental Results and Comparisons

2.2.1 Data Augmentation

The traditional data augmentation methods include several types of transformation: rotation, skew, rescaling, flipping, shearing and add noisy. The settings for these transformations used in the experiment are presented in Table 3. The original dataset increased from 1640 to 8370 through data augmentation. To get a clear idea for different types of transformation, the transformed images for the same image with different methods are shown in Fig. 4.

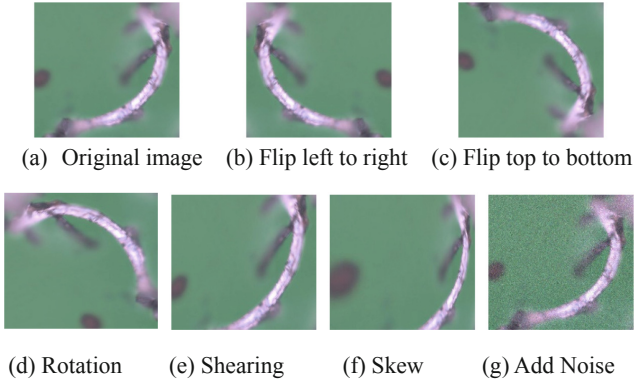


Fig. 4. The view of different types of transformation

Table 3. Parameter setting for data augmentation method

Method	Settings
Rotation	Random with angle in $[0^\circ, 360^\circ]$
Rescaling	Random crop to $227 * 227$
Flipping	Left to right
Flipping	Top to bottom
Shearing	Random with angle $[-25^\circ, 25^\circ]$
Skew	Random with magnitude 0.8
Add Noise	Gaussian

2.2.2 Experimental Configuration

All experiments in this study are performed on a desktop computer with i7-6700 (3.40 GHz), 16 GB RAM, NVIDIA GeForce GTX 1060 6G GPU. The train parameters are as follows: the learning rate is set to 0.001 with fixed policy, momentum: 0.9, weight decay: 0.0005, max iterations: 10000, and the mini-batch gradient descent method is used for parameter updating.

The experimental images are provided by a steel plant. The wear debris on ferrography are often overlapped with each other, so it is necessary to divide them for constructing the image database with single type wear debris. The size and shape of

each image are different due to the different shooting angles and magnification, but the input of CNN needs the same size image. The wear debris images are unified into $256 * 256$ size.

After preprocessing the images, the number of training dataset, validation dataset and test dataset for each class of wear debris images used in the experiment are shown in Table 4. In each training, the training dataset and validation dataset are divided randomly in the ratio of 4:1 in order to achieve the purpose of cross-validation.

Table 4. Number of experimental images

Wear debris classification	Training dataset	Validation dataset	Test dataset
Normal wear debris	1248	312	314
Spherical wear debris	1090	272	232
Cutting wear debris	930	232	236
Severe sliding wear debris	1011	252	302
Fatigue wear debris	1303	325	311
Total number	5582	1393	1395

2.2.3 Experimental Analysis

The basic UstbNet includes six conv layers and three fully connected layers. To investigate the behavior of Batch Normalization, SoftmaxWithLoss and Dropout as proposal methods, we conducted several ablation studies on the basic UstbNet. From Table 5, the results show that the network with SoftmaxWithLoss is more accurate than HingeLoss. Therefore, the following experiments are adopted SoftmaxWithLoss. As shown in Table 6, it is obviously that Batch Normalization can improve the classification accuracy and are better than Dropout. Dropout can reduce the training time while Batch Normalization slow down the training because of the large number of matrix operations. Furthermore, the combination of Batch Normalization and Dropout is the best.

Table 5. Ablation experiments of SoftmaxWithLoss and HingeWithLoss

Network structure	Average cross-validation accuracy (%)	Test accuracy (%)
Basic UstbNet + SoftmaxWithLoss	93.2	92
Basic UstbNet + HingeWithLoss	91	89

Table 6. Ablation experiments of Batch Normalization and Dropout

Network structure	Average cross-validation accuracy (%)	Test accuracy (%)	Average Training time (min)
Basic UstbNet + Batch Norm	95.6	94	138
Basic UstbNet + Dropout	94.2	93	113
Basic UstbNet + BatchNorm + Dropout	96.8	96	122

By using the same configuration as UstbNet, the experimental results of Cifar10, AlexNet, GooleNet and UstbNet on GPU are shown in Table 7. Both the validation accuracy and test accuracy of UstbNet are the highest. Through analyzing the accuracy and loss curve of above network structures as shown in Fig. 5, we can see that UstbNet guaranteed loss to decrease and stabilize gradually while achieving the highest accuracy. Besides, using GPU greatly speeds up the training speed and shortens the training time.

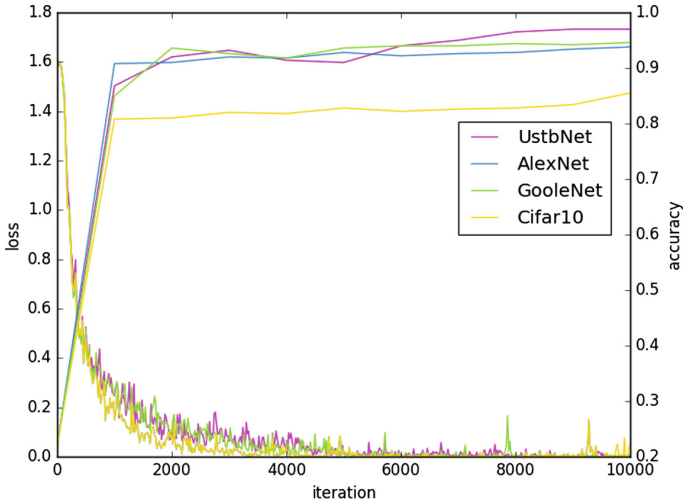


Fig. 5. The accuracy and loss curve

Table 7. Comparison of experimental results of cifar10 and UstbNet

Model	Layers	GPU training time (min)	Average cross-validation accuracy (%)	Test accuracy (%)
AlexNet	8	202	94	93.8
Cifar10	5	8	85.5	84
GooleNet	22	78	95	94.2
UstbNet	9	122	96.8	96

3 Wear Debris Quantity and Size Calculation

The wear debris image classification is used to judge whether there are wear debris or not, and the calculation in this section is for finding out the specific type of different wear debris.

3.1 Object Detection Algorithm Faster RCNN

Faster RCNN is a CNN object detection framework, gradually developed by RCNN. Faster RCNN consists of four parts. (1) Faster RCNN first uses a set of basic CNN to extract the feature maps of image. The feature maps are shared for subsequent Region Proposal Network (RPN) and full connection layer. (2) RPN is used to generate region proposals. The layer uses softmax to determine whether anchors belong to foreground or background, and then uses bounding box regression to correct anchors to obtain accurate proposals. (3) ROI pooling collects input feature maps and proposals. After synthesizing these information, proposal feature maps are extracted and sent to the subsequent full connection layer to determine the target category. (4) The proposal feature maps are used to calculate the classification of the proposal. The final detection box is obtained by bounding box regression again.

As shown in Fig. 6, an image ($P \times Q$) is input to Faster RCNN, scaling to a fixed size $M \times N$ after sending to the basic conv networks. RPN first performs 3×3 convolution on the feature map, then generates offset between foreground anchors and bounding box regression, and calculates proposals. The ROI pooling uses proposals to extract proposal features from feature maps and send them to subsequent full-connection and softmax to classify the proposals.

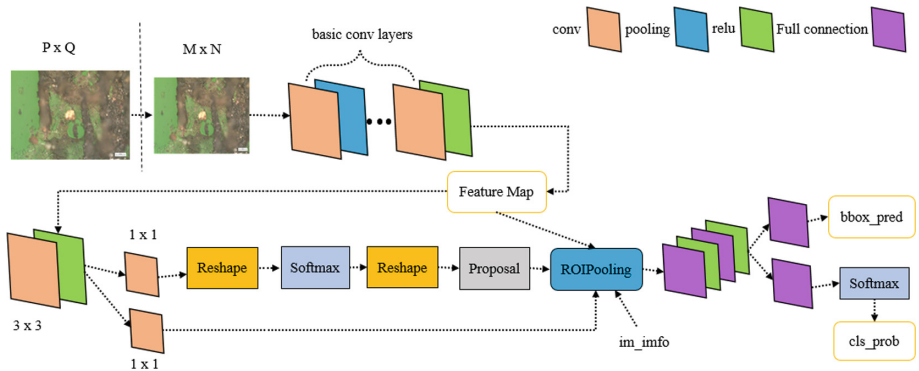


Fig. 6. Faster RCNN structure

3.2 Faster RCNN Improvement

3.2.1 Region-Based Fully Convolutional Networks R-FCN

Classification requires feature translation invariance, while detection requires accurate response to object translation. Faster RCNN are all conv layers before ROI pooling. It has translation invariance. After inserting ROI pooling, the full connection layers no longer have translation invariance and unable to share computing. Therefore, it has position translation-invariance and does not match the network's superior classification accuracy. In order to introduce translation variance, R-FCN uses a special conv layer to construct position-sensitive score maps and remove the full connection layers. R-FCN algorithm steps are shown in Fig. 7. Firstly, the preprocessed images are sent into a

pre-trained classification network. The corresponding network parameters are fixed. There are three branches on the feature map obtained from the last conv layer of the pre-trained network. One gets the corresponding ROI from the RPN operated on the feature map. Another gets a $k * k * (C + 1)$ dimension position-sensitive score map on the feature map for the classification. A $4 * k * k$ dimension position-sensitive score map is obtained on the feature map for regression. Finally, position-sensitive ROI pooling is performed on $k * k * (C + 1)$ dimension and $4 * k * k$ dimension position-sensitive score maps to obtain the corresponding classification and position information.

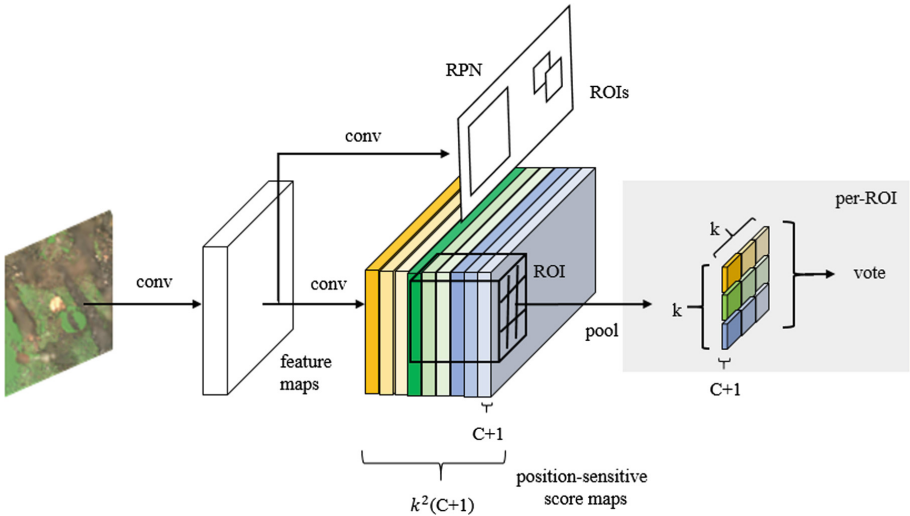


Fig. 7. R-FCN structure

3.2.2 Online Hard Example Mining

According to the loss of input samples, Online Hard Example Mining (OHEM) filters out hard examples to represent the samples that have a greater impact on classification and detection. The obtained hard examples will be trained in stochastic gradient descent. Hard example is selected according to the loss of each ROI and the largest loss ROIs are chosen. The specific operation is to extend the original ROI Network to two ROI Networks, which share parameters. The front ROI Network has only forward operations, mainly for computing losses. The latter ROI Network includes forward and backward operations. Hard examples are used as input to calculate the loss and pass back the gradient.

3.2.3 Feature Pyramid Network

Although Faster RCNN has the characteristic of high detection stability, it lacks the ability to detect fine-grained and small-size features. In this paper, a detection framework combining Faster RCNN and FPN (Feature Pyramid Network) is used to obtain

better small object detection results. As shown in Fig. 8(a) shows a sketch of Faster RCNN extracting and predicting features, a process that only uses the last layer feature map of the convolutional neural network. However, due to the small size of spherical wear debris studied in this paper, its information will be lost after several convolution and pooling operations. Figure 8(b) shows the structure of FPN, which uses the inherent multi-scale and multi-level structure of deep convolution neural network and adopts a top-down side connection to construct high-level semantic feature maps at all scales, gaining the ability to detect fine-grained features.

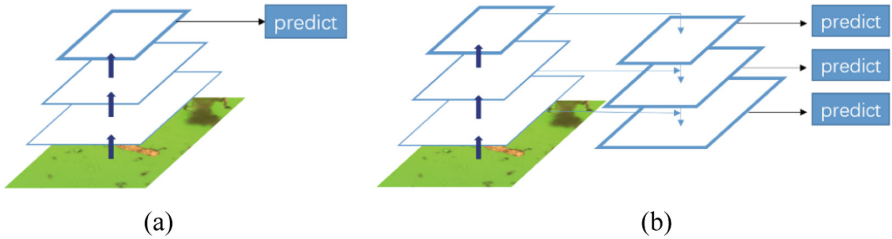


Fig. 8. Different structure of feature map (a) Single feature map (b) Feature pyramid network

3.3 Experiment Analysis

Wear debris detection use original images. The methods of data augmentation in Sect. 2.2.1 is applied. After data augmentation, the training dataset is 2238, both the validation dataset and test dataset are 745. The number of each type of wear debris label bounding boxes are shown in Table 8. In the following experiments, five types of wear debris (fatigue, severe sliding, cutting, spherical, copper) are tested. The learning rate is set to 0.001 with step policy and stepsize is 10000. Max iteration is 20000.

Table 8. Each type of wear debris label bounding boxes

Wear debris	Fatigue	Sever sliding	Cutting	Spherical	Copper
number	1732	1008	1064	3134	1012

Faster RCNN uses ZF, VGG1024, VGG16 and ResNet50 as a pre-trained model to initialize the network parameters. The experiment result uses AP value as evaluating indicator. AP is an indicator of global performance. It is the area value of the Precision-Recall (PR) curve. The formula is shown as Eq. (1).

$$AP = \int_0^1 P(R)dR \quad (1)$$

Faster RCNN detection results are shown in Table 9. Among these network structures, ResNet50 gets the best effort. ResNet50 trains the deeper network by using

residual modules and conventional SGD. R-FCN use ResNet50 and OHEM compared with Faster RCNN. As illustrated in Table 10, R-FCN with ResNet50 and OHEM gets better test result and shorter test time. In addition, the detection results in Table 9 are based on the framework including only Faster RCNN, and the last three rows in Table 10 are based on the framework including R-FCN, Faster RCNN, OHEM and FPN. Faster RCNN is used to detect the wear debris because the fatigue and severe sliding wear debris have more harm to the normal operation of mechanical equipment.

Table 9. Faster RCNN detection results

Detect model	<i>mAP</i>	Fatigue	Severe sliding	Cutting	Spherical	Copper
Faster RCNN+ZF	0.5812	0.7099	0.4727	0.7596	0.4458	0.5182
Faster RCNN+VGG1024	0.6355	0.7642	0.4976	0.7803	0.4636	0.6717
Faster RCNN+VGG16	0.7480	0.7323	0.7698	0.8588	0.5385	0.8403
Faster RCNN+ReNet50	0.7793	0.7920	0.8428	0.7734	0.6543	0.8338

Table 10. R-FCN detection results compared with Faster RCNN

Detect model	<i>mAP</i>	Fatigue	Severe sliding	Cutting	Spherical	Copper	Test time (sec/img)
Faster RCNN+ ReNet50	0.7793	0.7920	0.8428	0.7734	0.6543	0.8338	0.391
Faster RCNN + ReNet101	0.7700	0.7677	0.8571	0.8465	0.5293	0.8496	0.180
Faster RCNN+ ReNet101+ FPN+ OHEM	0.8297	0.8426	0.8868	0.8844	0.6522	0.8823	0.179
R-FCN+ ReNet50 + FPN + OHEM	0.8319	0.7491	0.8512	0.8252	0.8555	0.8787	0.178

According to the detected boxed number, we can get the quantity of each wear debris.

3.4 Grabcut Segmentation on Wear Debris

Graphcut is an image segmentation technology based on graph cut algorithm. It just needs foreground and background input. The algorithm can complete the background and foreground similar supervision weighted graph, and segment image by optimal cutting. Grabcut is the improvement of Graphcut. Grabcut doesn't require user interaction, and it just needs to input foreground region to segment the foreground from the background. The detected boxes in Faster RCNN are input to Grabcut as foreground region. The detected box is shown in Fig. 9. After open operation and close operation, the segmentation result is shown in Fig. 10. The long axis of wear debris can be calculated on the segmented image.

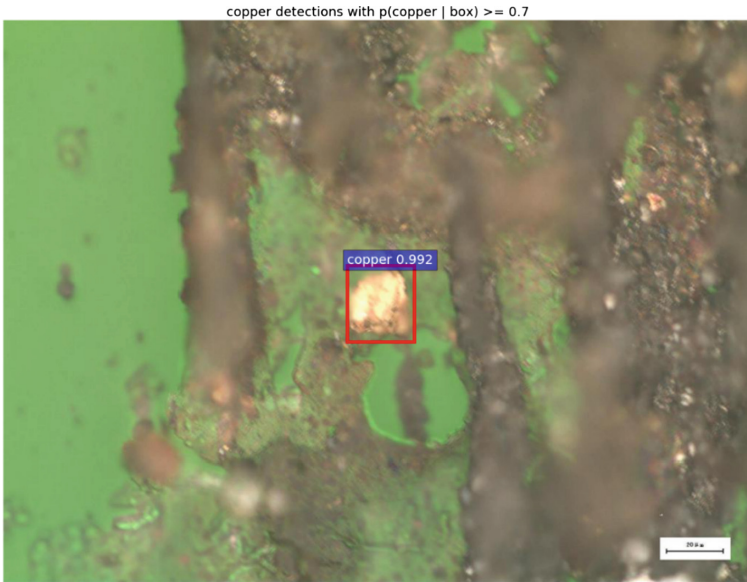


Fig. 9. Faster RCNN detected box in wear debris image

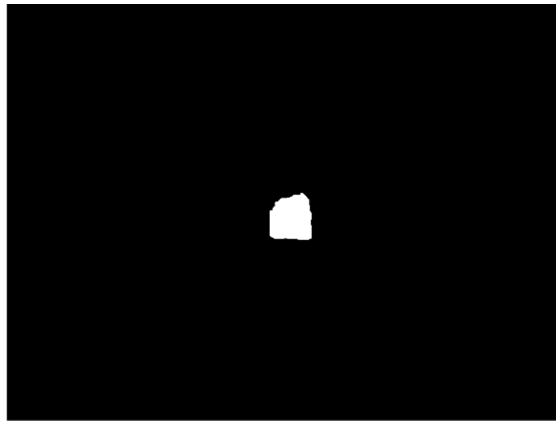


Fig. 10. Grabcut Segmentation result

4 Application

The wear debris in the oil of steel production equipment lubrication system are deposited on the ferrography. Then we use the above methods to analyze the wear debris images, so as to judge the wear degree and failure type of steel equipment and repair it in time.

4.1 Fault Analysis of Caster Ladle Turret Lubricating System

The caster ladle turret bearing of steel plant is the key equipment in the steelmaking production line, and the cost is very high. We evaluated the current wear state of a large ladle turret bearing in a steel plant, and a large number of large size wear debris were found on ferrography of the 4 sample points of the bearing. By analyzing the wear debris images, we find that there were mainly severe sliding and fatigue wear debris, as shown in Fig. 11.

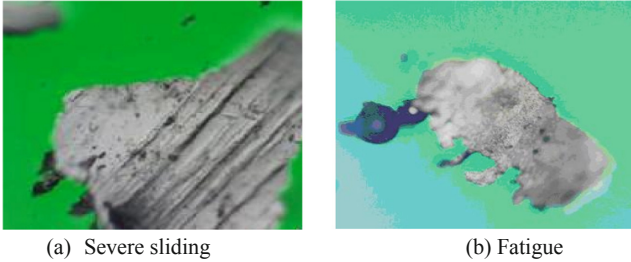


Fig. 11. Wear debris images generated by the bearing

The occurrence of large-size severe sliding wear debris indicates that the sliding wear between the friction pairs is serious. The occurrence of extra-large-size fatigue wear debris indicates that the bearing has a severe fatigue spalling phenomenon. It can be concluded that serious abnormal wear occurs in the bearing. Therefore, it is suggested that the manufacturer prepare as soon as possible so as to replace the bearing. According to the suggestion, the manufacturer disassembled and checked the bearing. The results show that there is a serious fatigue spalling in the main and outer raceway of the bearing, as shown in Fig. 12. The inspection results showed that the fatigue spalling of the bearing had made it unable to continue service, and it further proved that the previous classification results were completely accurate.

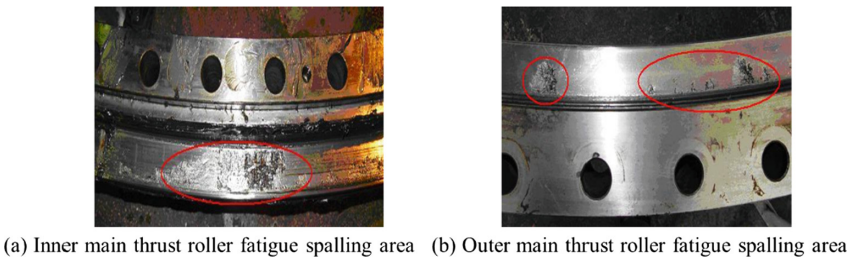


Fig. 12. Bearing dismantled results

4.2 Fault Analysis of Material Sintering Vibrating Screen Lubricating System

The vibrating screen of steel plant is used to screen ore, with the characteristics of large vibration amplitude and heavy load. The wear debris produced by the vibrator bearing of a vibrating screen in a steel plant. It was found that there were a large number of large size fatigue wear debris on ferrography, as shown in Fig. 13. Therefore, the bearing had serious fatigue wear and tear. It is recommended that the factory arranges the maintenance as soon as possible, and check the bearing damage. After the factory dismantle it, a large number of fatigue spalling were found in the inner ring and rolling body of the free side bearing, as shown in Fig. 14. The cage also had obvious abnormal wear and tear, so the bearing was replaced.



Fig. 13. Fatigue wear debris generated by the bearing



(a) Abnormal wear inner ring of bearing



(b) Abnormal wear of rolling body

Fig. 14. Bearing dismantled results

After checking the replacement bearing, it was found that although the prosecution took every 2 d oil change once the measure, but the bearing wear was very large. The wear debris deposited on ferrography were analyzed and we found large size of fatigue wear debris. It indicated that there was still a serious abnormal wear phenomenon in the bearing. Bearing wear status had further deteriorated trend, belonging to the typical fatigue failure. Consequently, the root cause of abnormal wear of the device was not

lubrication, but because of the unreasonable selection of bearings. The factory accordingly redesigned bearing models and replaced all the bearings. By tracking and monitoring the wear debris on ferrography, the new bearing wear rate significantly reduced compared with the original bearing, and the bearing is in good condition.

4.3 Fault Analysis of De-silication Dust Cleaning Fan

The de-silication dust cleaning fan is a tail-wagging equipment for the iron-making production line. Through the ferrographic analysis of sampling the lubrication oil on both sides of motor bearing, it was found that there were a large number of large size wear debris in the load side bearing. Among them, there were normal sliding, fatigue, cutting and spherical wear debris, as shown in Fig. 15. There was serious abnormal wear on the load side bearing, and the main reason for the fault is the wear of the bearing cage. After dismantling the bearing, we found that the motor load side bearing holder was worn by 2–4 mm depth, leaving an obvious indenter, and there was an indentation in the inner ring and outer ring of the bearing. After replacing the bearings on both sides of the motor, the condition of the motor was tested. The vibration of the motor had been restored to the normal level.

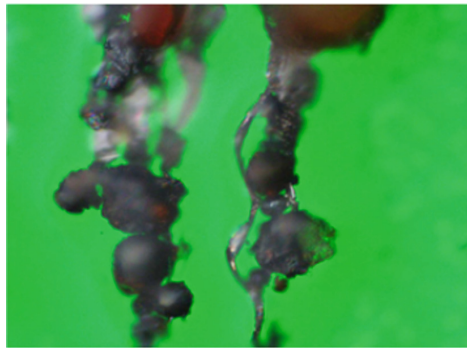


Fig. 15. Wear debris of load side bearing

5 Conclusion and Future Work

In this paper, an improved lightweight CNN UstbNet is proposed. It proves that CNN for the wear debris classification task is very effective. In addition, we use the improved Faster RCNN to detect wear debris and segment wear debris image on detected region proposals through grabcut. The feature pyramid network is added in Faster RCNN to improve the detection result of small objects such as spherical wear debris. The above methods are applied to analyze the fault of caster ladle turret lubricating system, material sintering vibrating screen lubricating system and desilication dust cleaning fan. The application shows that the methods are effective to find the severe wear in steel production equipment.

The UstbNet classification model for single-feature wear debris images has reached a higher classification accuracy, but it still needs to be further improved for multi-feature wear debris images. Future studies will focus more on the classification of multi-feature wear debris images by using multi labels to train the classification model.

Acknowledgment. This work is supported by National key R & D plan (2016YFB0601301), National Natural Science Foundation (51574032, 51674030) and Fundamental Research Funds for the Central Universities (FRF-TP-18-097A1).

References

1. Kun, X., Luxmoore, A.R., Deravi, F.: Comparison of shape features for the classification of wear particles. *Eng. Appl. Artif. Intell.* **10**, 485 (1997)
2. Zhao, R.: Study on lubrication of metallurgical rolling equipment. *Sci. Technol. Enterp.* 357–358 (2013)
3. Qin, H., Ren, Z., Zhao, J., Ye, C., Doll, G.L., Dong, Y.: Effects of ultrasonic nanocrystal surface modification on the wear and micropitting behavior of bearing steel in boundary lubricated steel-steel contacts. *Wear* **392**, 29 (2017)
4. Chang, Z., Jia, Q., Yuan, X., Chen, Y.: Main failure mode of oil-air lubricated rolling bearing installed in high speed machining. *Tribol. Int.* **112**, 68 (2017)
5. Mosleh, M., Bradshaw, K., Belk, J.H., Waldrop, J.C.I.: Fatigue failure of all-steel and steel-silicon nitride rolling ball combinations. *Wear* **271**, 2471 (2011)
6. Mao, J.: Study on preparation technology of self-lubricating wear-resistant coatings on mill gear surface by composite of laser cladding and shock peening. Master. Jiangsu University (2016)
7. Wang, F.: Study on the ferrography wear particle with image processing technology. Master. Wuhan University of Technology (2005)
8. Thomas, A.D.H., Davies, T., Luxmoore, A.R.: Computer image analysis for identification of wear particles. *Wear* **142**, 213 (1991)
9. Stachowla, G.P., Stachowiak, G.W., Podsladlo, P.: Automated classification of wear particles based on their surface texture and shape features. *Tribol. Int.* **41**, 34 (2008)
10. Roylance, B.J., Albidewi, I.A., Laghari, M.S., Luxmoore, A.R., Deravi, F.: Computer-aided vision engineering (CAVE)—quantification of wear particle morphology. In: STLE 48th Annual Meeting, Calgary, Alberta, Canada, 6 pp. (1993)
11. Xu, K., Luxmoore, A.R., Jones, L.M., Deravi, F.: Integration of neural networks and expert systems for microscopic wear particle analysis. *Knowl.-Based Syst.* **11**, 213 (1998)
12. Zuo, H., Wu, Z., Yang, Z.: Application of double BP-network in debris identification. *Acta Aeronautica ET Astronautica Sinica* **21**, 372 (2000)
13. Li, Q., Zhao, T., Zhang, L., Sun, W., Xi, Z.: Ferrography wear particles image recognition based on extreme learning machine. *J. Electr. Comput. Eng.* **2017**, 1 (2017)
14. Peng, Z.: An integrated intelligence system for wear debris analysis. *Wear* **252**, 730 (2002)
15. Xiong, A., Kong, X., Wang, J., Chen, D.: The sharable wear particle recognition and wear diagnosis system. *Mech. Sci. Technol. Aerosp. Eng.* **421**, 421–423 (2002)
16. Peng, Y., Wu, T., Wang, S., Peng, Z.: Wear state identification using dynamic features of wear debris for on-line purpose. *Wear* **376–377**, 1885 (2017)
17. Yuan, W., Chin, K.S., Hua, M., Dong, G., Wang, C.: Shape classification of wear particles by image boundary analysis using machine learning algorithms. *Mech. Syst. Signal Process.* **72–73**, 346 (2016)

18. Tian, Y., Wang, J., Peng, Z., Jiang, X.: A new approach to numerical characterisation of wear particle surfaces in three-dimensions for wear study. *Wear* **282–283**, 59 (2012)
19. Isa, M.C., Yusoff, N.H.N., Nain, H., Yati, M.S.D., Muhammad, M.M., Nor, I.M.: Ferrographic analysis of wear particles of various machinery systems of a commercial marine ship. *Procedia Eng.* **68**, 345 (2013)
20. Wang, J., Wang, X.: A wear particle identification method by combining principal component analysis and grey relational analysis. *Wear* **304**, 96 (2013)
21. Wang, H., Huang, R., Gao, L., Wang, W., Xu, A., Yuan, F.: Wear debris classification of steel production equipment using feature fusion and case-based reasoning. *ISIJ Int.* **58**, 1293 (2018)
22. Wang, J., Zhang, L., Lu, F., Wang, X.: The segmentation of wear particles in ferrograph images based on an improved ant colony algorithm. *Wear* **311**, 123 (2014)
23. Wu, Z.: An vehicle type recognition method based on Convolution Neural Network. *Mech. Electr. Eng. Technol.* **Z2**, 608 (2016)
24. Krizhevsky, A., Sutskever, I., Hinton, G.E.: ImageNet classification with deep convolutional neural networks. *Commun. ACM* **60**, 84 (2017)
25. Yu, S., Jia, S., Xu, C.: Convolutional neural networks for hyperspectral image classification. *Neurocomputing* **219**, 88 (2017)
26. Ferreira, A., Giraldo, G.: Convolutional Neural Network approaches to granite tiles classification. *Expert Syst. Appl.* **84**, 1 (2017)
27. Gomez Villa, A., Salazar, A., Vargas, F.: Towards automatic wild animal monitoring: identification of animal species in camera-trap images using very deep convolutional neural networks. *Ecol. Inform.* **41**, 24 (2017)
28. Dyrmann, M., Karstoft, H., Midtby, H.S.: Plant species classification using deep convolutional neural network. *Biosys. Eng.* **151**, 72 (2016)



ArcGIS Services Recommendation Based on Semantic and Heuristic Optimization Algorithm

Jiaqi Zheng¹, Jin Diao², Zhangbing Zhou^{2,3(✉)}, and Yongli Xing¹

¹ School of Science, China University of Geosciences (Beijing), Beijing 100083, China

² School of Information Engineering, China University of Geosciences (Beijing), Beijing 100083, China

zhangbing.zhou@gmail.com

³ Computer Science Department, TELECOM SudParis, 91011 Evry, France

Abstract. It is a common phenomenon that GIS service, a convenient tool, helps people to solve the problem in various fields. However, single GIS service can no longer meet the diverse needs of users. To address this challenge, a GIS services composition recommendation framework based on semantic and heuristic optimization algorithms is proposed in this paper. The Normalized Google Distance (NGD), as an indicator of invoking between two services, is used to construct dynamic semantic network. In order to save processing time, we use the hierarchical structure of ArcGIS services. In addition, we use the improved heuristic optimization algorithm to find the solution with the highest semantic value quickly. Consequently, once the initial parameters set and the end parameters set are given by the user, our GIS services composition recommendation framework will find the most appropriate Directed Acyclic Graph (DAG) to the user. The result of evaluation proves that our method could give more meaningful solution, compared with others.

Keywords: Semantic GIS service composition · Normalize Google Distance (NDG) · Heuristic optimization algorithm · ArcGIS service

1 Introduction

More and more tools and method for geospatial data analysis are being developed and distributed on the web, which makes it easier for us to solve problems in our lives [1]. For example, GIS services helps us find the best location to set up a fire station easily and quickly in [2]. Beside that, GIS services are also used in agriculture, medical care, transportation and various fields. Therefore, it is a trend that composing many GIS services together to provide added values to meet the user's requirement. Automatic services composition can be of great value to the GIS users, cause it can greatly broaden the functional ability to handle users' requirement [3]. However, it is still a big challenge for service

developers that making GIS service composition fulfill functional requirements [4].

The process of service discovery, selection and composition is a crucial task in web service based application development [5]. The methods of [6] is based on syntax matching, which didn't take the services semantics information into account. Later, in [11], the author proposed to optimize the service composition by considering QoS, which didn't consider the semantic information. And some scholar proposed that automate interactions between web services are important [7]. So the concept of ontology is proposed in [8–10], which is used to measure the semantic distance between services. However, it is a huge problem that how to build a comprehensive and standard ontology library of GIS.

To solve the problem mentioned above, we proposed a method that can compose and recommend GIS services in a semantic way. The main contributions of this article are summarized as follows:

- To get semantic relationships between services, we use Normalized Google Distance (NGD) to discover the actual inter-service invocation status.
- Considering the hierarchical structure of ArcGIS Services, a round of filtering is carried out before the network is built for reducing the retrieval time.
- In order to speed up the search time in the network, this paper use improved simulated annealing algorithm to get a relatively better solution.

The rest of this paper is organized as follows. Section 2 defines relevant concepts. Section 3 introduces the mechanism about how to construct the dynamic semantic model. Section 4 use an improved heuristic optimization algorithm to accelerate the processing of selecting DAG. Section 5 shows the result about our experimental evaluation and analysis the research. Section 6 introduces the related works of service recommendation. Finally, 7 concludes about this work.

2 Preliminaries

Definition 1 (User Requirement). *An user requirement is a tuple $req=(InP, OutP)$, where:*

- InP is a parameter set containing all user input parameters;
- $OutP$ is a parameter set containing all user output parameters;

A req is consist of input and output parameters set, given by the user.

Definition 2 (Directed Acyclic Graph). *A Directed Acyclic Graph, which can be performed to meet the user requirement, is a tuple $DAG = (S, INV)$, where:*

- S is the set of ArcGIS Services contained in this DAG, which can also regard as lots of vertices in this DAG;
- INV is the set of direct links, which represents the invocation relationships between these ArcGIS Services contained in this DAG;

A DAG is used to describe the invocation relationship between services, which is generated to meet user requirements.

Definition 3 (ArcGIS Service). An ArcGIS Service is a tuple $s = (nm, dsc, IuP, OutP)$, where:

- nm is the name of ArcGIS Service;
- dsc is an explanation of the functionality of this ArcGIS Service;
- IuP is the set of input parameters contained in this ArcGIS Service;
- $OutP$ is the set of output parameters contained in this ArcGIS Service;

Each s has a specific function, which can be used to solve specific problem.

Definition 4 (Semantic Services Network Model). A Dynamic Semantic Services Network is a triple $SNetM = (S, INV, WGT)$, where:

- S are the services contained in this Dynamic Semantic Services Network;
- INV is the set of direct links between ArcGIS Services, which represents the ability that this ArcGIS Services may invoke others;
- WGT are the weights defined upon the direct links INV , which represent the specific possibility that an ArcGIS Services is invoked by the other; contained in this ArcGIS Services.

There is an example in Fig. 5. Each vertex represents a service, each oriented edge represents the direction of service execution, and the value on the edge represents the semantic similarity between services.

3 Construction of Semantic Network Model

3.1 Hierarchical Structure of ArcGIS Services

ArcGIS offers advanced GIS functionalities geoprocessing tool to the users to solve the problem, which are organized in a tree structure [12]. Such a special structure can help us to remove off the unnecessary ArcGIS services to save the time and computing resources, which is shown in Fig. 1. For example, if the output parameter of the previous service(s) is vector data, there is no need to retrieve the cluster of ArcGIS services which could only use raster data as input parameters in the same subtree. Thus, using ArcGIS services tree structure can help us reduce the scope of the search and speed up the retrieve.

3.2 Services Semantic Calculation

(1) Normalized Google Distance (NDG)

Based on the principle that words with similar meanings appear more frequently in the browser web page, we use NGD to calculate the invocable between services. NGD is calculated by Eq. 1:

$$NGD(x,y) = \frac{\max(\log f(x), \log f(y)) - \log f(x,y)}{\log M - \min(\log f(x), \log f(y))} \quad (1)$$

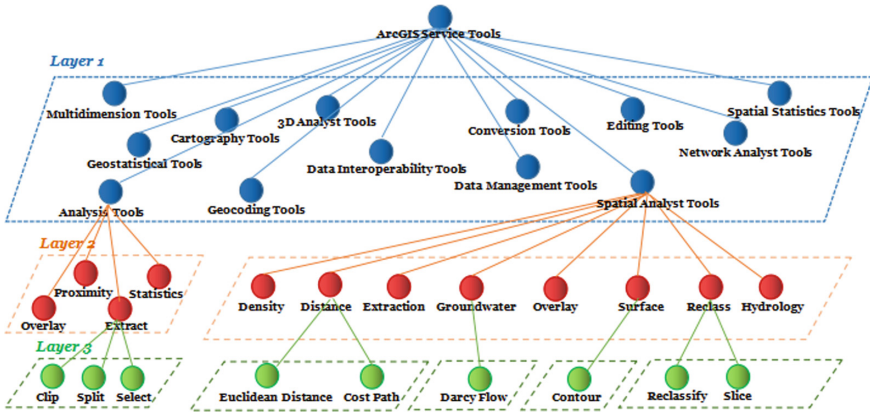


Fig. 1. ArcGIS services tree structure.

In Eq. 1, M represents the total number of pages searched by Google. $f(x)$ and $f(y)$ are the hits of the search terms x and y , respectively. $f(x, y)$ is the number of pages that appear in both x and y . If two search terms x and y never appear together on the same page, the normalized Google distance between them is infinite. Thus, the value of NDG ranges from 0 to infinity, the larger value represents the greater the distance, which meaning the greater semantic distance between two words, and vice versa.

(2) *Services Semantic Calculation*

The name of GIS services would be broken down into multiple words. Then use the minimum cost and maximum flow algorithm [13,14] adopted method to compute the cost between WD_{ArcNm1} and WD_{ArcNm2} . So, the names similarity can be computed by Eq. 2.

$$\begin{aligned}
 &sim_{serNm}(ser.nm_1, ser.nm_2) \\
 &= 1 - \frac{cost}{max(SizeOf(WD_{serNm1}, WD_{serNm2}))}
 \end{aligned}
 \tag{2}$$

The text description similarity of ArcGIS Services is calculated by Eq. 3, which use *xsimilarity* [15]. In this method, words similarity in sentences (denoted as *wordSim*) and the words order (denoted as *ordSim*) are taken as parameters. The specific calculation formula is as:

$$\begin{aligned}
 &sim_{serDsc}(ser_1.dsc_1, ser_2.dsc_2) \\
 &= \xi \times wordSim + (1 - \xi \times ordSim)
 \end{aligned}
 \tag{3}$$

The Similarity Computation between ArcGIS Services is calculated by parameters sim_{serNm} and sim_{serDsc} in Eq. 4.

$$\begin{aligned} sim_{act}(act_1, act_2) \\ = \varrho \times sim_{serNm}(Arc_1).nm_1, ser_2.nm_2) \\ + (1 - \varrho) \times sim_{serDsc}(ser_1.dsc_1, ser_2.dsc_2) \end{aligned} \quad (4)$$

(3) Calculating the Semantic value of Workflow Pattern

There are two common workflow patterns for GIS service composition: sequential workflow pattern and parallel workflow pattern, which can see in Fig. 2. The semantic value for sequential workflow pattern and parallel workflow pattern are calculated by Eqs. 5 and 6 respectively.

$$SIM_{seq} = \sum_{i=1}^n S_i \quad (5)$$

$$SIM_{para} = \frac{\sum_{i=1}^n S_i}{n} \quad (6)$$

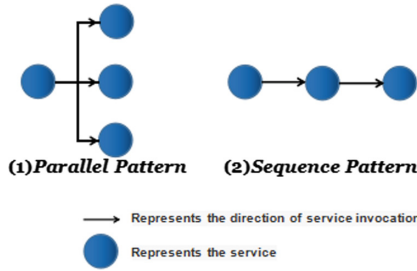


Fig. 2. Sequential workflow pattern and parallel workflow pattern.

3.3 Construction Network

(1) Narrowing Candidate Service Set

It would be a huge project that retrieving the entire set of ArcGIS services when we selected the candidate services. So we can use the unique tree structure of the ArcGIS services (refer to Sect. 3.1), which can help us reduce the services search space. Algorithm 1 tells about how to narrow the service candidate set.

In Algorithm 1, S can be obtained. T represents the set of all GIS services organized in a tree structure. I represents all the input parameters. S represents all candidate services which take these parameters as input parameters. First, set S copies all GIS services in T . Count the number of first level subtrees in the tree structure and assign this value to variable n (lines 1–2). By checking

Algorithm 1. Narrowing Candidate Service Algorithm

Require:

- T : all ArcGIS services set organized by tree structure.
- I : all input parameters set.

Ensure:

- S : all candidate services set.
- P : output parameters set generated by the candidate services

```

1:  $Var\_S \leftarrow T; S \leftarrow \emptyset; P \leftarrow \emptyset;$ 
2:  $n \leftarrow$  the number of tree categories in the first layer;
3: for  $i = 1: n$  do
4:   if  $I.par \neq subtree(i).par$  then
5:     remove  $subtree(i)$  from  $S$ ;
6:   end if
7: end for
8:  $k \leftarrow$  the number of subtree in  $S$ ;
9: for  $i = 1: n$  do
10:  for  $j = 1: i$  do
11:    if  $subsubtree(j).par \supseteq I.par$  then
12:      remove  $subsubtree(j)$  from  $Var\_S$ ;
13:    end if
14:  end for
15: end for
16: find candidate services set  $S$  by retrieving  $Var\_S(I)$ 
17:  $S \leftarrow s(I)$ ;
18:  $P \leftarrow S.OutP$ ;

```

the required parameter types between the subtree and I , we can remove the unmatched subtree from S . When all subtree nodes have been detected, count the number of subtrees left and assign the value to variable k (lines 3–8). For each subsubtree in the subtree, a parameter type check is performed again. If the required parameters for the service to run in the subsubtree are more than the parameter types in I , this subsubtree is deleted (lines 9–15). And then find the services in Var_S , taking all parameters in I as input (denoted as $Var_S(I)$), and assign it to S . Finally, put the output parameters of S into P (lines 16–18).

(2) Building Semantic Networks

The Algorithm 2 is used to build a solution space network, from which generate the DAG and recommend it to users. Therefore, the Algorithm 2 takes user requirements req as input and the solution space network model $SNetM$ as output. First, copy the parameters in InP to P and set Var_S, INV as empty sets, where Var_S is used to store the services generated in the process and INV is used to record invocation relationships between services. Record the number of parameters in P and put them into variable n . Set parameter Var_P to null to store the generated parameters (lines 1–2). For all parameters in P , if using Algorithm 1 (denoted as $NarrSer$) finds a narrowed service set, then find the appropriate service from the narrowed service set and put it into the variable

Var_s . The output parameters of all services generated during this process are put into the variable Var_p . Record the relationship and semantic value between these services into the INV (lines 3–9). Looking for a candidate service with multiple parameters as input is similar to looking for one parameter as a candidate service (lines 10–18). Then, the number of iterations k is increased once and the parameters in the intermediate variable Var_P are copied into the P set. $NetM$ can be output if the generated parameters include the parameters required by the user or if the number of iterations is greater than the threshold. Otherwise, jump to the line 2 and continue with the above procedure (lines 19–24).

Algorithm 2. Building Semantic Networks Algorithm

Require:

- req: req = (InP, OutP).

Ensure:

- SNetM: service network model.

```

1:  $P \leftarrow InP$ ;  $Var_S \leftarrow \emptyset$ ;  $k \leftarrow 0$ ;  $INV \leftarrow \emptyset$ ;
2:  $Var_P \leftarrow \emptyset$ ;  $n \leftarrow$  the number of parameters in  $P$ ;
3: for  $i = 1: n$  do
4:   if  $NarrSer(P(i))$  then
5:      $Var_S \leftarrow$  find services in  $NarrSer(P(i)).S$ ;
6:      $Var_P \leftarrow Var_S.P$ ;
7:     recording  $INV$  and  $INV.SIM_{seq}$ ;
8:   end if
9: end for
10: for  $i = 1: n$  do
11:   for  $j = 1: n$  do
12:     if  $NarrSer(P(i), P(j))$  then
13:        $Var_S \leftarrow$  find services in  $NarrSer(P(i), P(j)).S$ ;
14:        $Var_P \leftarrow Var_S.P$ ;
15:       recording  $INV$  and  $INV.SIM_{para}$ ;
16:     end if
17:   end for
18: end for
19:  $k++$ ;  $P \leftarrow Var_P$ ;
20: if  $Var_P \supseteq OutP$  ||  $k \leq 50$  then
21:    $SNetM = (Var_s, INV)$ ;
22: else
23:   turn to Line 2;
24: end if

```

In this way, a dynamic semantic web is formed, which contains the DAG required by users. For instance, Fig. 5 is a $SNetM$. According to the user input and output parameters $Req.I$, Algorithms 1 and 2 are used to constructing semantic network model, which contains the DAG needed by users.

4 Recommendation System Based on Improved Simulated Annealing Algorithm

4.1 Generating New Path

To reach global optimal solution instead of local optimal solution, the simulated annealing algorithm is required to accept the new solution with a certain probability. Therefore, this section will talk about how to generate new path.

- *Dividing the Solution into Small Module*: The resulting graph solution could be divided into blocks according to workflow patterns (Fig. 2).
- *Selecting the Replacement Module*: The marked block should be replaced by the other block(s) in the SNetM. So use the random number generator to select a block, which will be replaced by other block, which is shown in Fig. 4.
- *Generating New Solution*: Replace the selected block and connect the selected block between the former block and the latter block. Consequently, a new graph result is produced, which can be seen example B in Fig. 3.

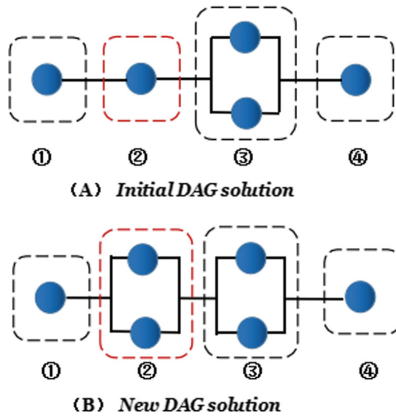


Fig. 3. Dividing into blocks.

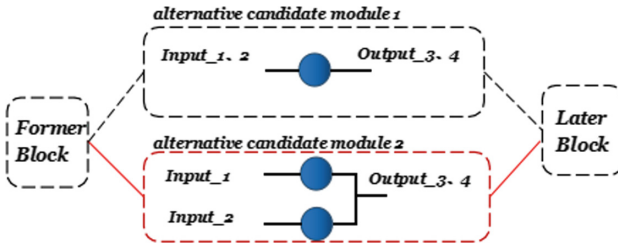


Fig. 4. Dividing into blocks.

4.2 Improved Simulated Annealing Algorithm

Algorithm 3. Building Dynamic Semantic Network Model Algorithm

Require:

- *Cur_DAG*: an arbitrary initial DAG.
- *coolingtable*(*t*, α , *EPS*, *ILOOP*): the parameters of simulated annealing algorithm were recorded
- *LIMIT*: upper limit of probability selection.
- *OLOOP*: number of external cycles.
- *Best_DAG*: DAG recommended to user.

Ensure:

```

1: P_L = 0; P_F = 0;
2: Best_DAG = Cur_DAG; New_DAG = Best_DAG;
3: while 1 do
4:   for i = 0; i < ILOOP; i++ do
5:     New_DAG = changeSolution(Cur_DAG);
6:     dE = SIMNew_DAG - SIMCur_DAG;
7:     if dE < 0 then
8:       Cur_DAG = New_DAG;
9:       P_L=0; P_F=0;
10:    else
11:      if exp(dE/t) > rand(0,1) then
12:        Cur_DAG = New_DAG;
13:        P_L ++;
14:      end if
15:    end if
16:    if P_L > LIMIT then
17:      P_F ++; break;
18:    end if
19:  end for
20:  if SIMCur_DAG < SIMBest_DAG then
21:    Best_DAG = Cur_DAG;
22:  end if
23:  if P_F > OLOOP || t < EPS then
24:    break;
25:  end if
26:  t * =  $\alpha$ ;
27: end while

```

The simulated annealing algorithm starts with the initial solution *i* and the control parameter *t* and the process is controlled by the cooling schedule, which includes the initial value of the control parameter *t* and its attenuation factor α , the iteration number *ILOOP* of each *t* and the stop condition *EPS* in Algorithm 3. *Cur_DAG* is a result randomly found from the network that meets the user's input and output requirements. The *Best_DAG* represents the DAG

which can better meet the user’s requirement. Coolingtable represents a set of parameters that control the progress of an algorithm.

Parameters P_L and P_F are set to record the times of receiving bad results in a certain stage of annealing process and the times of this process respectively. Temporarily set $Best_DAG$ and New_DAG to be the same value as the Cur_DAG (lines 1–2). Use the algorithm $changeSolution()$ to generate the New_DAG and calculate the semantic value difference between the two path (denoted as dE). If the semantic values of New_DAG (denoted as SIM_{New_DAG}) is higher than that of Cur_DAG (denoted as SIM_{Cur_DAG}), the New_DAG will be accepted as the Cur_DAG . Otherwise, the above operation is carried out with a certain probability to avoid falling into local optimal and increment the value of the P_L by 1. If PL is greater than LIMIT, jump out of the loop (lines 3–19). After the above process, if the SIM_{Cur_DAG} is higher than SIM_{Best_DAG} , replace the Cur_DAG with $Best_DAG$ (lines 20–22). Then, determine whether the program is completed by judging whether P_F is greater than $OLOOP$ or the temperature t reaches the minimum value EPS . If the exit condition is not reached, use attenuation coefficient α to cool the temperature and continue the cycle (lines 20–27). As a result, the DAG is found in the semantic web in Fig. 5 and recommended it to the user.

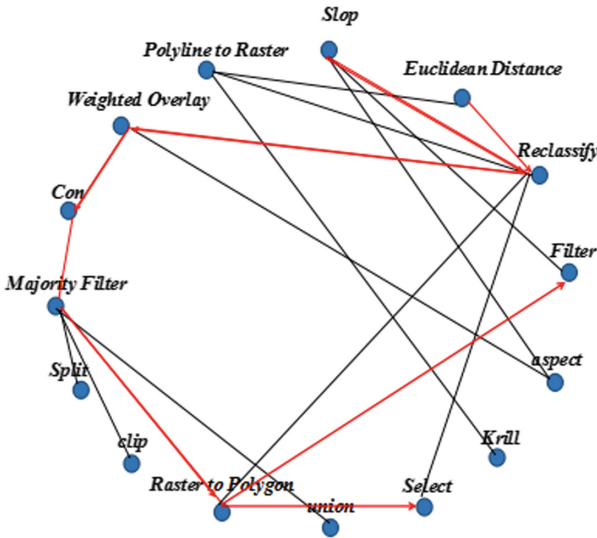


Fig. 5. The dynamic semantic network model.

5 Experiment

5.1 Dataset Description and Precision

In order to verify the effectiveness of our proposed method, we use the Java language to test the method and use MySQL database to store the data, which is conducted on a desktop with an Inter (R) Core (TM) i7-3770 CPU @ 3.40 GHz, 8.00 GB memory, and a 64-bit Windows 10 operating system.

The data uses 300 geoprocessing services organized by tree from ArcGIS Toolbox. In addition, 112 DAG rules, which represents the invocation rules between services based on different requirements, are found from numerous communities such as CSDN.

Our experimental results will be evaluated by precision and running times. The precision is computed as follows:

$$precision = \frac{DAG_P \cap DAG_R}{N} \quad (7)$$

In Eq. 7, DAG_P represents the DAG generated by our method and the DAG_R represent the right DAG that really meets the requirements of the user in the DAG rule set. N is the operation number contained in a DAG_P . To get a more correct value of precision, we proceed experiment with different user requirement for 112 times. The average precision is 76.4%.

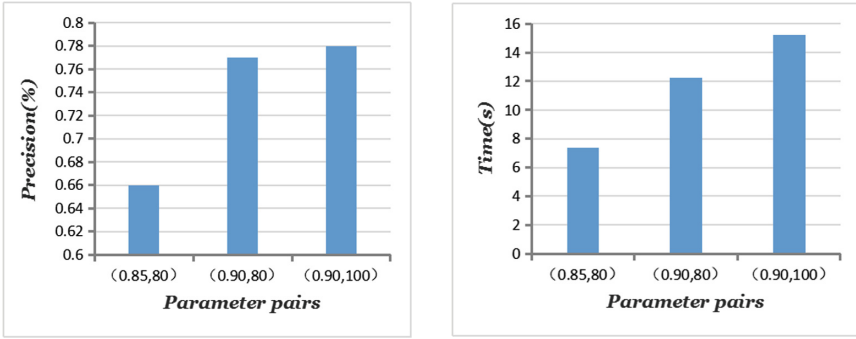
5.2 Impact of Parameters in Cooling Table

To investigate the effect of Cooling Table parameters in the proposed method in Algorithm 3. As show in Fig. 6, we set the parameters in the Cooling Table to three different sets of values and compared them.

The cooling Table contains four parameters t_0 , α , EPS and $ILOOP$. Normally, the values of t_0 and α are 1000 and 0, so we only consider α and $ILOOP$, which are denoted as $(\alpha, ILOOP)$ in Fig. 6. α represents the rate of temperature decay and $ILOOP$ represents the number of temperature drops in the same stage, which are mutually dependent. Although the higher value of α represents the better ability to cool the temperature in Fig. 6(a). It will also take a lot of times. For the same reason that higher value of $ILOOP$ will cost more computing resource in Fig. 6(b), the value of parameter $ILOOP$ should not be very large. Therefore, the experimental accuracy is relatively high and the computation time consumption is relatively small, when α is 0.9 and $ILOOP$ is 80.

5.3 Compare with Other Method

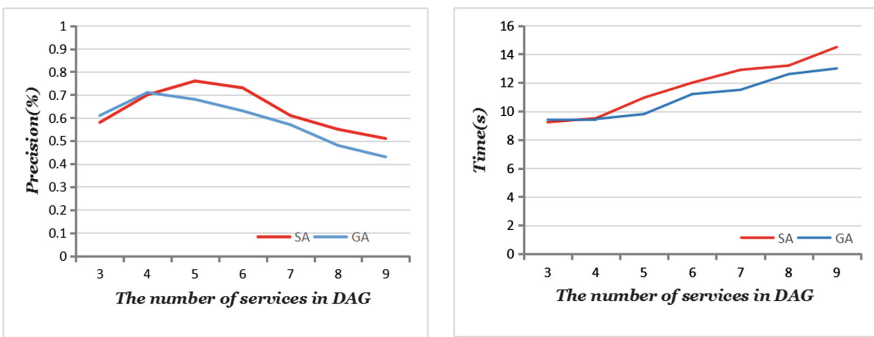
The number of services is varies from 3 to 9, so we consider the impact of the number of services on the service composition. We compare our method with the method proposed by the author in [16], which used the GA as heuristic optimization algorithm.



(a) Effect of Cooling Table on precision (b) Effect of Cooling Table on Running time

Fig. 6. Influence of parameters in cooling tables.

Figure 7 shows that the precision value reaches the peak value when the service number of DAG is from 4 to 6. The reason for this phenomenon are as follows. If a large number of services need to be found in the required DAG, but some detailed or transitional services may not be found during the actual execution, thus affecting the precision. That is the reason why precision decreases as the number of services increases. Because comparison method can only get services chain, the precision of our method is higher than compared one in Fig. 7(a). And as the number of services in the DAG increases, the service composition consumes more time. The reason why our method takes more time is that our graph structure solution is much more complex than chain structure in Fig. 7(b). But the usability of our proposal is much higher than the comparison one.



(a) Compare Precision for SA and GA (b) Compare Running time for SA and GA

Fig. 7. The precision and run time of proposed method.

6 Related Work

6.1 Service Composition Technology

Web services composition technology, aiming to provide added values by loosely coupling web services, has been used to efficiently find near-optimal composite services to satisfy users' requirements reasonably well [17]. The syntax-based service composition depends on the matching between selected keywords and Web service description [18], which takes little account of the semantics of web services. To get the concepts relationship, scholar use a certain criterion to measure the semantic distance in [19]. In [10], the authors proposed a novel Permutation-based Multifactorial Evolutionary Algorithm to solve the fully automated semantic service composition problem for diverse user segments with different QoS preferences. And the principle of [20,21] is that using ontology as a fundamental criterion to measuring the concept distance of the user's requirement and the services. The method of using ontology is not suitable for direct application in GIS domain, cause it's a hard work to construct the ontology. It is obviously that the accuracy of web services semantic annotations will significantly improve the effectiveness of the web service discovery, recommendation and composition [22]. In [11], the author proposed an invocation-based technique to verify the QoS accuracy by using annotations.

6.2 GIS Services Composition

The GIS domain service composition can be divided into three categories: semi-automated GIS services composition, syntax-based GIS services composition, and semantic GIS services composition. In [23], the author proposed the registration-binding-lookup mechanism, which is a semi-automated approach to service composition recommendation. In order to provide services to user automatically, some authors suggest that taking services context into consider. In [24], the authors proposed an active proxy, which can regard service context and user's requirement, extract useful information and send it to the server. But this method can only used in location-based service. In [25], the authors mapped the OWS input/output message to WSRF ResourceProperties, which could bring higher efficient. But this method doesn't incorporate many useful WSRF function. Besides, high performance data transfer is a challenge in GIS service.

7 Conclusion

The enhancement of Internet technologies has improved the technology in GIS services discovery, composition and recommendation. It is becoming increasingly important to combine GIS services to help users solve a various problems. Therefore, in this paper, we discusses the related technologies of service composition in GIS and computer fields, and analyzes the principles of these technologies. We

find that effective use of semantic information between services can improve the quality of service composition, which could meet the users' requirement better. To solve this problem, by using the tree organization structure of ArcGIS service, we can quickly select the set of services that meet the requirements according to the syntax matching relationship between services. To further explore the semantic correlation between services we use the NDG to build the dynamic semantic network. Then simulated annealing algorithm is used to find the DAG with high semantic value and recommend it to the user. Experiments show that our method could recommend a meaningful DAG with higher precision.

References

1. Scheider, S., Ballatore, A., Lemmens, R., Hartmann, S.: Finding and sharing GIS methods based on the questions they answer. *Int. J. Digit. Earth* **12**, 594–613 (2019). <https://doi.org/10.1080/17538947.2018.1470688>
2. Linn, K.N.Z., Lupin, S., Linn, H.H.: Analysis of the effectiveness of fire station locations using GIS-model. In: 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Saint Petersburg and Moscow, pp. 1840–1843. (2019). <https://doi.org/10.1109/EIConRus.2019.8657048>
3. Di, L.: Distributed geospatial information services-architectures, standards, and research issues. *Int. Arch. Photogramm. Remote. Sens. Spat. Inf. Sci. (Part 2)* (2004). <https://doi.org/10.4018/978-1-60960-192-8.ch001>
4. Sadeghiram, S., Ma, H., Chen, G.: Distance-guided GA-based approach to distributed data-intensive web service composition. arXiv preprint [arXiv:1901.05564](https://arxiv.org/abs/1901.05564). Arxiv (2019). <https://doi.org/10.1145/3319619.3322015>
5. Kamath, S., Ananthanarayana, V.S.: Discovering composable web services using functional semantics and service dependencies based on natural language requests. *Inf. Syst. Front.* **21**, 175–189 (2019). <https://doi.org/10.1007/s10796-017-9738-2>
6. Zhang, S., Wang, F.: GIS geoprocessing services search based on breadth-first reverse share pruning AND/OR tree algorithm. In: 2014 10th International Conference on Natural Computation (ICNC), vol. 12, pp. 850–855. IEEE (2014). <https://doi.org/10.1109/ICNC.2014.6975949>
7. Farzi, P., Akbari, R., Bushehrian, O.: Improving semantic web service discovery method based on QoS ontology. In: 2017 2nd Conference on Swarm Intelligence and Evolutionary Computation (CSIEC), pp. 72–76. IEEE (2017). <https://doi.org/10.1109/CSIEC.2017.7940175>
8. Yue, P., Di, L., Yang, W., Yu, G., Zhao, P.: Semantics-based automatic composition of geospatial web service chains. *Comput. Geosci.* **33**, 639–665 (2007). <https://doi.org/10.1016/j.cageo.2006.09.003>
9. Zaharia, R., Vasiliu, L., Hoffman, J., Klien, E.: Semantic execution meets geospatial web services: a pilot application. *Trans. GIS* **12**, 59–73 (2008). <https://doi.org/10.1111/j.1467-9671.2008.01135.x>
10. Țucăr, L., Diac, P.: Semantic web service composition based on graph search. *Procedia Comput. Sci.* **126**, 116–125 (2018). <https://doi.org/10.1016/j.procs.2018.07.215>
11. Huang, K., Zhang, J., Tan, W., Feng, Z., Chen, S.: Optimizing semantic annotations for web service invocation. *IEEE Trans. Serv. Comput.* **12**, 590–603 (2016). <https://doi.org/10.1109/TSC.2016.2612632>

12. Kulawiak, M., Dawidowicz, A., Pacholczyk, M.E.: Analysis of server-side and client-side web-GIS data processing methods on the example of JTS and JSTS using open data from OSM and geoportal. *Comput. Geosci.* **129**, 26–37 (2019). <https://doi.org/10.1016/j.cageo.2019.04.011>
13. Stein, C., Wein, J.: Approximating the minimum-cost maximum flow is P-complete. *Inf. Process. Lett.* **42**, 315–319 (2019). [https://doi.org/10.1016/0020-0190\(92\)90229-O](https://doi.org/10.1016/0020-0190(92)90229-O)
14. Zhou, Z., Cheng, Z., Zhang, L.-J., Gaaloul, W., Ning, K.: Scientific workflow clustering and recommendation leveraging layer hierarchical analysis. *IEEE Trans. Serv. Comput.* **11**, 169–183 (2018). <https://doi.org/10.1109/TSC.2016.2542805>
15. Zhou, Z., Cheng, Z., Ning, K., Li, W., Zhang, L.-J.: A sub-chain ranking and recommendation mechanism for facilitating geospatial web service composition. *Int. J. Web Serv. Res. (IJWSR)* **11**, 52–75 (2014). <https://doi.org/10.4018/ijwsr.2014070103>
16. Hu, B., Zhou, Z., Cheng, Z.: Web services recommendation leveraging semantic similarity computing. *Procedia Comput. Sci.* **129**, 35–44 (2018). <https://doi.org/10.1016/j.procs.2018.03.041>
17. Wang, C., Ma, H., Chen, G., Hartmann, S.: A memetic NSGA-II with EDA-based local search for fully automated multiobjective web service composition. In: *Genetic and Evolutionary Computation Conference Companion*, vol. 11, pp. 52–75. ResearchGate (2019). <https://doi.org/10.1145/3319619.3321937>
18. Cheng, B., Li, C., Zhao, S., Chen, J.: Semantics mining & indexing-based rapid web services discovery framework. *IEEE Trans. Serv. Comput.*, 1. (2018). <https://doi.org/10.1109/TSC.2018.2831678>
19. Wang, C., Ma, H., Chen, G., Hartmann, S.: Evolutionary multitasking for semantic web service composition, pp. 2490–2497. arXiv preprint [arXiv:1902.06370](https://arxiv.org/abs/1902.06370). arxiv.org (2019). <https://doi.org/10.1145/2481492.2481495>
20. Arul, U., Prakash, S.: A unified algorithm to automatic semantic composition using multilevel workflow orchestration. *Clust. Comput.* **126**, 1–22 (2018). <https://doi.org/10.1007/s10586-018-2604-2>
21. Fellah, A., Malki, M., Elci, A.: A similarity measure across ontologies for web services discovery. In: *Web Services: Concepts, Methodologies, Tools, and Applications*, pp. 859–881. IGI-Global (2019). <https://doi.org/10.4018/978-1-5225-7501-6.ch047>
22. Derczynski, L., Maynard, D., Aswani, N., Bontcheva, K.: Microblog-genre noise and impact on semantic annotation accuracy. In: *Proceedings of the 24th ACM Conference on Hypertext and Social Media*, pp. 21–30. DLACM (2013). <https://doi.org/10.1145/2481492.2481495>
23. Wenjue, J., Jianya, G., Bin, L.: GIS integration and interoperability based on GIS service chain. In: *Proceedings of the 2005 IEEE International Geoscience and Remote Sensing Symposium, IGARSS 2005*, vol. 7, pp. 4962–4965. IEEE(2005). <https://doi.org/10.1109/IGARSS.2005.1526788>
24. Li, X., Shin, W., Li, L., Yoo, S.B.: GIS web service using context information in mobile environments. In: Gavrilova, M., et al. (eds.) *ICCSA 2006*. LNCS, vol. 3980, pp. 895–903. Springer, Heidelberg (2006). https://doi.org/10.1007/11751540_97
25. Gui, Z., Song, K.: Building improved GIS service based on WSRF. In: *2008 International Conference on Internet Computing in Science and Engineering*, vol. 33, pp. 274–277. IEEE (2008). <https://doi.org/10.1109/ICICSE.2008.12>



Designing Public Digital Cultural Service Interactive System Based on Reality–Based Interaction Principles

Jinhua Dou^{1,2}(✉)

¹ School of Art and Design, Tianjin University of Technology, Tianjin, China

² School of Computer and Communication Engineering,
University of Science and Technology Beijing, Beijing, China
Doujinhua.6971@163.com

Abstract. Internet of Things (IoT), big data, artificial intelligence (AI), and the new media environment have changed the traditional pattern of communication in public cultural service. Public digital cultural service (PDCS) system is a kind of cyber physical system that integrates physical and digital cultural resources. The public could access cultural knowledge more conveniently from the PDCS system. However, there are existing of some accessibility issues in the interactive process between the public cultural service digital terminals and users. This paper explored methods of designing PDCS interactive system using reality-based interaction (RBI) principles to enhance the user experience. RBI principles using in PDCS provides natural communication and displays ways, which are helpful in solving the problem of traditional public culture service transmission. The proposed methods supply the intelligent services according to the different information input by users such as the actions, facial expressions, voice, and physiological signals. User's context is also considered. At the same time, public cultural service data is obtained, analyzed and visualized to provide public digital cultural knowledge to users. In this way, the general population and special groups like the elderly people could use the PDCS interactive system without any obstacles. The research is helpful to improve the accessibility and usability of PDCS system.

Keywords: Reality–Based Interaction (RBI) · Interactive system · User experience · Public Digital Cultural Service (PDCS) · Accessibility

1 Introduction

The aims of public cultural service are to meet the cultural needs of the public. With the development of social economy, the public cultural service has developed rapidly which provides the public with cultural products and services, as well as its related regulations and systems in general [1]. The public service areas discussed in this paper are mainly including museums, libraries, art galleries, cultural centers, intangible cultural heritage administrations and other nonprofit public service institutions. Public digital culture service (PDCS) is a kind of cyber physical system that integrates physical and digital cultural resources. The goal of the public digital cultural services is

to provide rich and convenient digital cultural services for all kinds of people. It is of great significance to enhance the efficiency and quality of public cultural service [2].

Information technology like big data, artificial intelligent (AI) are helpful in providing new contents and forms for the public digital cultural service. Media is everywhere in the new media environment by-network TV, computers, mobile devices and users can obtain information anytime and anywhere. People would like to participate the information building, feedback and dissemination instead of simple information receiving in new media environment. However, a series of problems are also produced accompany with the universal usage of new media and digital technology. Massive data are generated with the rapid expansion of cultural information. People can't find the desired knowledge quickly among the massive public culture data. The public digital cultural service aims at both the ordinary people and the special groups, such as the elderly people, the disabled people, and the people with low education. But some existing digital service systems are difficult to operate, especially for some special groups. Persons with disabilities such as the blind, limbs disabled people often have obstacles in using digital service system [3–7]. These factors affect the usage experience of the public, leading to low usage intention and few interesting for public digital cultural service.

To address these issues, we studied interactive methods to enhance the user experience of public digital cultural service. Different methods and technologies of human computer interaction (HCI) based on reality-based interaction (RBI) principles were explored in this paper. Smart interaction services and user interfaces were designed which could facilitate the cultural cognition of public. In this way, the interactive system of public digital cultural service became more intelligent and the accessibility of it was greatly improved.

The rest of the paper is organized as follows. Section 2 introduces the related work of PDCS interactive system. Technology architecture of PDCS interactive system based on RBI principles is proposed in Sect. 3. Section 4 studies the key technology and methods of the PDCS interactive system based on RBI principles. Section 5 presents a case study. Finally, conclusion and future work are given in Sect. 6.

2 Related Work

The main public cultural institutions include museums, libraries, art galleries and cultural heritage management institutions. Many scholars and cultural service institutions had done the research work to explore the innovative interactive form of digital culture service.

Carrozzino et al. [8] presented a 3D virtual interactive platform to protect the intangible cultural heritage and traditional technologies through the virtual display of bronze sculpture manufacturing process. Kiourt et al. [9] presented DynaMus, a novel fully dynamic web-based virtual museum framework that relied entirely on user creativity and rich content of web-based resources. Cianciarulo [10] described an experimental augmented reality project in a small museum in Viggiano (Basilicata, Italy) and explained the use of augmented reality (AR) technology to change the perception of small local museums. Rattananungrot et al. [11] developed a service-oriented mobile

AR architecture for a variety of applications, such as museum interaction or web applications. Shichinohe et al. [12] introduced the augmented calligraphy system that could give feedback to learners. Some notice was given when learner's posture moved into a bad shape by this system. With this, the learners could learn by themselves. Soontornvorn et al. [13] developed a system for training human calligraphy skills utilizing AR technology and dynamic font method. The dynamic font was used to generate a model character. The AR technology was used to produce visual information consisting of not only static writing path but also dynamic writing process of model character. The Palace Museum used virtual reality technology in multi-scene interactive exhibitions of Duanmen digital museum. Google, in conjunction with the British Museum, built virtual reality museums.

Soga et al. [14] created video content for a special exhibition at Nerikuyo. A virtual fitting system had been proposed that could identify a user's gestures or poses and provide virtual fitting. Baraldi et al. [15] developed a system which could provide a more natural and interesting way of accessing museum knowledge based on distributed self-gesture and picture recognition. Saha et al. [16] proposed gesture recognition algorithm for Indian Classical Dance Style using Kinect sensor, which recognized body gestures and obtain higher recognition accuracy. Khan and de Byl [17] proposed a system based on motion detection technology that allowed children to be in a heritage-related environment to create awareness of local dance movements.

Kolay [18] had explored new media, such as game design and animation, to educate the target audience by translating the visual language of Indian local art forms. Hashim et al. [19] proposed the integration of technical and cultural heritage that could create innovative museum's display, providing the best knowledge and interactively understand experience to meet the public's needs. Zongming and Wenjin [20] constructed the digital platform module of Chinese traditional furniture culture. Papangelis et al. [21] presented a 3-phase model for the design, development and application of mobile technologies within cultural heritage projects. Yeung et al. [22] proposed a novel multimedia human computer interface that allowed untrained users to write with the physical hairy brushes in a virtual paper. Vaz et al. [23] presented the design of a tangible user interface to enhance the experience of visitors with visual impairments. Yang et al. [24] presented an integrated, interchangeable visualization approach used in public culture service system. Intuitive and efficient views for cultural topic popularity, topic contents, document clusters, and relationships between cultural topics and document clusters were provided.

The above research works are all based on modern information technology. Virtual and augmented reality technology has been widely used in the museum for cultural heritage communication. Game and animation, digital service platforms, gesture recognition and tangible user interface are also applied to public culture display and transmission, which could give people a novel experience. However, the interaction form between human and service system is still not natural enough.

Reality-Based Interaction (RBI) [25, 26] put forward the new thinking of human-computer interaction. It redefined the understanding of computer and interaction, and realized the universal perception of the physical world, such as gravity, friction, and scaling; the perception of body consciousness, i.e. the human perception of their own bodies, perception of their ability to control and coordinate the body; the perception of

the surrounding environment, and the ability to operate and navigate in the environment; the perception of others in the environment, and other human interactions. The reality-based interface stems from user’s original skills and expectations from the real world instead of trained computer skills. RBI principles provide a more natural interaction paradigm. We will explore the methods and the key technology to realize the interactive system of PDCS based on RBI principles in this paper.

3 PDCS Interactive System Architecture Based on RBI Principles

Human interact with themselves and the real outside world through the vision, hearing, touch, taste, smell and intuition. As shown in Fig. 1, RBI imitates the interaction of the real world based on the user’s prior knowledge, which is a critical factor for interaction with a new product [27, 28]. It is an intuitive natural human-computer interaction paradigm, as well as visual language and interactive forms. We propose to design natural interactive system for PDCS based on user’s prior knowledge and the ways people interact with themselves and the outside world. Users operate PDCS interactive system like they communication in real world, e.g. input and output information through vision, hearing, touch, taste, smell and intuition.

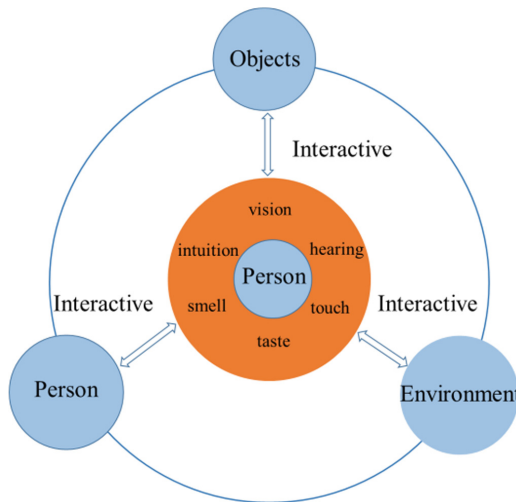


Fig. 1. Interaction among person, object and environment

Our PDCS interactive system follows the RBI interaction paradigms between human and physical world, between human and body consciousness, between human and environment, and enables the users to perceive the external world more intuitively. The intelligent system may have the human intention expression and perception ability that can realize the human behaviors, tasks, intention, emotion and environment.

Combining with content of service system terminals, the intelligent service system can provide more intuitive information expression, effective feedback as well as the needed service content and interactive experience for users. These methods can promote the public cultural service communication more effectively, as shown in Fig. 2.

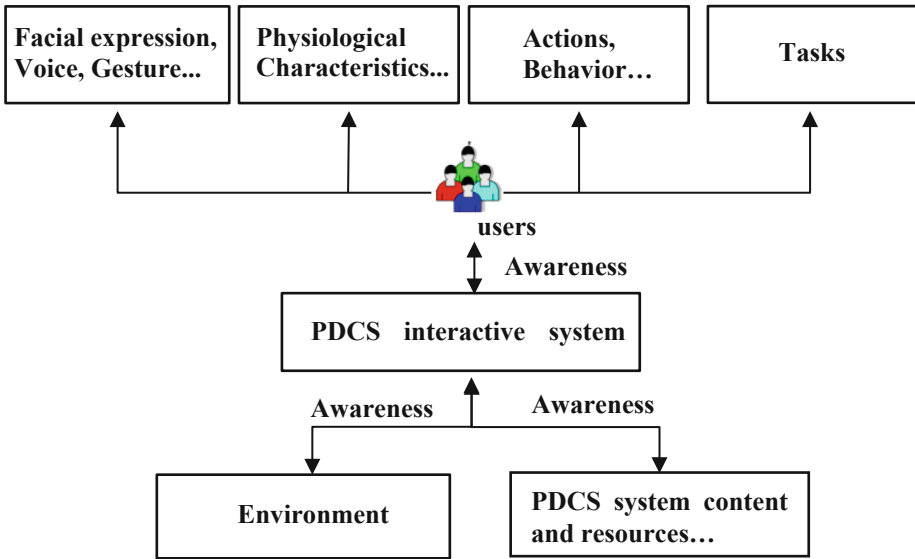


Fig. 2. PDCS interactive system based on RBI principles

The technology architecture of PDCS interactive system is presented, as shown in Fig. 3. The context data in interactive process, user emotional data, user conscious data and big data of public culture service are collected in data acquisition layer. Some knowledge reasoning rules including context awareness computing, affective computing, brain-computer interface technology and data mining technology are adopted to extract the cultural service knowledge. The function and service content of intelligent interactive system of PDCS are produced based on the extracted knowledge patterns. Finally, the natural PDCS interactive system is constructed and intelligent public cultural service content is provided to users.

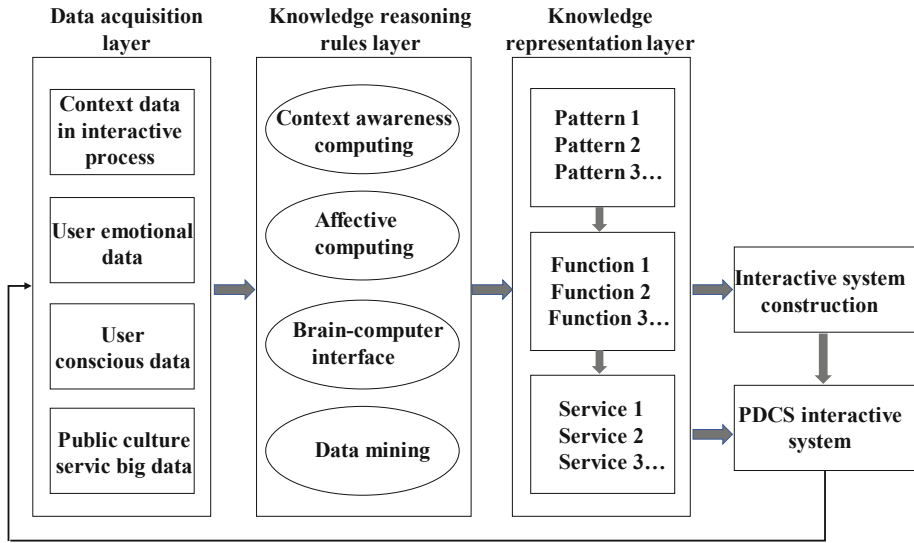


Fig. 3. Technology architecture of PDCS interactive system

4 The Key Technology and Methods of RBI Interactive System for Public Digital Culture Service

4.1 PDCS Interactive System Based on Affective Computing

People hope to communicate with the computer as easy as human communication. The most difficult problem of the human-computer interaction is how to teach computers understand human emotion. Affective computing is a calculation method that is related to emotion, derived from emotion or can affect emotion [29, 30]. Affective computing creates a computing system that senses, identifies, and interprets human emotions intelligently, empowering computers to observe, understand, and generate various emotional features like human do. Affective computing plays an important role in improving the natural and harmonious of human-computer interaction.

Moods and emotions are a subjective internal emotional experience. We obtain user emotional data by collecting physiological and psychological feature data, e.g. voice, postures, facial expressions, and physiological signals from the users of PDCS interactive system. Some devices include eye trackers, sensors and behavioral analysis instruments are used. Data preprocessing, feature extraction, and feature selection are executed based on the obtained physiological signal, expression, voice, and posture data. The emotion model of ordinary users and special groups, such as the elderly, the disabled, and the patients, is constructed using the methods such as OCC emotional model, Kismet emotional model, HMM emotional model, and the emotion generation mechanism in psychological research. By selecting the affective computing models and optimizing it, the emotion recognition rate can be improved and the recognition result can be obtained. By this means, the PDCS interaction system can understand user's

emotion and make appropriate response. Based on the construction of emotion signal recognition result and emotion model, the intelligent interactive terminals of PDCS system with emotion understanding and feedback function is constructed. The system can perceive the user’s emotions and context to infer the emotional state, e.g. when the PDCS interactive system perceives the user’s frustration, then the public cultural service content can be adjusted to be more reasonable and easier to use. The architecture of PDCS interactive system based on affective computing technology is shown in Fig. 4.

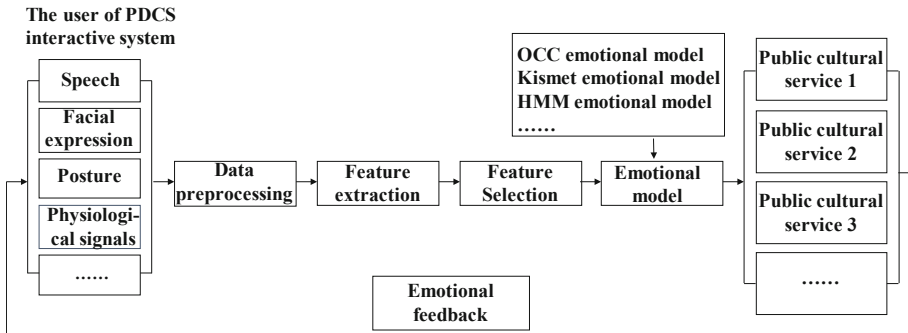


Fig. 4. The architecture of PDCS interactive system based on affective computing technology

4.2 PDCS Interactive System Based on Context Awareness

The trigger and development of human emotion are inseparable from the context. When operating the product service terminals, the context adaptation brings the dynamic update to meet user needs. Real-time perception of the context can further clarify the user’s emotional and internal needs. We divide the context type into user context, environment context, task context, and device context. The context data include user context data, such as the physiological and psychological context data of users. Environmental context data include various factors, such as location, time, temperature, light, and other environmental data. Task context data indicate the tasks and related activities to be done. Device context data describe the type and operation status of the device.

We obtain context data using the context awareness measurement instruments, e.g. wireless sensor, behavior measurement system, video recording device, GPS and eye tracker. Context awareness computing [31–33] technology is adopted. The acquired context data are processed, then calculated and analyzed. The system can reason and extract the context information around the users. It can also visualize the context information. Hence, the PDCS interactive system can acquire and understand the context and user needs, and provide appropriate service application needed by the user, so that the service is more natural and humane. The architecture of PDCS interactive system based on context awareness technology is shown in Fig. 5.

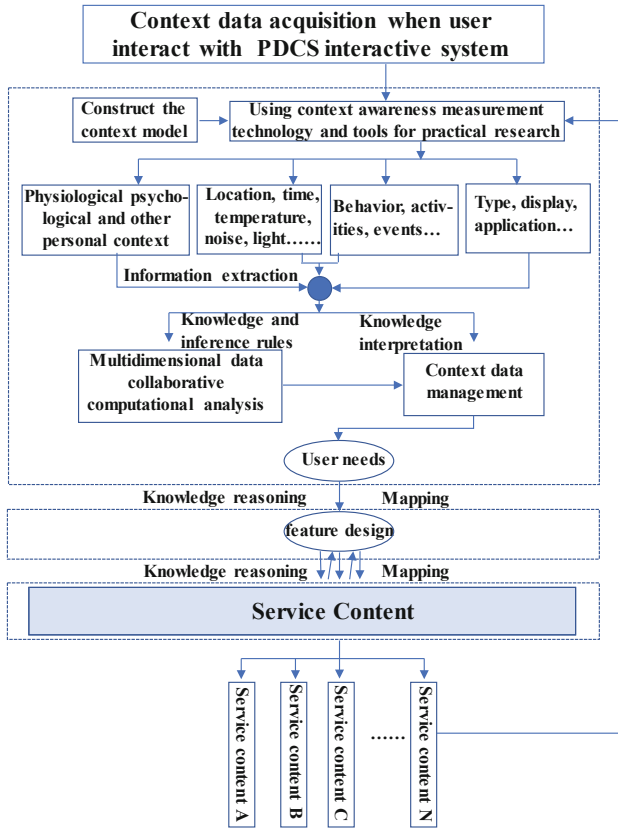


Fig. 5. The architecture of PDCS interactive system based on context awareness technology

4.3 The Natural Interactive System of PDCS Based on Brain-Computer Interface

Brain-Computer Interface (BCI) is able to transfer and use information from distinct brain states for communicating with an external device, so to enhance people’s ability to manipulate external systems [34]. BCI technology can achieve better natural user interaction with the product service system. In the medical, neuroergonomics and intelligent environment, game entertainment, security and certification fields have broad application prospects [35]. The user can interact with the service system through the brain nerve signal, and communicate with the external environment. The application of brain-computer interface technology in the field of public cultural services is of great significance to the disabled and the elderly, who are the disadvantaged groups. The EEG signals are measured by magnetic resonance imaging (MRI) and ultrasound projection. The brain signal preprocessing, removal of clutter, artifacts and noise, are followed by feature extraction and classification, and ultimately into control instructions for external devices, to achieve the public digital cultural services interactive system of intelligent control and the feedback to the brain, as shown in Fig. 6.

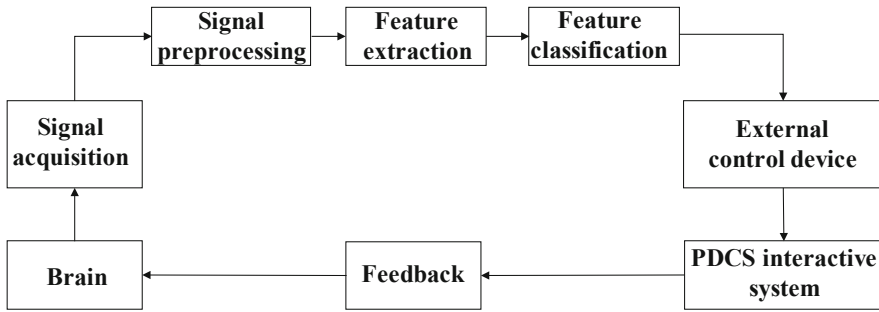


Fig. 6. The architecture of PDCS interactive system based on BCI technology

4.4 Big Data for PDCS Interactive System

In the new media environment, the users are diverse and dispersed. The public service agencies and government can hardly obtain the user's requirements dynamically. On the other hand, users can hardly identify the authenticity of data due to the diversity and complexity of information. In this case, it needs the personalized content services because users cannot quickly obtain the desired knowledge. The PDCS system provides content services through various new media terminals. Tremendous data are generated in this process and we can discover the hidden values by mining the big data.

4.4.1 Data Collection for Public Digital Cultural Service

Public cultural services data comes from various resources including traditional paper media, the network sources, the public cultural experience equipment, cultural institutions, big data platform and other data source. Data from network sources mainly includes data generated in cyberspace, such as public cultural service-related websites, WeChat, microblog, blog, social network. Network data are mainly obtained by the web crawler technology in the case of obtaining permission from the website.

Service end-user data from digital cultural experience equipment, e.g. network TV, mobile phone, and cultural experience terminals mainly includes users' physiological, psychological and behavioural data. Service end-user physiological, psychological and behavioural data can be obtained by sensors, eye tracking, video surveillance, and other technologies.

All kinds of public cultural services data from cultural institutions mainly include data collection through a specific access interface and other related means, e.g. a unified data access interface based on RESTful API (Application Programming Interface). OCR (Optical Character Recognition) technology is adopted to collect the data from traditional paper media to realize the public culture digitization.

The data from big data platform mainly include the data generated automatically by the public digital cultural national sharing service platform. This part of the data is the most objective and truthfully records the visiting heat of the platform, the operating efficiency and fault of the platform, and the interaction between users and public cultural service platform. The data from big data platform mainly include the log data of the platform, and the user behavior data, such as search, browsing content, browsing

time, scoring, commenting, favorites operating, adding resources to access the list of expectations, and its shared services platform, such as participation in the discussion, communication through BBS platform, user interaction, and all other behavioral data. The data are collected by the user detailed behavior data capture software running on the platform.

The data from other data sources are collected by using website public API, a specific system interface working with enterprise or research organization, DPI (Deep Packet Inspection) or DFI (Deep/Dynamic Flow Inspection) and other bandwidth management technology. Figure 7 shows the data sources and collection techniques for public digital cultural service.

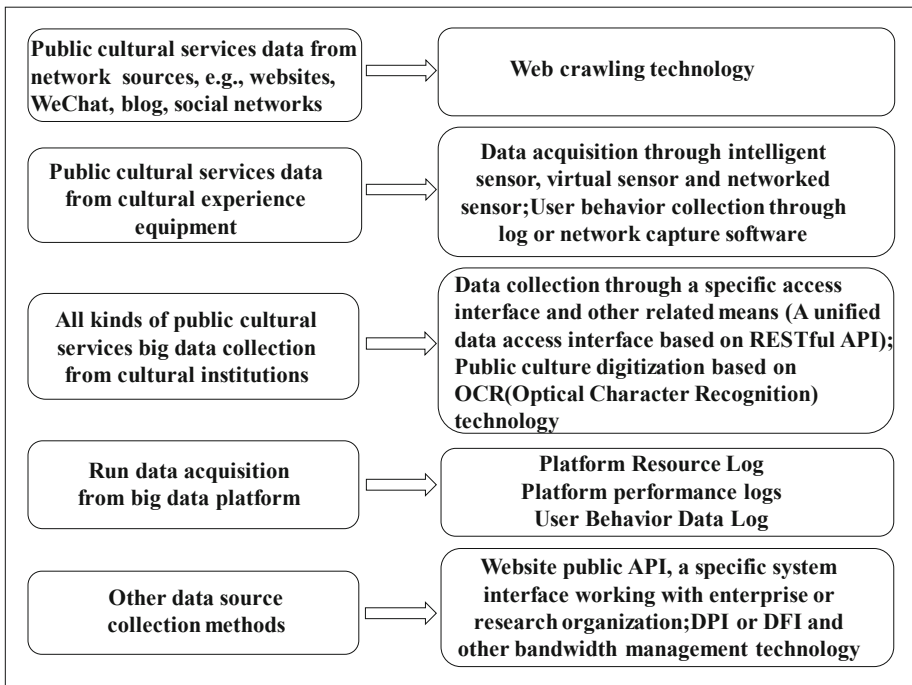


Fig. 7. The data sources and collection techniques for public digital cultural service

4.4.2 Data Analysis for Public Digital Cultural Service

Data analysis is important for the enhancement of the quality and efficacy of public digital cultural service. Analyzing public digital culture data can obtain user behaviour and preferences. It can help public cultural management department better understand the needs of user and provide service content to users. The culture distribution, communication trends, existing problems and other public culture knowledge can also be presented by analyzing various public culture data.

Data including structured data, semi-structured data and unstructured data are collected from various resources. The obtained data must be cleaned, converted, and

stored. Apache Spark [36, 37] algorithm based on Hadoop [38, 39] technology is used to realize the data clean quickly. The distributed messaging system Apache Kafka [40] serves as a data buffer between data cleaning and data loading. The preprocessed data will be sent to Kafka for temporary storage.

Data mining [41] is the computing process of discovering patterns in large data sets. It aims at extracting information from a data set and transforming it into an understandable structure for further use. Some commonly used data mining methods like statistical analysis, association analysis, sequence pattern analysis, classification analysis, and cluster analysis are adopted in public digital cultural service platform. Figure 8 shows the extracted interesting, implicit and potentially useful patterns or knowledge from the public cultural service data, such as resource visiting heat, regional resource access characteristics, and different time periods of resource access features, public cultural hot spots, and user’s personalized needs, resource allocation of public culture big data platform.

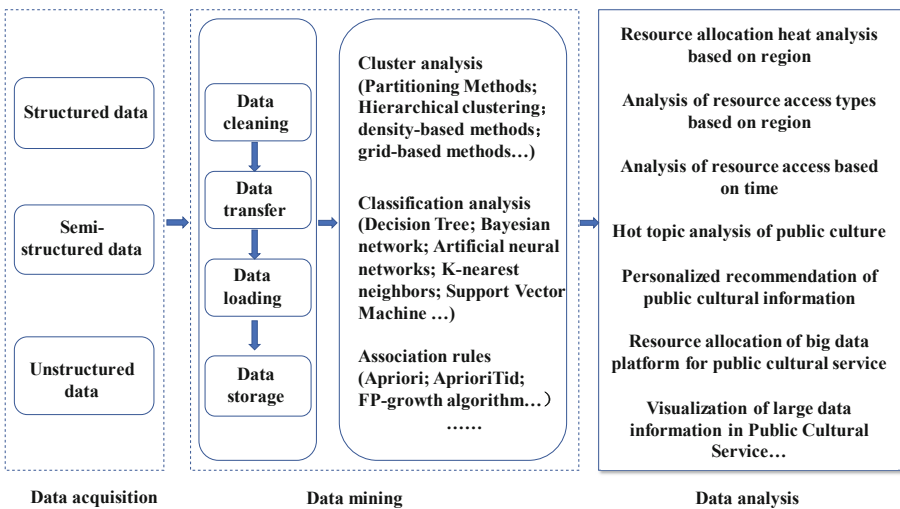


Fig. 8. Data analysis for public digital cultural service

Information visualization aims at conveying abstract information in intuitive ways and producing interactive visual representations of abstract data to reinforce human cognition [42]. The information visualization model [43, 44] is explored to provide a reference method for the visualization of public cultural information. The interactive visualization of the analysis process allows the user to perform more accurate data analysis. It can greatly improve the efficiency of public culture data understanding and analysis.

PDCS interactive system based on RBI principles provide natural and intuitive interface for various user groups. The affective computing, context awareness, brain-computer interface and big data mining technology are applied to the PDCS interactive system. The smart system can intelligently perceive user’s mood, emotion, conscious,

context, service content and so on. The real state and requirement of the user in the process of interacting with the PDCS interactive system are analyzed, and the function and service of the user demand are provided under the support of the ubiquitous computing. A large amount of public cultural information can also be presented by visualization so as the users can find the public cultural knowledge quickly. These methods can effectively enhance the user experience of the PDCS interactive system.

5 Case: Intelligent Square Dance Service System

The square dance is organized spontaneously by the residents. It is a dance for the purpose of recreation and fitness. The activities are mostly carried out in open spaces such as squares and dams. The square dance has a wide participation group, and the middle-aged and elderly people are the main groups. Square dance provides dynamic music and rich content, which has become the most popular form of dance.

The popularity of square dance in China has caused many problems, the main problems as follows:

- The number of participants in the square dance is large, and the sound of music equipment is loud, which creates noise and interferes with the lives of people around.
- The venue and time of dancing are not fixed, which brings trouble to the organization of the square dance activities.
- Square dance teachers lack professional knowledge. The teacher's posture is not easy to see when the learner's position is far away from the teacher, which affects the learning effect.

In view of the existing problems, we proposed intelligent square dance service system. The interactive system was designed based on the RBI principles. Some technologies including virtual display, context awareness and motion capture were adopted to achieve the smart interactive system.

The display screen and Kinect camera were adopted to construct the interaction environment and physical interface of new media interactive system. The intelligent square dance service system provides rich square dance resources such as different types of square dance videos and square dance teaching resources, which could bring a novel experience to participant.

The intelligent square dance service system based on context awareness technology can perceive the external environment and time. Then, the system can automatically adjust the sound constraint range and music volume according to changes in the external environment. The system can also perceive the dancer's context and provide appropriate teaching content to the users. It can perceive dancer's location, actions and emotion state by GPS, wireless sensor and camera. For example, when the dancer learns difficult or their posture is not standard, the square dance system will intelligently adjust the learning content, e.g. Repeatedly playing the difficult dance moves.



Fig. 9. Interactive scene of intelligent square dance service

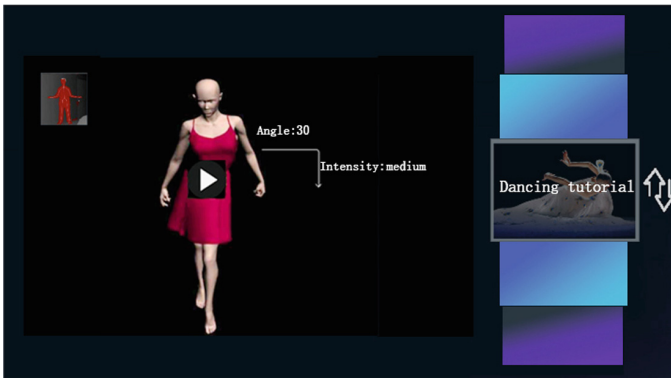


Fig. 10. Interactive content of dance teaching section

In the dance teaching section, the system provides a real-time virtual human based on Kinect technology. The dancer can control the virtual human's activities using motion capture technology. The dancer's movement of head, hands and legs will be captured by Kinect camera and drive the action of the virtual human. Thus, the dance teaching actions are shown in the big screen in front of all participants. The prototype for interactive scene and content of square dance service system are shown in Figs. 9 and 10.

6 Conclusions

This paper proposed interactive system design method based on RBI principles for PDCS interactive system. The key technology of PDCS interactive system based on RBI principles was explored in this study. We presented the architecture of natural PDCS interactive system by using big data mining, context awareness computing,

affective computing, and brain-computer interface computing. A natural PDCS interaction system was explored. The PDCS System based on RBI principles presented the rich service content and intelligent interactive interface, which can improve the user experience of public service.

Acknowledgements. We would like to thank Bingxuan Fan students who helped in the completion of intelligent square dance interactive system design. Funding: This work was supported by the Ministry of Education Humanities and Social Sciences Research Youth Fund Project [grant numbers 15YJCZH034].

References

1. Cao, A.J., Yang, P.: Theory and Practice of Public Cultural Service, 1st edn. Science Press, Beijing (2011)
2. Ministry of Culture and Ministry of Finance: Guiding Opinions on Further Strengthening the Construction of Public Digital Culture. <http://www.mcprc.gov.cn>. Accessed 12 Dec 2018
3. Barnard, Y., Bradley, M.D., Hodgson, F., Lloyd, A.D.: Learning to use new technologies by older adults: perceived difficulties, experimentation behavior and usability. *Comput. Hum. Behav.* **29**(4), 1715–1724 (2013)
4. Im, H., Jung, J., Kim, Y., Shin, D.H.: Factors affecting resistance and intention to use the smart TV. *J. Media Bus. Stud.* **11**(3), 23–42 (2014)
5. Helbig, N., Gil-Garcia, J.R., Ferro, E.: Understanding the complexity of electronic government: implications from the digital divide literature. *Gov. Inf. Q.* **26**(1), 89–97 (2009)
6. Duplaga, M.: Digital divide among people with disabilities: analysis of data from a nationwide study for determinants of internet use and activities performed online. *PLoS ONE* **12**(6), 1–19 (2017)
7. Fox, S.: Americans living with disability and their technology profile. Pew Research Center (2011)
8. Carrozzino, M.: Virtually preserving the intangible heritage of artistic handicraft. *J. Cult. Herit.* **12**(1), 82–87 (2011)
9. Kiourt, C., Koutsoudis, A., Pavlidis, G.: DynaMus: a fully dynamic 3D virtual museum framework. *J. Cult. Herit.* **22**, 984–991 (2016)
10. Cianciarulo, D.: From local traditions to “Augmented Reality”. The MUVIG Museum of Viggiano (Italy). *Procedia Soc. Behav. Sci.* **188**, 138–143 (2015)
11. Rattanaarungrot, S., White, M., Jackson, B.: The application of service orientation on a mobile AR platform—a museum scenario. In: 2015 Digital Heritage, Conference 2015. LNCS, vol. 1, pp. 329–332. IEEE, New York (2015)
12. Shichinohe, T., Yamabe, T., Iwata, T., Nakajima, T.: Augmented calligraphy: experimental feedback design for writing skill development. *Int. J. Image Graph.* **8**(8), 473–493 (2011)
13. Soontornvorn, R., Pongkarn, S., Fujioka, H.: A development of AR calligraphy skill training system using dynamic font. In: International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), pp. 555–558 (2015)
14. Soga, A., Niwa, Y., Shiba, M., Okada, Y.: Digital archive and exhibiting methods of a buddhist ceremonial procession. In: 2013 International Conference on Signal-Image Technology & Internet-Based Systems, pp. 372–377 (2013)
15. Baraldi, L., Paci, F., Serra, G., Benini, L., Cucchiara, R.: Gesture recognition using wearable vision sensors to enhance visitors’ museum experiences. *IEEE Sens. J.* **15**(5), 2705–2714 (2015)

16. Saha, S., Ghosh, S., Konar, A., Nagar, A.K.: Gesture recognition from Indian classical dance using kinect sensor. In: 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, pp. 3–8 (2013)
17. Khan, M., De Byl, P.: Creating tangible cultural learning opportunities for indigenous dance with motion detecting technologies. In: Games Innovation Conference, pp. 1–3. IEEE (2012)
18. Kolay, S.: Cultural heritage preservation of traditional Indian art through virtual new-media. *Procedia Soc. Behav. Sci.* **225**, 309–320 (2016)
19. Hashim, A.F., Taib, M.Z.M., Alias, A.: The integration of interactive display method and heritage exhibition at museum. *Procedia Soc. Behav. Sci.* **153**, 308–316 (2014)
20. Zongming, L., Wenjin, L.: Construction and international popularization of digital platform for Chinese traditional furniture culture. In: 2016 Eighth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), pp. 162–166 (2016)
21. Papangelis, K., Chamberlain, A., Liang, H.N.: New directions for preserving intangible cultural heritage through the use of mobile technologies. In: Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct (MobileHCI 2016), pp. 964–967 (2016)
22. Yeung, C.H., Au, O.C., Tu, S.F., Wu, Y., Luo, E.: Multimedia human computer interface for oriental calligraphies. In: International Symposium on Intelligent Signal Processing and Communication Systems, Conference 2011. LNCS, pp. 1–4. IEEE, New York (2011)
23. Vaz, R.I.F., Fernandes, P.O., Veiga, A.C.R.: Proposal of a tangible user interface to enhance accessibility in geological exhibitions and the experience of museum visitors. *Procedia Comput. Sci.* **100**, 832–839 (2016)
24. Yang, Y., Wang, J., Huang, W., Zhang, G.: TopicPie: an interactive visualization for LDA-based topic analysis. In: IEEE Second International Conference on Multimedia Big Data, pp. 25–28 (2016)
25. Jacob, R.J.K., et al.: Reality-based interaction: unifying the new generation of interaction styles. In: Extended Abstracts Proceedings of the 2007 Conference on Human Factors in Computing Systems (CHI 2007), pp. 2465–2470 (2007)
26. Jacob, R.J.K., et al.: Reality-based interaction: a framework for post-WIMP interfaces. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2008), pp. 201–210 (2008)
27. Shaer, O., Jacob, R.J.K.: A visual language for programming reality-based interaction. In: Visual Languages and Human-Centric Computing, Conference 2006. LNCS, pp. 244–245. IEEE, New York (2006)
28. Lewis, T., Langdon, P.M., Clarkson, P.J.: Prior experience of domestic microwave cooker interfaces: a user study. In: Langdon, P., Clarkson, J., Robinson, P. (eds.) *Designing Inclusive Futures*, pp. 95–106. Springer, London (2008). https://doi.org/10.1007/978-1-84800-211-1_10
29. Picard, R.W.: *Affective Computing*. MIT Press, London (1995)
30. Picard, R.W.: Surprising discoveries from affective computing. In: The Fifteenth Conference on Computing in Twenty-First Century (2013)
31. Schilit, B., Adams, N., Want, R.: Context-aware computing applications. In: IEEE Workshop on Mobile Computing Systems and Applications, pp. 85–90 (1994)
32. Abowd, G.D., Dey, A.K., Brown, P.J., Davies, N., Smith, M., Steggle, P.: Towards a better understanding of context and context-awareness. In: Gellersen, H.W. (ed.) *HUC 1999*. LNCS, vol. 1707, pp. 304–307. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48157-5_29
33. Kaltz, J.W., Ziegler, J., Lohmann, S.: Context-aware web engineering: modeling and applications. *Revue d'Intelligence Artificielle* **19**(3), 439–458 (2005)
34. Schalk, G.: Brain-computer symbiosis. *J. Neural Eng.* **5**(1), 1–15 (2008)

35. Abdulkader, S.N., Atia, A., Mostafa, M.S.M.: Brain computer interfacing: applications and challenges. *Egypt. Inform. J.* **16**, 213–230 (2015)
36. Zaharia, M., Chowdhury, M., Franklin, M.J., Shenker, S., Stoica, I.: Spark: cluster computing with working sets. In: *Proceeding HotCloud 2010 Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing*, pp. 1–10 (2010)
37. Zaharia, M., et al.: Resilient distributed datasets: a fault-tolerant abstraction for in-memory cluster computing. In: *USENIX Conference on Networked Systems Design and Implementation*, vol. 70, pp. 1–2 (2012)
38. Shvachko, K., Hairong, K., Radia, S., Chansler, R.: The hadoop distributed file system: Mass Storage Systems and Technologies (MSST). In: *2010 IEEE 26th Symposium*, pp. 1–10 (2010)
39. White, T.: *Hadoop: The Definitive Guide*. O'Reilly Media Inc, California (2012)
40. Kreps, J., Narkhede, N., Rao, J.: Kafka: a distributed messaging system for log processing. In: *Proceedings of 6th International Workshop on Networking Meets Databases (NetDB)*. ACM (2011)
41. Han, J., Kamber, M., Pei, J.: *Data Mining: Concepts and Techniques*, 3rd edn. Morgan Kaufmann, San Francisco (2011)
42. Bederson, B.B., Shneiderman, B.: *The Craft of Information Visualization: Readings and Reflections*. Morgan Kaufmann, San Francisco (2003)
43. Card, S.K., Mackinlay, J.D., Shneiderman, B.: *Readings in Information Visualization: Using Vision to Think*. Morgan Kaufmann, San Francisco (1999)
44. Chi, E.H.: A taxonomy of visualization techniques using the data state reference model. In: *IEEE Symposium on Information Visualization Infovis*, pp. 69–75. IEEE, New York (2000)



Modeling and Verification of Resource-Oriented Internet of Things Services with Context Constraints

Lei Yu^{1,2(✉)}, Yang Lu³, BenHong Zhang³, Ya Li¹,
FangLiang Huang¹, YuLian Shen⁴, and TongPing Shen¹

¹ School of Medical Information Technology,
Anhui University of Chinese Medicine, Hefei 230012, China
Fishstonehfu1006@163.com

² Institute of Computer Application in Traditional Chinese Medicine,
Anhui Academy of Chinese Medicine, Hefei 230012, China

³ School of Computer and Information,
Hefei University of Technology, Hefei 230009, China

⁴ The First Affiliated Hospital, Anhui University of Chinese Medicine,
Hefei 230038, China

Abstract. In order to ensure the correctness and reliability of the Internet of Things service system, it is very necessary to fully test before the system is deployed. However, due to the particularity of the Internet of Things environment, conventional simulation and test methods are more costly and have longer cycles than traditional software systems. Therefore, based on the resource-oriented thinking of REST and with the context constraints of Internet of Things services, a formal modeling and verification method of Internet of Things services is proposed. Firstly, the resource of Internet of Things service is formally described from the aspects of resource service port, resource type, resource interface operation method and resource link attribute. Then, combined with the method of CSP (communication sequence process) in process algebra, a resource-oriented Internet of Things service model with the context constraints is constructed. Furthermore, the atomic service and composite services are abstractly modeled and analyzed by taking the Internet of Things application scenario of hospital intelligent clinic as an example. Finally, the model is verified by the model checking tool named PAT from the aspects of security, certainty and accessibility. This method provides a scientific basis and implementation reference for the correctness and reliability test before the deployment of the Internet of Things service system.

Keywords: Resource-oriented · Context constraints · Internet of Things services · Formal modeling · CSP (communication sequence process)

1 Introduction

The Internet of Things is the third information technology revolution after computers and the Internet, and its ultimate value lies in services and their applications. It needs to be application-oriented and provide reliable and efficient services [1, 2]. In the Internet

of Things, the service-oriented approach to information development and integration has been widely accepted and has attracted great attention. The essence of Internet of Things service is the combination of service computing and Internet of Things technology, and its core idea is to uniformly package the capabilities provided by heterogeneous physical devices and then provide services to users [3–5]. By reusing the existing Internet of Things services and constructing an on-demand Internet of Things service system, the disadvantages of high cost caused by redevelopment can be avoided. In order to ensure the correctness and reliability of the Internet of Things service system, it is very necessary to carry out full testing and inspection before the system is deployed, which has become a key problem to be urgently solved in the Internet of Things project.

The methods to verify the system include simulation, software testing and formal methods. Conventional simulation methods sometimes face the problem that they are quite different from actual systems and cannot carry out targeted tests. The traditional testing method cannot completely test the system and the testing cycle and cost will increase dramatically due to the deployment and debugging of actual hardware equipment and networks. Formalization method is a system description and verification method based on mathematical method [6], and it can provide efficient verification methods and steps under the premise of low cost and short cycle for conventional Internet of Things service applications, which provides a better implementation method for pre-deployment verification of Internet of Things service systems.

In the formal research of Internet of Things service system, service modeling is the core content of formal methods. For example, document [7] proposes a WSDL-based Internet of Things service description meta-model based on the traditional Web service description model WSDL by extending the physical objects and service contents of Internet of Things services. The model uses the adjacency matrix method of directed graph to represent the precursors and successors of events, and it can only express the order of services, but not the context constraints of services through the weight of directed graph. In addition, its processing method is single and fixed, which does not meet the intelligence requirements of the Internet of Things. Literature [8–11] takes time automata as modeling tool to model the behavior of Internet of Things services as its interaction with related environmental entities, and introduces environmental entities to depict the attributes and behaviors of various objects in the physical world, emphasizing the description of the behaviors of physical environmental entities, atomic services and composite services and the verification of related attributes. Ge [12] and others model the Internet of Things service and physical environment as probabilistic time automata on the basis of the aforementioned documents, and analyzes and verifies the non-functional constraint attributes such as response speed, reliability and resource consumption of the Internet of Things service. However, the above-mentioned methods only focus on the order of service and do not consider the context constraints when modeling and verifying by timed automata, and the resource-oriented ideas and methods have not yet been embodied. Document [13] constructs the Internet of Things service model based on differential dynamic logic and quantitative differential dynamic logic, and proposes a modeling and verification framework of Internet of Things service based on hybrid system theory. Although the explosion problem of state space is effectively avoided, the application of hybrid system theory to the research of Internet

of Things service is not mature and in-depth enough, and further exploration is needed. Although literature [14] models the Internet of Things service based on the resource-oriented idea, context constraints have not been considered in the modeling process.

From the above, it can be seen that most of the formal modeling of the existing Internet of Things services focus on service content, service functions, dynamic interaction of services, etc. However, the context constraints of services are rarely involved, and it is even less to analyze and verify the modeling of Internet of Things services from the perspective of service resources.

For this reason, this paper proposes a formal modeling method of resources-oriented Internet of Things service based on resource-oriented thinking and considering context constraints for the pre-deployment inspection of Internet of Things service system. Taking the application scenario of the Internet of Things in hospital intelligent clinic as an example, the model is analyzed and its key properties are verified by using the model detection tool PAT, which provides scientific basis and implementation reference for the correctness and reliability inspection of the Internet of Things service system.

The rest of this paper is organized as follows: Sect. 2 discusses the formal description of Internet of Things service resources; Sect. 3 combines context constraints and communication sequence process method in process algebra to build a resource-oriented Internet of Things service model, and takes the application scenario of Internet of Things in hospital intelligent clinic as an example for abstract modeling and analysis. Section 4 analyzes how to verify the above model through the model testing tool PAT. Section 5 summarizes the full text and discusses the next research direction.

2 Formal Description of Internet of Things Service Resources

2.1 Internet of Things Services Based on REST Architecture

At present, there are two styles of Web services, namely, representational state transfer (REST) and Simple Object Access Protocol (SOAP). Because the resource equipment in the Internet of Things service system does not have high storage capacity, computing capacity and communication capacity, traditional SOAP-based Web services are difficult to meet the needs of Internet of Things services, while REST-based Web services are simple in form, lightweight in design, fast in implementation, and more suitable for Internet of Things services.

REST is a distributed system architecture design style [15, 16], whose core idea is the concept of resource orientation. In REST architecture style, everything is regarded as a resource, which can be not only physical objects such as rooms and sensors, but also abstract concepts such as software and network environment. Based on this idea,

all elements in the application scenario of the Internet of Things, such as environmental entities, equipment, perceived data, services, state information, management information, etc., can be abstracted as resources. REST's resources are addressable and are uniquely identified by using the Uniform Resource Identifier (URI) through the operation method defined by the HTTP protocol. The above ideas provide a new idea for the formal description of resources in the Internet of Things service system.

2.2 Construction and Implementation of Internet of Things Service Resource Description Model

REST has the characteristics of addressability, unified interface, connectivity and statelessness. According to the user needs in the Internet of Things service, the following key issues need to be solved when describing its resources: (1) Determination of the resource identifier of the Internet of Things service; (2) Determination of the unified interface and operation method of Internet of Things service resources; (3) Definition of the expression format of Internet of Things service resource, so as to form links with each other through resource expression; (4) Efficient management of the service resource states of Internet of Things to achieve stateless resource-oriented architecture.

From the above questions, it can be seen that the description of the resource identifier is very important to describe the service resources of the Internet of Things. The following first gives a description of the resource identifier of the Internet of Things service, which is represented by a seven-tuple as follows:

Definition 1: Uniform Resource Identifier

$$URI = (RIP, RType, RID, RName, RPro, RAct, RPara)$$

RIP indicates the root directory, that is, the service port address; *RType* is the type of resources, such as article resources, computing resources, management resources and communication resources, etc., where the article resources refer to the functional units required by the capabilities directly related to articles provided by the Internet of Things, and communication resources refer to the communication functional units for network data transmission in the Internet of Things; *RID* is the resource identification number; *RName* is the name of the resource; *RPro* represents resource-related attributes; *RAct* indicates the resource operation method; *Rpara* represents the parameters to be called during the operation. *RAct* and *RPara* can be set according to specific conditions, for example:

$$Http : // \dots / \{ Communicationresources, Sensors \} / \{ HeartRateSensor.Id \} / \{ HeartRateSensor / \{ PatientId, BedNumber \} / \{ RAct.Id \} / \{ RPara \}$$

Http://... is the port address of the resource service; $\{Communication\ resources, Sensors\}$ indicates that the resource type is a communication resource, specifically a sensor class in the communication resource; *HeartRateSensor.Id* is the resource identification number; *HeartRateSensor* is the name of the resource, that is the heart rate sensor; $\{PatientId, BedNumber\}$ is the attribute of the resource, namely the patient Id number and its bed number of the heart rate sensor installed; $\{RAct.Id\}$ indicates the resource operation method; $\{RPara\}$ represents the parameters to be called during the operation.

Next, based on the idea of resource-oriented architecture, a formal description model of Internet of Things service resources is given as follows:

Definition 2: Internet of Things service resources are formally described as a four-tuple

$$RS = (URI, Method, Link, MediaType)$$

URI represents the uniform resource identifier of the Internet of Things, and its related description is specifically shown in Definition 1.

Method indicates the interface operation method of the resource and the relevant information exists in HTTP methods. The basic operation interface methods of HTTP include reading resources GET, updating resources PUT, adding resources POST and deleting resources DELETE. In order to meet the complex operation requirements of users, the method of operation interface can be expanded according to user requirements.

Link represents the link attribute of a resource, by which resources can be connected to each other.

MediaType indicates the media type of the resource. The transmission format of data in the transmission process under the media type is defined, such as text, binary stream, XML, JSON, etc.

Next, the concrete implementation of the formal description model of Internet of Things service resources is illustrated by taking the application scenario of Internet of Things in hospital intelligent wards as an example. In the intelligent ward service, the heartbeat data of critically ill inpatients are collected in real time by wearing a heart rate sensor. When the heartbeat data is not within the normal threshold range, a real-time alarm will be given, and the medical staff on duty will quickly check and take decisive measures. In order to realize the above functions, first of all, all sensor lists must be searched. Secondly, heart rate information of critically ill patients is obtained by searching heart rate sensors. Finally, whether the heart rate information is within the normal threshold range is judged, and if not, an alarm is sent out in real time. The specific process is shown in Table 1.

Table 1. Formal description instance data of Internet of Things service resources

Resource	URI	Method	MediaType	Description
Resource 1	<i>Http : //.../{Communicationresources, Sensors}</i>	GET	XML/JSON	To get all sensors
Resource 2	<i>Http : //.../{Communicationresources, Sensors}/ {HeartRateSensor.Id}/HeartRateSensor/ {PatientId, BedNumber}</i>	GET	XML/JSON	To obtain the resource information of the heart rate sensor, namely the heart rate information of the patient
Resource 3	<i>Http : //.../{Communicationresources, Sensors}/ {HeartRateSensor.Id}/HeartRateSensor/ {PatientId, BedNumber}/{RAct}/{RPara}</i>	GET	XML/JSON	To monitor the patient's heart rate and automatically trigger to change the working state of the alarm
Resource 4	<i>Http : //.../{Managementresources, Alarms}/ {Alarm.Id}/Alarm/{Alarm.RPro}/{RAct.Id}/ {On, Off}</i>	PUT	XML/JSON	To change the status information of the alarm

3 Resource-Oriented Internet of Things Service Modeling with Context Constraints

3.1 Construction of Resource-Oriented Internet of Things Service Model with Context Constraints

Based on the formal description of the Internet of Things service resources mentioned above, a resource-oriented Internet of Things service model with context constraints is constructed based on the resource-oriented idea and considering context constraints. The model is as follows:

Definition 3: The Internet of Things service is modeled as

$$S = (URI, SN, SR, CSP, OP, CC)$$

URI represents the unique identification and address of the resource-oriented service, as shown in Definition 1.

SN indicates the name of the resource-oriented service, which corresponds *URI* one to one;

SR represents a collection of resources that make up a service, including atomic services and composite services;

CSP represents the Communication Sequential Processes (CSP) [17, 18] method in process algebra, which is used to describe the dynamic behavior of Internet of Things services. CSP is a typical process algebra method to describe the specification and design of distributed concurrent software systems. As the Internet of Things service system is a distributed concurrent system, CSP method is adopted to describe and analyze the dynamic behavior of REST-based Internet of Things services.

OP represents the set of operations for resource-oriented services, as shown in Definition 2, respectively referring to the HTTP basic operation methods GET, PUT, DELETE, POST;

CC represents context constraints for resource-oriented services. It can be divided into subjective constraints and objective constraints. For example, for the hospital diagnosis and treatment service, the subjective constraint condition is the patient's needs. For example, the closer the patient wants to see a doctor to his home, the better; the shorter the waiting time, the better; the higher the credibility of the doctor, the better; and the cheaper the medical expenses, the better. Objective constraints are diagnosis and treatment rules, including the objective requirements for the time and place of diagnosis and treatment, as well as related matters needing attention, such as liver function blood test requires fasting blood in the morning, and female gynecologic B-ultrasonography requires bladder filling.

Internet of Things services include atomic services and composite services. Atomic services refer to services that are indivisible and cannot be decomposed into finer-grained services during execution. The composite service refers to a new and more complex Internet of Things service which is formed by aggregating multiple atomic services according to specific business processes in order to meet different application requirements of users. According to the modeling method of Internet of Things service given in Definition 3, the modeling method of resource-oriented Internet of Things atomic service and composite service with context constraints is further refined below.

Definition 4: Internet of Things atomic service can be modeled as $AS = (URI, SN, SR, CSP, OP, CC)$, where *URI*, *SN* and *OP* are not empty. *SR* represents a collection of resources that make up the atomic service; *CSP* is not empty, indicating that the dynamic behavior of atomic services to the Internet of Things is represented by *CSP* methods; *CC* indicates the context constraints of the atomic service.

For example, take the atomic service of mobile ward rounds of resident doctors in a smart hospital environment as an example, the constraint condition of the atomic service is that the ward round doctors must complete the routine ward rounds (objective constraint condition) for the patients in charge at the surgical hospital building between 7: 30 and 9: 00 every morning, and the expected waiting time of the patients cannot exceed 10 min (subjective constraint condition). Then the constraint condition is formally expressed as follows:

$$\begin{aligned} & \textit{Time between 7 : 30 and 9 : 00} \cap \textit{Location} = \textit{urgical hospital building} \\ & \cap \textit{Patient.Waitingtime} \leq 10 \textit{ min} \end{aligned}$$

Definition 5: The Internet of Things composite service can be modeled as $CS = (URI, SN, SR, CSP, OP, CC)$. URI , SN and OP are not empty, which are the addresses, names and related operation sets of the combined new service respectively. SR represents a resource set of composite services formed by the combination of atomic services; CSP is not empty, which means that the dynamic behavior of composite services in the Internet of Things service is modeled according to the composite operation of processes; CC indicates the context constraints of the composite service, including not only the constraints of the atomic services that make up the service, but also the constraints between the atomic services during the composition of the service.

From the above analysis, it can be seen that when modeling the Internet of Things service, the CSP method is the most critical to describe the dynamic behavior of the Internet of Things. Next, with a specific scenario example, the modeling of resources-oriented Internet of Things services will be described in detail.

3.2 Application Example of Resource-Oriented Internet of Things Service Modeling

Intelligent diagnosis and treatment service is the core service content of hospital Internet of Things, of which the Internet of Things application system in intelligent clinic is the most direct application of Internet of Things system in hospital outpatient service. It is assumed that the intelligent clinic of the hospital is equipped with air conditioner, fluorescent lamp, access control system, film viewing light box for observing X-ray films, CT films, magnetic resonance films and other films, as well as curtain and other equipment to protect the privacy of patients when they need to undergo in-depth examination. The specific description of its application scenario is as follows:

- Air conditioner: when the room temperature is lower than 20°C, the air conditioner automatically turns on the heating mode to raise the room temperature to 22°C; When the room temperature is higher than 28°C, the air conditioner automatically turns on the cooling mode to reduce the room temperature to 22°C; When the room temperature is between 20°C and 28°C, the air conditioner stops working.
- Fluorescent lamp: when the indoor light does not reach the preset brightness standard, the system will automatically turn on the fluorescent lamp.
- Film viewing light box: when x-ray films, CT films, magnetic resonance films and other films are pasted on the light box, the light box will automatically open and light up. On the contrary, when the above film is removed from the light box, the light box is automatically closed and the light box is extinguished.
- Curtain: The examination area is set in the examination room, separated from the examination room by curtain, with beds and stools, suitable for examination of private parts. When the patient enters this area and needs to be examined, the curtain automatically descends to play the role of shielding. When the patient leaves this area and the examination is finished, the curtain will automatically rise.
- Access control system: Call sign system sorts call signs according to registration order and check-in order, and patients visit doctor in sequence according to call sign prompts. The patient enters the clinic by brushing the RFID card, and the entrance guard service carries out perception control on the door according to the card. When

it is detected that the swiped card number is consistent with the current call sign of the system, the door opens automatically; Otherwise, you will be prompted “Please wait patiently before you go to see a doctor”. If no one swipes the card within 1 min, the system will directly enter the call of the next serial number.

Next, taking the application scenario of Internet of Things in hospital intelligent clinic as an example, the atomic service and composite service are modeled respectively, and how to use CSP method to describe and analyze its dynamic behavior is emphatically discussed.

- (1) **Atomic Services.** Monitoring the temperature in the clinic is an atomic service. If it is not within the set range, the system will automatically turn on the air conditioner, which can be modeled as $(URI, TempMonitor, SR, CSP, OP, CC)$. URI is the unique identification of room temperature monitoring service; $TempMonitor$ is the name of service for room temperature monitoring; SR is a collection of resources serving the atom, etc.; OP includes acquiring information of a room temperature sensor, monitoring room temperature information to trigger an air conditioner, changing the working state of the air conditioner and other related operations; CC is the constraints serving the atom; CSP is used to describe the dynamic behavior of room temperature monitoring, which can be expressed as:

$$\begin{aligned}
 & RoomTempMonitor() = \\
 & [RoomTemp < 20] TurnOnAirconditioner\{AirconditionerSwitch = 1; Mode = heat;\} \\
 & \quad \rightarrow ControlRoom(RoomTemp = 22;) \rightarrow RoomTempMonitor() \\
 & [] [RoomTemp > 28] TurnOnAirconditioner\{AirconditionerSwitch = 1; Mode = cool;\} \\
 & \quad \rightarrow ControlRoom(RoomTemp = 22;) \rightarrow RoomTempMonitor() \\
 & [] [RoomTemp \geq 20 \& \& BodyTemp \leq 28] TurnOffAirconditioner\{AirconditionerSwitch = 0;\} \\
 & \quad \rightarrow Skip()
 \end{aligned}$$

The brightness monitoring service in the clinic is also an atomic service. When the indoor light does not reach the set brightness standard, the system will automatically turn on the fluorescent lamp. It can be modeled as $(URI, RoomLightMonitor, SR, CSP, OP, CC)$, in which CSP is used to describe the dynamic behavior of indoor brightness monitoring, which can be expressed as:

$$\begin{aligned}
 & RoomLightMonitor() = \\
 & [RoomLight < 60] TurnOnChandelier\{ChandelierSwitch = 1;\} \rightarrow RoomLightMonitor() \\
 & [] [RoomLight \geq 100] TurnOffChandelier\{ChandelierSwitch = 0;\} \rightarrow RoomLightMonitor()
 \end{aligned}$$

Monitoring the patient’s position in the clinic is also an atomic service. If the patient is detected to enter the examination area, the curtain will automatically descend, effectively protecting the patient’s privacy and facilitating the doctor’s diagnosis. On the other hand, when it is detected that the patient leaves the examination area, the curtain will automatically rise. It can be modeled as $(URI, PatientLocMonitor, SR, CSP, OP, CC)$, in which CSP is used to describe the dynamic behavior of monitoring the patient’s position in the clinic, which can be expressed as:

$$\begin{aligned}
 & \text{PatientLocMonitor}() = \\
 & \quad [PatientLoc \in R] \text{DescendCurtain}\{CurtainSwitch = 1; Mode = down;\} \\
 \rightarrow & \text{ControlCurtain}\{CurtainLoc = bottom; CurtainSwitch = 0;\} \rightarrow \text{PatientLocMonitor}() \\
 & \quad [PatientLoc \notin R] \text{RiseCurtain}\{CurtainSwitch = 1; Mode = up;\} \\
 \rightarrow & \text{ControlCurtain}\{CurtainLoc = top; CurtainSwitch = 0;\} \rightarrow \text{PatientLocMonitor}()
 \end{aligned}$$

Gesture monitoring of doctors in the clinic is also an atomic service. If it is detected that the doctor's gesture is to approach the film viewing light box, the light box will be automatically turned on to facilitate the doctor to view the film, otherwise, it will be turned off. It can be modeled as $(URI, \text{GestureMonitor}, SR, CSP, OP, CC)$, in which CSP is used to describe the dynamic behavior of doctor gesture monitoring in the clinic, which can be expressed as:

$$\begin{aligned}
 & \text{DoctorGesMonitor}() = \\
 & \quad [DoctorGes = near] \text{TurnOnLamp}\{LampSwitch = 1;\} \rightarrow \text{DoctorGesMonitor}() \\
 [] & [DoctorGes = leave] \text{TurnOffLamp}\{LampSwitch = 0;\} \rightarrow \text{DoctorGesMonitor}()
 \end{aligned}$$

Hospital entrance guard service is also atomic service. When the system call sign is used, it will automatically detect whether the card number of the RFID card swiped by the patient is consistent with the current call sign. If so, the clinic door will automatically open, otherwise, it will prompt "It is not your turn to see a doctor, please wait patiently". If no one swipes the card within 1 min, the call will go directly to the next medical serial number. When the system does not have a call sign, if a patient swipes his card to enter the clinic at this time, he will be directly prompted "There are still patients visiting, please be patient". The atomic service can be modeled as $(URI, \text{CardMonitor}, SR, CSP, OP, CC)$, in which CSP is used to describe the dynamic behavior of the clinic entrance guard service, which can be expressed as:

$$\begin{aligned}
 & \text{CardMonitor}() = \\
 & \text{if } Call(\text{VisitSeriNum}) \\
 & \quad \text{if } (\text{waittime} < 60\text{s}) \\
 & \quad \quad \{ [CardId = \text{VisitSeriNum.PatientId}] \text{OpenDoor}\{DoorSwitch = 1;\} \\
 & \quad \quad \rightarrow \text{CardMonitor}(); \\
 & \quad \quad [] [CardId \neq \text{VisitSeriNum.PatientId}] \\
 & \quad \quad \quad \{ \text{CloseDoor}\{DoorSwitch = 0;\} \\
 & \quad \quad \quad \text{alert}(\text{"It is not your turn to see a doctor, please wait patiently"}) \} \\
 & \quad \quad \rightarrow \text{CardMonitor}(); \\
 & \quad \text{else } \{ \text{VisitSeriNum} ++; \text{CardMonitor}(); \} \\
 & \text{else } \text{alert}(\text{"There are still patients visiting, please be patient"}) \\
 & \quad \rightarrow \text{CardMonitor}();
 \end{aligned}$$

- (2) **Composite services.** For the Internet of Things application scenario of hospital intelligent clinic, clinic monitoring and control is a composite service, which can be modeled as $(URI, CompositeService, SR, CSP, OP, CC)$. URI is the unique identification of the clinic monitoring and control service; $CompositeService$ is the name of the monitoring and control service for the clinic; SR is all resource sets of the composite service, OP comprises acquiring information of various sensors (such as temperature sensors, brightness sensors, infrared sensors and so on), monitoring information to trigger relevant equipment, changing various equipment states and other relevant operations; CC is the constraints serving of the composite service; CSP is used to describe the dynamic behavior of each service in the clinic monitoring control, which can be expressed as:

```

CompositeService() = if(time > 10) {RoomMonitor()} else{StopMonitor()};
RoomMonitor() = {RoomTempMonitor(); RoomLightMonitor(); PatientLocMonitor();
                 DoctorGesMonitor(); CardMonitor(); TimeSet();}
TimeSet() = timeset{time = 0;} → CompositeService();
StopMonitor() = change{time ++; CurtainSwitch = 0; CurtainLoc = top;
                    LampSwitch = 0; DoorSwitch = 0;}
                → CompositeService();

```

4 Verification of Internet of Things Service Based on PAT

PAT Model Detector [19] is a tool for modeling, reasoning and verifying concurrent real-time systems, and next PAT is used as a tool for verifying the timeliness correctness of Internet of Things services. In PAT, linear temporal logic LTL (LTL) [20] is used to verify relevant attributes.

The verification of Internet of Things service mainly verifies the five properties of Internet of Things service, such as security, non-divergence, certainty, accessibility and activity. The specific explanation is as follows:

- **Security:** that is, verifying that the service can be in a running state all the time under abnormal shutdown conditions, and unexpected events will never occur. Deadlock-free service is a typical security.
- **No divergence:** that is, verifying that the service does not contain useful services.
- **Certainty:** that is, verifying that the transition of any state in the service will not result in two different states.
- **Accessibility:** that is, verifying that the final desired target state of the service can be achieved. For example, in the room temperature monitoring service of the clinic, it is hoped that the room temperature will be maintained at a certain set value. When the room temperature is higher than 28°, the air conditioner can be started for cooling, and when the room temperature is lower than 20°, the air conditioner can be started for heating.

- **Activity:** that is, verifying the information collected by the sensor can trigger the corresponding operation, and all the desired events can eventually occur. For example, when it is detected that the patient is located in the examination area of the clinic, the curtain descends to facilitate examination.

The verification of the Internet of Things service includes the verification of its atomic services and composite services. Next, PAT tool is used to verify the modeling example of the Internet of Things application scenario of the 3.2 hospital intelligent clinic.

(1) Atomic Service Verification

Take the monitoring service for the patient's location in the clinic *PatientLocMonitor* as an example.

- **Security (mainly verifying deadlock-free)**

#assert PatientLocMonitor() deadlockfree;

- **No divergence**

#assert PatientLocMonitor() divergencefree;

- **Certainty**

#assert PatientLocMonitor() deterministic;

- **Accessibility**

Verify that the curtain in the service are operational. Represented by CSP# assertion as follows:

*#define goal10(CurtainSwitch == 1);
#assert PatientLocMonitor() reaches goal10;
#assert PatientLocMonitor() | = <> goal10;*

- **Activity**

Verify that when the patient is monitored to be in the examination area of the clinic, the curtain will automatically descend, effectively protecting the patient's privacy and facilitating the doctor's diagnosis. Represented by CSP# assertion as:

*#define PatientLoc(PatientLoc ∈ R);
#assert PatientLocMonitor() | = [] Curtain → <> DecscendCurtain;*

Verify that when the patient is not in the examination area, the curtain will automatically rise. Represented by CSP# assertion as:

```
#define PatientLoc(PatientLoc  $\notin$  R);
#assert PatientLocMonitor() | = [] Curtain  $\rightarrow$   $\langle$  RiseCurtain;
```

Similarly, through PAT platform to automatically verify the models of each atomic service, it can be concluded that all atomic service models in the application scenario of the Internet of Things in the hospital intelligent clinic have the above properties.

(2) Composite Service Verification

- **Security (deadlock-free)**

```
#assert CompositeService() deadlockfree;
```

- **No divergence**

```
#assert CompositeService() divergencefree;
```

- **Certainty**

```
#assert CompositeService() deterministic;
```

- **Accessibility**

Verify that the temperature of the clinic in the service can reach the expected state value and the fluorescent lamp, curtain, viewing light box and entrance guard system can reach the running state. Represented by CSP# assertion as follows:

```
#definegoal6 ((RoomTemp  $\geq$  0 && RoomTemp  $\leq$  28)
&& ChandelierSwitch = 1 && CurtainSwitch = 1
&& LampSwitch = 1 && DoorSwitch = 1)
#assert CompositeService() reaches goal6;
#assert CompositeService() | = []  $\langle$  goal6;
```

- **Activity**

In the composite service, it is verified that when the room temperature is lower than 20°C, the air conditioner will eventually be turned on for heating; When the brightness of the light in the clinic is less than 60, the fluorescent lamp is automatically turned on; When the patient is monitored to be in the examination area of the clinic, the curtain automatically descends; When the doctor's gesture is detected to be close to the film viewing lamp box, the film viewing lamp box is automatically opened; When it is detected that the card number of the RFID card swiped by the patient visiting to the doctor is consistent with the current call sign, the clinic door is automatically opened. Represented by CSP# assertion as follows:

$$\begin{aligned}
\#assert CompositeService() | &= [] RoomTemp \rightarrow \langle \rangle TurnOnAirconditioner \\
\#assert CompositeService() | &= [] RoomLight \rightarrow \langle \rangle TurnOnChandelier \\
\#assert CompositeService() | &= [] PatientLoc \rightarrow \langle \rangle DescendCurtain \\
\#assert CompositeService() | &= [] DoctorGes \rightarrow \langle \rangle TurnOnLamp \\
\#assert CompositeService() | &= [] CardId \rightarrow \langle \rangle OpenDoor
\end{aligned}$$

In the same way, PAT platform is used to verify the satisfiability of the related properties in each atomic service and composite service mentioned above. The results show that other properties are also satisfied.

5 Conclusion

With the continuous development and wide application of Internet of Things technology, the correctness and security problems of Internet of Things service system are increasingly prominent. Formal analysis and verification are the key issues that need to be solved urgently in Internet of Things engineering. Based on REST's resource-oriented idea and the context constraints of Internet of Things services, this paper proposes a formal modeling method of resource-oriented Internet of Things services with context constraints. Firstly, the service resources of the Internet of Things are formally described from the aspects of resource service ports, resource types, resource interface operation methods, resource link attributes, etc. Then, the resource-oriented service model of the Internet of Things with context constraints is constructed by the communication sequence process CSP method in process algebra. Furthermore, the atomic service and composite service are abstractly modeled and analyzed respectively by taking the application scenario of the Internet of Things in the intelligent clinic of the hospital as an example. Finally, the model testing tool named PAT is used to verify the above example models from five aspects: deadlock-free, divergence-free, certainty, accessibility and activity, which provides effective support for the correctness and reliability testing of the Internet of Things service system before deployment.

However, when modeling the Internet of Things service system abstractly, this paper studies the simplest mode of service combination of the Internet of Things—sequential combination mode. The next step is to study other combination modes of services corresponding to actual scenes, such as parallel combination, mixed combination, etc. For example, when taking the model as an example, the application scenario of the Internet of Things in the intelligent clinic with relatively simple functions in the smart hospital is selected and the service combination mode of the scenario is sequential combination. In fact, the smart hospital also has more complex intelligent ward scenarios (including mobile ward round service and mobile nursing service) and intelligent diagnosis guidance scenarios (real-time suggestions for diagnosis and treatment process according to the number of people in each link), etc., which require a variety of service combination modes. The next step is to describe all the Internet of Things application scenarios of the smart hospital through this model to provide

effective support for the specific deployment and full implementation of the smart hospital.

In addition, context constraints are considered in the abstract modeling of the Internet of Things service system in this paper, and the static combination of Internet of Things services is studied, but the dynamic combination of atomic services into services satisfying the constraints according to the context constraints of services has not been involved. In connection with practical application scenarios, such as intelligent guidance services in smart hospitals, how to provide recommendations of diagnosis and treatment processes and service schemes according to the actual needs of users is the next direction to be paid attention to.

Acknowledgments. This study was financially supported by the Natural Science Foundation of China (Grant No. 61701005), the Key Project of Outstanding Young Talents Support Program of Anhui Higher Education Institutions (Grant No. gxyqZD2016128), the Key Project of Natural Science Research in Anhui Higher Education Institutions (Grant No. KJ2015A054, No. KJ2019A0437), the Key Project of Humanities and Social Sciences Research in Anhui Higher Education Institutions (Grant No. SK2019A0242, No. SK2018A0216), the Domestic Visiting Research Project of Excellent Young Backbone Talents from Anhui Higher Education Institutions (Grant No. gxgnfx2019009), the Quality Project Foundation of Anhui Province (Grant No. 2017-mooc220, No. 2018zhkt079, No. 2015sxxz011, No. 2012sjjd025), the Teaching Research Key Project of Anhui University of Chinese Medicine (Grant No. 2017xjjy_zd011), the School-based Online Course Construction Project of Anhui University of Chinese Medicine (Grant No. 2017XBWL06), the Pilot Project of Ideological and Political Education Reform of Anhui University of Chinese Medicine in 2019 (Course Name: Software Engineering), the Natural Science Research Foundation of Anhui University of Chinese Medicine (Grant No. 2019zrzd11, No. 2018zryb06), the National Innovation and Entrepreneurship Training Program for College Student (Grant No. 201810369021, No. 201810369022, No. 201610369044, No. 201710369052).

References

1. Zhao, C., Fanping, Z., Guozhu, C., et al.: Overview of Internet of Things security assessment technology. *J. Inf. Secur.* **4**(3), 1–16 (2019)
2. Qibo, S., Jie, L., Shan, L., et al.: Internet of Things: a review of concepts, architecture and key technologies. *J. Beijing Univ. Posts Telecommun.* **33**(3), 1–9 (2010)
3. Li, Ma.: Formal Modeling and Verification of Resource-Oriented IoT Systems. Taiyuan University of Technology, Taiyuan (2018)
4. Thoma, M., Meyers, S., Sperner, K., et al.: On IOT-services: survey, classification and enterprise integration. In: IEEE International Conference on Green Computing and Communications (GreenCom), pp. 257–260. IEEE, Besancon (2012)
5. Haiming, C., Li, C.: Service-oriented IoT software architecture design and model detection. *Chin. J. Comput.* **39**(5), 853–871 (2016)
6. Ji, W., Najjun, Z., Xinyu, F., et al.: Overview of formal methods. *J. Softw.* **30**(1), 33–61 (2019)
7. Yu, L., Lu, Y., Zhu, X.-J., et al.: A web services description language-based description model of Internet of Things services. *Sens. Lett.* **12**(2), 448–455 (2014)
8. Lixing, L., Zhi, J., Ge, L.: Modeling and verification of Internet of Things services based on time automata. *Chin. J. Comput.* **34**(8), 1365–1377 (2011)

9. Lixing, L.: Description and Performance Analysis of Internet of Things Services based on Environmental Modeling. University of Chinese Academy of Sciences, Beijing (2013)
10. Guoqing, W., Lei, Z., Ruimin, W., et al.: Modeling and verification of IoT gateway security system based on time automata. *J. Commun.* **39**(3), 63–75 (2018)
11. Xuefeng, D., Ruizhi, S., Juan, N., et al.: Modeling of greenhouse environment monitoring IoT system based on time automata. *J. Agric. Mach.* **47**(7), 301–308 (2017)
12. Ge, L., Qiang, W., Lixing, L., et al.: Modeling of Internet of Things services: a method based on environmental modeling. *Sci. China Inf. Sci.* **43**(10), 1198–1218 (2013)
13. Lin, Y., Tang, P., Lipeng, G., et al.: Modeling and verification of Internet of Things services based on hybrid system. *Small Micro Comput. Syst.* **34**(12), 2663–2668 (2013)
14. Li, Ma., Weikang, L., Chen, L., et al.: Formal modeling and verification of resource-oriented IoT systems. *Small Micro Comput. Syst.* **39**(1), 140–145 (2018)
15. Han, L.: Combat of Java RESTful Web Service. Mechanical Industry Press, Beijing (2014)
16. Fielding, R.T.: Architectural Styles and the Design of Network-Based Software Architecture. University of California, Irvine (2000)
17. Hoare, C.A.R., Chaochen, Z.: Communication Sequence Process. Peking University Press, Beijing (2011)
18. Lingzhong, Z., Zhongyi, Z., Junyan, Q., et al.: Detection of CSP model based on key trace and ASP. *J. Softw.* **26**(10), 2521–2544 (2015)
19. Junwei, Ma.: Formal Analysis and Verification of Smart Home Platform Based on PAT Tool. Taiyuan University of Technology, Taiyuan (2016)
20. Ming, D., Shuling, Z., Chen, Z.: Formal design and verification of business process. *J. Beijing Inst. Technol.* **36**(11), 1147–1153 (2016)



Sc-Ge: Multi-Factor Personalized Point-of-Interest Recommendation Model

Wen Hu^(✉) and Yuhai Jing

School of Computer and Information Engineering,
Harbin University of Commerce, Harbin 150028, Heilongjiang, China
huw@hrbcu.edu.cn

Abstract. For most current POI (point-of-interest) recommendation algorithms, only the common visited POIs among users are used to calculate the similarity among users. Due to the high sparsity of the data, the recommendation result of POI is inaccurate. Aiming at this problem this paper proposes a method to determine the similarity among users by combing the similarity that using Cosine similarity with the similarity among users by Jensen-Shannon divergence (JS divergence) after mining the user interest distribution with the Latent Dirichlet Allocation (LDA). At the same time combining POI's commentary text information, rating information, geographical location information and friend relationship information in social networks, a multi-Factor personalized POI recommendation model Sc-Ge is proposed to improve the precision and recall rate of POI recommendation. Experiments are carried out on the comment dataset Yelp, and it is concluded that this model is better than other mainstream POI recommendation algorithms.

Keywords: Point-of-interest · Latent Dirichlet Allocation · Yelp · Jensen-Shannon divergence · Cosine similarity

1 Introduction

Due to the emergence of Web 2.0 technology, the Internet has completed the transformation from passive user reception of information to active creation of information quality. With the rapid spread of the Internet, more and more users actively exchange and share information with other users through the Internet. The explosive growth of this information has declared that people are in an era of “information overload” [1] that cannot effectively screen out the information they need from the vast ocean of information. How to help users efficiently filter out the POI that they may like from countless POIs is also an urgent problem in the background of this era.

Today, most of the mainstream POI recommendation algorithms are based on POI explicit feedback data (such as POI's ratings, likes or dislikes) and contextually implicit feedback information (such as comments, comments, time, etc.) to explore POIs which mach user preferences, so that the data sparseness problem of the users-POIs sign-in matrix and the cold-start problem of recommendation are alleviated to different degrees. The variant collaborative filtering (CF) [2] algorithm is more common in which other information sources are combined to improve the precision of similarity

calculation. Huang et al. [3] used the social, sequential, temporal and spatial modes to characterize the user's registration behavior, and integrated the heterogeneous stream data in the Cyber-Physical Systems (CPS) system into the multi-mode Bayesian embedding model to jointly recommend for user decision-making. Dai et al. [4] combined the four factors of geographic location information, personal hobbies, social relations and time period, and proposed the PRAFF heuristic recommendation algorithm to improve the recommendation performance. Ye et al. [5] proposed a hybrid CF (collaborative filtering) algorithm which combined User-based CF (based on user collaborative filtering) algorithm, collaborative filtering based on friend relationship, and recommended method for applying geographic location information based on personal preference, friend relationship and POI distance factors, so that the POI recommendation precision is improved.

In general, the above POI recommendation algorithm has achieved certain results in data sparseness mitigation, which further improves the recommendation quality, but also leaves some shortcomings:

- (1) Only the common scoring POIs checked by the user are used in calculating the POIs or the users similarity, but since the user-POI check-in matrix is highly sparse, the recommendation result is inaccurate;
- (2) The training model takes a long time, and the model calculation cost is large.

In order to effectively solve the problems in the above recommendations and the imperfections included in the research, this paper combines POI's comments, ratings, geographic location and friend relationships in social networks to design a personalized POI recommendation model Sc-Ge. In summary, the contribution of this article to the recommendation of POI is as follows:

- (1) This paper combines the multi-heterogeneous information such as social service information, comment text information and geographical location information, and forms two major influencing factors of society and geography, so that the recommendation system has good robustness and has a good effect in dealing with the cold start problem;
- (2) Reduce the amount of calculation, make the program less expensive when running, and improve efficiency;
- (3) The recommendation experiments on the real (Location-Based Social Networks, LBSN) dataset show that the precision and recall are improved compared with other mainstream POI recommendation algorithms.

2 Related Work

2.1 Social Factor Modeling Based on LBSN Friends Relationship

In daily life, social members (ie, friend relationships) that are grouped into groups often have strong similarities in certain aspects, such as interests, language, lifestyle, values, and so on. According to research findings [6], in a person's social circle, friends share their position more often than non-friends. In a location-based social network, friend

relationships play a role in calculating similarity between users than non-friend relationships. The greater role, which just proves that the above daily life phenomenon is reasonable.

Therefore, when the user-based collaborative filtering algorithm is used to calculate the probability of the target user accessing a certain POI and the similarity between the users is calculated, only the friend relationship is considered, the calculation overhead is reduced, and the efficiency is improved. The process is as follows:

Definition 1: Assuming that all users collection is U , the total number of friend users in the total user is $U_f \in U$, and U_f is much smaller in number than U . The total set of POIs is P , and the users-POIs visit scoring comment matrix is V , and the size of V is greatly reduced when U_f is used instead of U to calculate the similarity between users. Given that the target user is $A_u \in U$, and the POI that has not been visited in the friend collection is P_m , the social factor visit probability that the target user A_u may visit the POI P_m in the future is $\delta(A_u, P_m)$. The calculation formula is as follows:

$$\delta(A_u, P_m) = \frac{1}{R_{\max}} \left(\frac{\sum_{A_v \in U_f(A_u, K)} sml(A_u, A_v) R_{A_v, P_m}}{\sum_{A_v \in U_f(A_u, K)} |sml(A_u, A_v)|} \right) \tag{1}$$

Where R_{A_v, P_m} is the score of the user A_v at the POI P_m , $U_f \in (A_u, K)$ is the set of K friends most similar to the user A_u , and R_{\max} is the maximum score item, which is the normalized processing item. In this paper, $sml(A_u, A_v)$ is defined as the social factor similarity between any two users. It is the core element to obtain the probability of social visit. It is obtained through the following two steps in the experiment:

2.1.1 Definition and Calculation of Interest Similarity Among Users

In real life, friends and friends are more likely to watch movies, fitness, meals, etc., a series of behaviors involving visit to POIs in LBSN [7], because they are more likely to have a common interest, here we have the following definition:

Definition 2: Assume that $P_{list}(A_u)$ represents a collection of POIs that user A_u has visited, and $P_{list}(A_v)$ represents a collection of POIs that user A_v has visited. We define $sml_i(A_u, A_v)$ as the similarity of interest between users. In the course of the experiment, cosine similarity is mainly used to calculate the similarity of interest. According to formula (2), the interest similarity between any two users is:

$$sml_i(A_u, A_v) = \frac{|P_{list}(A_u) \cap P_{list}(A_v)|}{\sqrt{|P_{list}(A_u)| |P_{list}(A_v)|}} \tag{2}$$

2.1.2 Definition and Calculation of Users’ Sentiment Orientation Similarity

In order to further improve the similarity between users and make the POI recommendation more accurate, in the process of obtaining the target user social factor access probability, this paper obtains the similarity of emotional sentiment among users based

on the calculation of the similarity of interest between users. Finally, the two are linearly combined to obtain social factor similarity.

Definition 3: In this paper, $sml_e(A_u, A_v)$ is defined as the similarity of emotional sentiment between users and added to the calculation of the similarity among users. The process of calculating the similarity of sentiment between users is as follows:

- (1) Through the three-layer Bayesian model LDA, through the unsupervised learning process in machine learning, the probability distribution of each user's sentiment tendency is explored. The method steps are as follows: Since the short commentary in the comment text information left by the user on the POI in the LBSN accounts for a large proportion, the text that can express the user's emotion is sparse, which is not conducive to training LDA, therefore, this paper extracts the comment information of any user who has visited all the POIs as a small document d . Each document consists of several words. In this paper, d is defined as a sentiment orientation document, and all users' emotional tendency documents are collected in the data set. d gather together to form a large emotional tendency document for mining the user's emotional tendencies. The obtained large sentiment orientation document is input into the LDA model, and the document-word distribution is mapped to the document-topic distribution and the topic-word distribution by the process of maximum likelihood estimation and Gibbs sampling to make the topic distribution convergence. Assuming that the number of topics entered during the LDA process is T_{num} (ie, the document-theme's matrix dimension is N), then

$$\vec{\phi}_{tw} = \frac{n_t^{(w)} + \beta}{\sum_{l=1}^L n_t^{(w)} + L\beta} \quad (3)$$

$$\vec{\theta}_{dt} = \frac{n_d^{(t)} + \alpha}{\sum_{t=1}^N n_d^{(t)} + N\alpha} \quad (4)$$

Where $n_t^{(w)}$ is the number of w for the topic t , $n_d^{(t)}$ is the number of topics t for the document d , V and N are the number of the vocabulary and the number of topics, and α and β are hyperparameters, respectively representing the document-topic distribution density and topic-word distribution density. Because each topic represents the characteristics of a POI, but also represents a person's emotional preference. Thus, the probability distribution of the emotional tendency between users is defined as $\vec{\theta}_{dt}$, and the specific realization form of the result is as follows:

$$P(A_u) : [x_1, x_2, x_3, x_4, x_5]$$

$$Q(A_v) : [x_{11}, x_{22}, x_{33}, x_{44}, x_{55}]$$

Where X_1-X_5 and $X_{11}-X_{15}$ are both probability values between [0–1], the probability distribution of A_u is $P(A_u)$, and the probability distribution of A_v is $Q(A_v)$.

- (2) According to the emotional tendency probability distribution $\vec{\theta}_{dt}$, Jensen-Shannon divergence (JS divergence) is introduced to obtain the similarity degree of emotional tendency among users. JS divergence, also known as JS distance, is a variant of KL scatter (Kullback-Leibler divergence), which is an index for calculating the similarity of two variables from the perspective of probability distribution in information theory [8]. The difference from the KL divergence is that the JS divergence value range is [0–1], the same is 0, and the opposite is 1, which makes the calculation of the similarity more precise and adds symmetry to the KL divergence. That is, $JS(P(A_u) || Q(A_v)) = JS(Q(A_v) || P(A_u))$. The process of obtaining the similarity of the user’s emotional inclination is as follows:

First, calculate the KL divergence according to formula (5) based on any two probability distributions $P(A_u)$ and $Q(A_v)$ obtained from the first step of this section.

$$KL(P(A_u) || Q(A_v)) = \sum P(A_u) \log \frac{P(A_u)}{Q(A_v)} \tag{5}$$

$$JS(P(A_u) || Q(A_v)) = \frac{1}{2} KL(P(A_u) || \frac{P(A_u) + Q(A_v)}{2}) + \frac{1}{2} KL(Q(A_v) || \frac{P(A_u) + Q(A_v)}{2}) \tag{6}$$

After obtaining the KL divergence, it is taken into the formula (6) to obtain the JS divergence between any two users. According to JS divergence, the formula for calculating the similarity of emotional tendency among users is as follows:

$$sml_e(A_u, A_v) = \frac{1}{1 + JS(P(A_u) || Q(A_v))} \tag{7}$$

The smaller $JS(P(A_u) || Q(A_v))$ is, the greater the similarity of the emotional tendency between any two users, and a rule that measures the similarity between two variables in accordance with JS divergence.

2.1.3 Definition and Calculation of Social Factors Similarity Among Users

Definition 4: After the interest similarity and sentiment similarity between users obtained by 2.1.1 and 2.1.2, we define the social factor (ie, interest + sentiment) similarity between any two users as the final The basic formula is as follows:

$$sml(A_u, A_v) = \eta sml_i(A_u, A_v) + (1 - \eta) sml_e(A_u, A_v) \tag{8}$$

$sml_i(A_u, A_v)$ is the interest of similarity between any two users, and $sml_e(A_u, A_v)$ is the similarity of sentiment orientation between any two users. Thus, the social factor

visit probability $\delta(A_u, P_x)$ of the user visiting an unvisited POI on social factors can be obtained, and the probability has been normalized. Where η is the weight coefficient. If $\text{sml}_i(A_u, A_v)$ is 0, it means that the interest similarity between user A_u and user A_v does not work, that is, it means that two users in real life have not visited the same POI jointly. At this time, the similarity of sentiment orientation plays a role, it is a good solution to the case where the numerator is equal to 0 when the interest similarity among users is calculated by the cosine similarity. To some extent, the problem of data sparsity is alleviated.

2.2 Modeling Based on Geographic Features in LBSN

The geographical feature in LBSN is to add unique spatial attributes based on Social Networking Services (SNS). This attribute plays an important role in POI recommendation because this factor is the essential difference between social networks and LBSNs. In real life, every user likes to visit the POI near his living place or near his work. On the other hand, the user prefers to visit the POI around the nearby points of interest he has visited, even if it is far from home. In other countries, the emergence of this phenomenon shows that geographical factors affect the probability of visit. Related research [9] shows that this kind of user visit behavior has geographical clustering phenomenon, which proves the above life phenomenon, and the distance between the same user to visit two POIs and the probability of their visit can be fitted by power law distribution, so this paper uses this method is used to get the probability that any user A_u can visit any POIs that he has not visited.

The process of obtaining geographic feature visit probability is as follows:

- (1) Calculate the distance between any two POIs by formula (9), (10) according to any two POI latitude and longitude coordinates (ie geographic features):

Assuming that the latitude and longitude of the two POIs are $P_x(\text{lat1}, \text{lon1})$ and $P_y(\text{lon2}, \text{lat2})$, then:

$$h = \sin^2(dlat / 2) + \cos(lat1) \times \cos(lat2) \times \sin^2(dlon / 2) \quad (9)$$

$$Dis(P_x, P_y) = 2 \times \sin(\text{sqrt}(h)) \times R \times 1000 \quad (10)$$

Where h is the large circle distance expressed in radians, $dlat = \text{lat1} - \text{lat2}$, $dlon = \text{lon1} - \text{lon2}$, and R is the radius of the earth (6,371 km), so the distance between any two POIs can be obtained.

- (2) Bringing the power law distribution formula (11) on the basis of obtaining the distance of any two POIs, the probability that the target user accesses the unvisited POI can be obtained.

$$Y = a \times X^b \quad (11)$$

Where Y is the probability of the user visiting the POI, X is the distance between the two POIs, a is the normalization constant, b is the scaling parameter. The values of a and b are obtained by training the power law distribution model through the training set using the maximum likelihood estimation method and the least square method, respectively.

Suppose the target user is A_u and the POI set he has visited is P_{list} . According to the distance between POIs, the probability that user A_u visits all POIs in P_{list} is as follows:

$$P_g[P_{list}] = \prod_{P_x, P_y \in P_{list} \wedge x \neq y} P_g[Dis(P_x, P_y)] \quad (12)$$

Where $Dis(P_x, P_y)$ represents the geographic distance between P_x and P_y in P_{list} , and $P_g[Dis(P_x, P_y)] = a \times [Dis(P_x, P_y)]^b$ conforms to our power-law distribution model.

Definition 5: Assume that the set of POIs for the entire data set is P , the target user is A_u , and his historical visited POIs list is P_{list} . For any one of the possible recommended POI $P_m \in (P - P_{list})$, the probability of A_u visiting P_m is:

$$P_g[P_m | P_{list}] = \frac{1}{P_{gmax}} \left\{ \prod_{P_n \in P_{list}} P_g[Dis(P_m, P_n)] \right\} \quad (13)$$

$P_g[P_m | P_{list}]$ is the geographical factor visit probability, where P_{gmax} is the normalized processing item, and $P_{gmax} = \max_{P_m \in P - P_{list}} \{P_g[P_m | P_{list}]\}$.

2.3 Sc-Ge Model

This paper combines the POI's geographical location information, comment text information, rating information and social relationship information in social networks. After the processing of 2.1 and 2.2, the probability that the target user visits an unvisited POI is affected by two aspects. The influence of factors, namely social visit probability factors and geographic visit probability factors. Therefore, this paper proposes a POI recommendation model Sc-Ge. The POI recommendation model considers that the probability of the target user visiting the POI is determined by the social factor visit probability and the geographic factor visit probability. Therefore, the two influencing factors are linearly combined to determine the final visit probability, and the final probability is defined as $P_{last}(A_u, P_m)$. The calculation formula is as follows shown as follows:

$$P_{last}(A_u, P_m) = \tau \times \delta(A_u, P_m) + (1 - \tau) \times P_g[P_m | P_{list}] \quad (14)$$

Where $\delta(A_u, P_m)$ represents the social factor visit probability, $P_g[P_m | P_{list}]$ represents the geographic factor visit probability, and τ represents the balance factor that

regulates the weight of the two factors. When $\tau = 1$, it means that only the social factor visit probability plays a role in the recommendation. At this time, it is not necessary to deal with the geographical factor visit probability. Similarly, when $\tau = 0$, only the geographical visit probability plays a role, and it is not necessary to deal with the social visit factor.

2.4 Sc-Ge Model Flow Chart

The overall flow of the Sc-Ge model is shown in Fig.1.

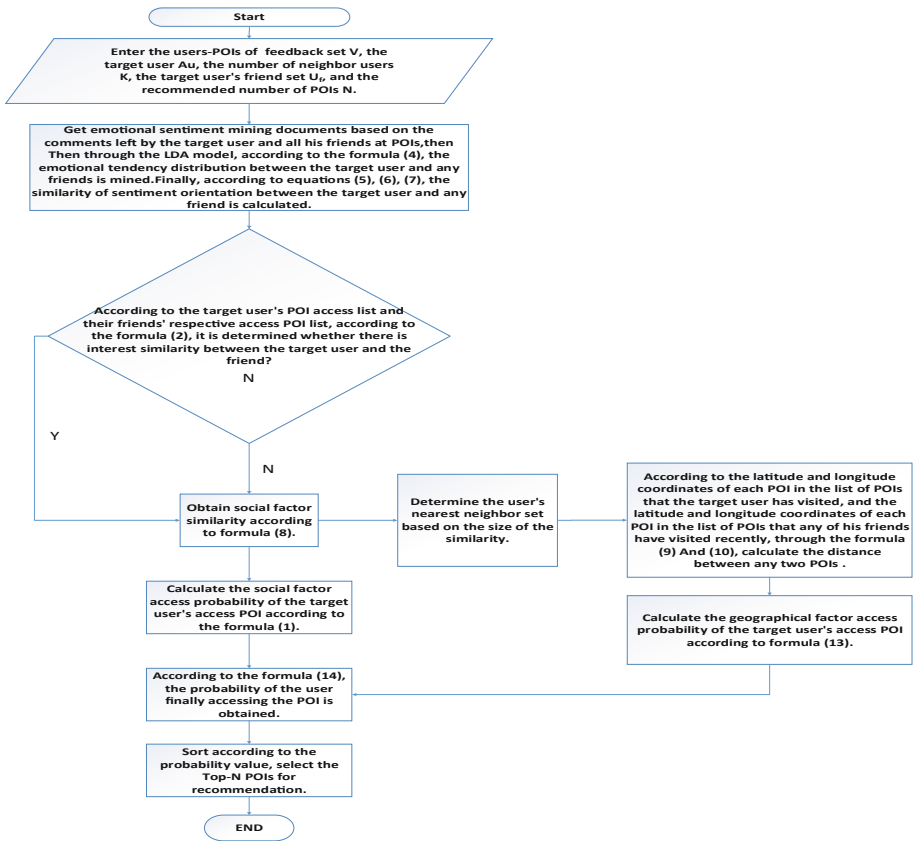


Fig. 1. Sc-Ge model flow chart

2.5 Algorithm Implementation in This Paper

Based on the above modeling and analysis process, this paper proposes the Sc-Ge POI recommendation model. The basic steps of its implementation are as follows:

Algorithm 1: Sc-Go Model Algorithm

Input: users-POIs feedback information matrix V , target user A_u , number of neighbor users K ,

number of recommendations N .

Output: N POIs recommended to the target user A_u .

Step 1: Calculate the similarity $sml(A_u, A_v)$ between the target user A_u and any other user

A_v by using formula (8);

Step 2: Determine the most similar neighbor set $U_f(A_u, K)$ of the target user A_u according to the size of $sml(A_u, A_v)$;

Step 3: Using the data in the neighbor set, calculate the social factor visit probability $\delta(A_u, P_m)$ between any two users according to the formula (1) in the definition 1;

Step 4: Using the data in the neighbor set, calculate the geographic factor visit probability $P_g[P_m | P_{list}]$ between any two users according to the formula (13) in the definition (5);

Step 5: According to the visit probability in step 3 and step 4, the final visit probability is calculated by formula (14), and the top- N POIs are recommended to the target user A_u according to the size of the values of $P_{last}(A_u, P_m)$.

3 Experimental and Experimental Results Analysis

In order to verify the superiority of the POI recommendation model of this paper compared with other mainstream POI recommendation algorithms, applying the POI recommendation model and other mainstream POI recommendation algorithms to the real life LBSN dataset, the experimental results are obtained, and the conclusions are obtained through comparison and analysis.

3.1 Experimental Data Set

In this section, we use data collected from the Yelp dataset, the largest review site in the United States, for data analysis. The Yelp data set includes 1,326,101 users and 174,567 POIs. In addition, Yelp also included 5,261,669 comments and 4,962,957 friendship pair, and the statistical results and data formats are shown in Tables 1, 2 and 3.

Table 1. Yelp data set statistic.

Number of related data	Yelp data set
Users	1326101
POIs	174567
Comments text	5261669
Friendship pairs	49626957

Table 2. Social relationship data format.

Data attribute	Yelp data set
user_id	oMy_rEb0UBEmMlu-zcxnoQ
Friend_id	cvVMmlU1ouS3I5fhutaryQ

Table 3. Rating and comment text data format.

Data attribute	Yelp data set
business_id	Ue6-WhXvI-_1xUIuapl0zQ
user_id	gVmUR8rqUFdbSeZbsg6z_w
Text	Red, white and bleu salad was super yum and a great addition to the menu!
Starts	1-5
Latitude	43.8409
Longitude	-79.3996

3.2 Evaluation Model Validity Index

In order to evaluate the performance of the POI recommendation model, this paper selects two effective evaluation indicators, Precision and Recall, to verify its performance.

$$Precision = \frac{N(I_{visited} \cap I_{re})}{N(I_{re})} \quad (15)$$

$$Recall = \frac{N(I_{visited} \cap I_{re})}{N(I_{visited})} \quad (16)$$

Where $I_{visited}$ represents the set of POIs that the target user has visited in the test data set. I_{re} represents a collection of the top-N recommended POIs.

3.3 Comparative Experiment and Analysis of Results

In order to verify the effective performance of the model, three mainstream POI recommendation algorithms are selected as the comparison algorithm. The representation and detailed description are as follows:

User-Cos: Calculate the similarity among users based on the cosine similarity of the user's common visit POIs, that is, the traditional user-based collaborative filtering for recommendation, without context information related to the user;

Fcf-Cos: Calculate the similarity among users based on the relationship using cosine similarity, that is, the traditional user-based collaborative filtering variant using the cosine similarity to calculate the similarity among users is improved, and there is no context information related to the user;

CoRe [10]: The POI recommendation model incorporates social relationship factors (ie, using traditional user-based collaborative filtering calculations) and geographic factors, but its geographic factor modeling uses a kernel density estimation method.

This article selects 100,500 socially friendly friendship pairs from 49,625,957 friendship pairs, including 1,304,243 comments, and the number of POIs visited is 42,830. In order to further improve the recommendation quality, the number of comments and visited POIs less than 3 times are filtered out. The data set was randomly divided into a 70% training set and a 30% test set according to a ratio of 7:3, and the experimental comparison analysis was performed.

After a number of parameter adjustment experiments to obtain the best experimental results, the paper finally sets the subject number parameter T_{num} of the LDA model to 75, the density of the document-topic distribution $\alpha = 50/T_{num} + 1$ and the topic-word distribution density $\beta = 0.15$. Set $\eta = 0.46$ when adjusting the social factor similarity in definition 4, and set $\tau = 0.35$ in formula (14) when making the final interest point recommendation.

3.3.1 Discussion on the Impact of Data Sparsity

The mainstream POI recommendation algorithm mainly uses the common visit items among users to calculate the similarity among users. In the actual LBSN, the common visit POI data is sparse and affects the result of POI recommendation. When $\tau = 1$, the influence of data sparsity on the recommendation results is discussed. That is to discuss the social influence factors of traditional user-based collaborative filtering calculation and the influence of social influencing factors on the experimental results in linear fusion similarity calculation in this paper. The comparison experiment is shown in Figs. 1 and 2:

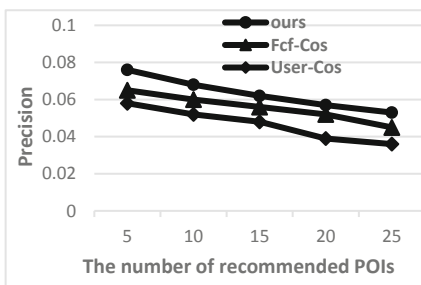


Fig. 2. Comparison of the precision of the 3 algorithms

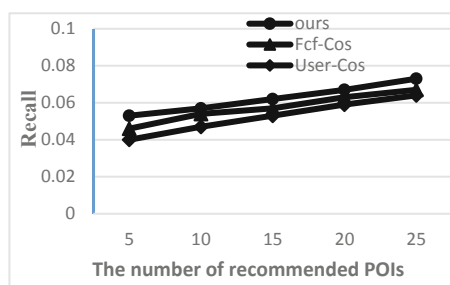


Fig. 3. Comparison of the Recall of the 3 algorithms

It can be seen from Figs. 2 and 3 that Fcf-Cos is higher than User-Cos in Precision and Recall, which indicates that the performance of collaborative filtering based on friend relationship in POI recommendation is better than the traditional user-based collaborative

filtering recommendation algorithm; At the same time, the performance of the Sc-Ge model is better than the other two algorithms in terms of Precision and Recall. It proves that the Sc-Ge model reduces the sparseness of the data and improves the performance of the recommendation by incorporating the comment text information related to the user.

3.3.2 Analysis of Final Recommendation Results

This paper combines the POI's geographical location information, comment text information, rating information and friend relationship information in social networks to design the Sc-Ge POI recommendation model. In the actual LBSN dataset Yelp, it is compared with the mainstream POI recommendation algorithms. The results are shown in Figs. 3 and 4:

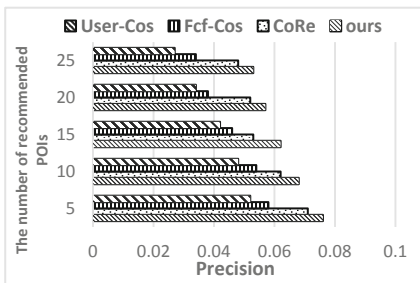


Fig. 4. Comparison of the Precision of the 4 algorithms

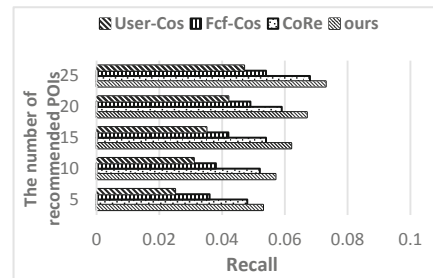


Fig. 5. Comparison of the Recall of the 4 algorithms

It can be seen intuitively from Figs. 4 and 5 that compared with the mainstream POI recommendation algorithms, Sc-Ge, a personalized POI recommendation model that combines heterogeneous information, has improved both Precision and Recall. Both this paper Sc-Ge model and CoRe's performance is better than that of Fcf-Cos and User-Cos. The fusion of user-related context information (especially geographic location information) helps to improve the performance of the POI recommendation system. Based on the above comparative experimental analysis, it can be seen that the fusion of multi-heterogeneous information personalized POI recommendation model Sc-Ge alleviates data sparsity to some extent. At the same time, social influence factors and geographical influence factors can be adjusted to have better robustness, which improves the performance of the POI recommendation system and has good application value.

4 Conclusion

This paper combines the multi-heterogeneous information of POI's commentary text information, rating information, geographical location information and friend information in social networks, and proposes the Sc-Ge model. The model considers that there are two main factors that determine if the user will visit to POI, namely social

factors and geographical factors. When recommended, the model has good robustness due to the fusion of multi-heterogeneous information. At the same time, after calculating the user similarity that combining similarity calculated by cosine similarity with similarity that using the LDA to mine the user interest topic distribution then use JS divergence to calculate applying to the POI recommendation. It eases the impact of data sparsity and improves the Precision and Recall of recommendations. In recent years, machine learning and artificial intelligence have become more and more hot. Integrating new technologies such as network representation learning, reinforcement learning and game theory into POI recommendation is a good research direction.

References

1. Jones, S.L., Kelly, R.: Dealing with information overload in multifaceted personal informatics systems. *Hum.-Comput. Interact.* **33**(1), 1–48 (2017). <https://doi.org/10.1080/07370024.2017.1302334>
2. Li, X.: Survey of collaborative filtering algorithms. *J. Shanqiu Normal Univ.* **34**(285(09)), 13–16 (2018)
3. Huang, L., Ma, Y., Liu, Y., et al.: Multi-modal Bayesian embedding for point-of-interest recommendation on location-based cyber-physical-social networks. *Future Gener. Comput. Syst.* S0167739X17310191 (2017)
4. Dai, S., Li, Y., Hai, L.: Personalized location recommendation algorithm mixing multi-factors. *Comput. Eng.* **44**(6), 300–304,311 (2018)
5. Ye, M., Yin, P., Lee, W.C., et al.: Exploiting geographical influence for collaborative point-of-interest recommendation. In: *Proceeding of the 34th International ACM SIGIR Conference on Research and Development in Information Retrieval, SIGIR 2011, Beijing, China, 25–29 July 2011*. ACM (2011)
6. Fang, M.-Y., Dai, B.-R.: Power of bosom friends, POI recommendation by learning preference of close friends and similar users. In: Madria, S., Hara, T. (eds.) *DaWaK 2016*. LNCS, vol. 9829, pp. 179–192. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-43946-4_12
7. Zhu, J., Wang, C., Guo, X., et al.: Friend and POI recommendation based on social trust cluster in location-based social networks. *EURASIP J. Wirel. Commun. Netw.* **2019**(1) (2019)
8. Kullback, S., Leibler, R.A.: On Information and sufficiency. *Ann. Math. Stat.* **22**(1), 79–86 (1951)
9. Wang, X., Yuan, J., Qin, F.: Point-of-interest recommendation based on comment text in location social network. *Comput. Sci.* **2017**(12), 251–254, 284 (2017)
10. Zhang, J.D., Chow, C.Y.: CoRe: exploiting the personalized influence of two-dimensional geographic coordinates for location recommendations. *Inf. Sci.* **293**, 163–181 (2015)



RFT: An Industrial Data Classification Method Based on Random Forest

Caiyun Liu, Xuehong Chen, Yan Sun^(✉), Shuaifeng Yang, and Jun Li

China Industrial Control Systems Cyber Emergency Response Team,
Beijing, China
cic2019sy@163.com

Abstract. Large amounts of data are generated daily in the industrial field, the safety of which is related to national security and social interests. Data classification is an important component of data protection because different types of data may require different protection methods. When compared with traditional data, industrial data mostly comprise real-time monitoring data, thereby possessing high requirements for time efficiency. However, the existing classification methods aimed at accuracy optimization cannot meet the requirements of time efficiency. To solve this problem, a random tree-based random forest model is proposed. This model is a combination classification model with attribute sampling, which can have the accuracy of random forest and the rapidity of random tree. Experiments show that the proposed model improves the accuracy of the existing single model, decreases the lost time of random forest, and is suitable for data classification in an industrial environment.

Keywords: Random forest · Time efficiency · Classification · Random tree

1 Introduction

With the advent of the new industrial revolution era, the industrial control system has slowly moved from being closed to open, and its security has become increasingly severe. The protection of industrial data security is an urgent problem begging for solutions in the development of the industrial Internet. In this study, data classification is the precondition and the core foundation of industrial Internet data security considering its usefulness when making strategies for classification decision-making in data protection. However, compared with traditional data, the volume of industrial Internet data is extremely large, causing difficulty in data classification. Furthermore, the data mostly comprise real-time monitoring data; thus, they have higher requirements for time efficiency. Relevant industry enterprises are accelerating the formulation of classification standards and classification technology. The automatic classification of industrial Internet data has been an emerging trend.

The application of data classification algorithms in machine learning to industrial Internet data classification is an experimental approach to the automatic classification of industrial data. However, compared with traditional data, industrial data require higher time efficiency. Therefore, establishing a model that considers accuracy and time is necessary to ensure the performance of industrial Internet data. However, the current

single classifier does not consider both accuracy and time efficiency. To solve this problem, this research proposes the *RFT* classification model using fault data of fan tooth belts. The research contributions are as follows.

- An automatic classification method for industrial data is proposed on the basis of random tree. Compared with the general random forest model, attribute sampling is applied to improve classification time efficiency. Experiments show that the proposed model can save more time than the random forest.
- The model proposed in this paper is based on ensemble learning. Experiments show that this model has higher classification accuracy compared with the single models such as Naive Bayes and random tree.

The remainder of this paper is organized as follows. Section 2 introduces the related works. Section 3 establishes the classification model proposed in this research. Section 4 conducts an experimental analysis of the proposed model. Section 5 summarizes the work of this research.

2 Related Works

Many studies at home and abroad focus on data protection and data classification, but studies scarcely specialize in industrial data classification. To solve the problem of industrial data classification, Xu et al. [1] proposed a classification method for remotely sensed data sources using the two-branch convolution neural network (CNN); Dörksen et al. [2] presented a ComRef-2D-ConvHull method for linear classification optimization in lower-dimensional feature space, which is based on ComRef. However, these algorithms focused on accuracy, and their time efficiency is not very good. Platos et al. [3] described the processing of two different datasets acquired from a steel-mill factory using three different methods, namely, SVM, Fuzzy Rules, and Bayesian classification. However, its accuracy is insufficient. For other typical classification models, Chutia et al. [4] developed an effective method based on the principal component analysis technique to improve the classification accuracy of Random Forest both on predictive ability and computational expenses, but the principal component analysis technique assumes that the variables obey Gaussian distribution. When the variables do not obey Gaussian distribution (e.g., uniform distribution), scaling and rotation will occur; thus, it is not suitable for time-series data of the industrial Internet. Tong et al. [5] proposed a novel privacy-preserving naive Bayes learning scheme with multiple data sources. The proposed scheme enables a trainer to train a naive Bayes classifier over the dataset provided jointly by different data owners, without the help of a trusted curator; however, its time performance is poor. Augereau et al. [6] proposed a document image classification method by combining textual features extracted with the bag of words technique and visual features extracted with the bag of visual words technique, but data generated by Internet of Things devices are often structured and numerical and is thus unsuitable for non-text industrial data.

In summary, current classification methods mostly focus on text and image data, and little research is specialized for industrial data classification. Furthermore, current classification methods highly focus on accuracy, which cannot meet the time efficiency

requirements of industrial data. Moreover, classification accuracy requires continued improvements.

3 Classification Model

The single classifier has limited classification accuracy, whereas the combination model of the naive Bayes algorithm and decision tree consumes considerable time. Decreasing the time consumption of the combined model is a core idea of the model built in this research. On this basis, a random forest model based on random tree is proposed. Random forest is an ensemble classifier that integrates many decision trees into forests and uses them together to predict the final results. The classifier can solve the inherent shortcomings of a single model, compensating for shortcomings and avoiding limitations. Specifically, it first generates j training sets using a bootstrap method that can regenerate many new samples of the same size from the samples. For each training set, a decision tree is constructed. When the nodes search for features to split, some features are randomly extracted from the feature set, and the optimal solution is found among the extracted features to split nodes. Considering the bagging idea, the random forest method is equivalent to sampling both samples and features, possibly avoiding over-fitting. At the same time, given that it is a combination-based algorithm, its accuracy is usually higher than other machine-learning algorithms. Random tree is a method of randomly selecting several attributes to construct a tree; thus, its classification time is relatively low. This research applies the concept of random tree to random forest to improve the efficiency of random forests. First, we generate several training samples, and then some attributes are randomly selected. Then, we extract features to make decisions. In other words, all samples, attributes, and features are sampled to construct classifiers in our model. The principle of the model is as follows:

Assuming that the training sample has l records, then the total sample can be marked as $G = \{g_1, g_2, \dots, g_l\}$. j trees are generated after sampling and $j \in \{1, 2, 3, \dots, d\}$ $d > 0$. The sample attribute $X \subseteq R^n$ is a set of n -dimensional vectors. Attribute probability $P = \{0, 1\}$ is a set of two-dimensional vectors, and $E \subseteq R^s$ is a set of s -dimensional eigenvectors. The output $Y = \{c_1, c_2, c_3, \dots, c_k\}$ is a set of class tags, and the input attribute vector is $x \in X$. The attribute probability vector is $p \in P$, the feature vector is $e \in E$, and the output vector is $y \in Y$.

Then, the RFT is constructed as follows:

For the i th ($i \leq j$) subsample in a Random Forest $T = \{g_1, g_3, \dots, g_{2h-1}\}$, $h < \frac{l+1}{2}$, assuming that the selection of attributes uses even multiple interpolation sampling. Then, the set of input attributes is

$$\begin{aligned} X &= \{p_0 \cdot x_1, p_1 \cdot x_2, p_0 \cdot x_3, \dots, p_1 \cdot x_n\} \\ p_0 &= 0, p_1 = 1, n = 2m, m > 0 \end{aligned} \tag{1}$$

The feature vectors are extracted from the input attributes as follows:

$$X \rightarrow E = \{e_1, e_2, e_3 \dots e_s\} \tag{2}$$

Then, the eigenvector is input into the classifier to obtain the classification result of the *i*th tree marked as y_i .

The final classification result of the classifier is

$$Y = vote\{y_1, y_2 \dots y_i \dots y_j\} \tag{3}$$

Figure 1 shows the classification principle.

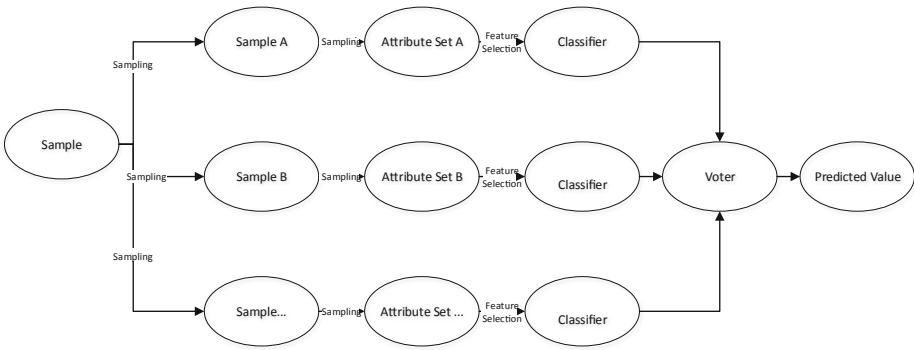


Fig. 1. Principle of the RFT model

4 Experiment

This section illustrates the classification performance of the RFT model via multi-round experiments on fault data of fan tooth profiles, and we comprehensively analyze the performance of the model via comparative experiments.

4.1 Description of Source Data

This study uses the fan tooth profile with fault data as the research object; these data usually comprise hundreds of variables as a type of SCADA monitoring data. Thus, the data used in this screening retained 28 continuous numerical variables, which cover the fan working parameters, environmental parameters, state parameters, and other dimensions. Table 1 presents the name and description of the variables.

Table 1. Description of source data.

Serial number	Attribute	Description
1	time	time stamp
2	wind_speed	wind speed
3	generator_speed	generator_speed
4	power	active power (kw) on network side
5	wind_direction	wind direction (°)
6	wind_direction_mean	25 s average wind direction
7	yaw_position	yaw position
8	yaw_speed	yaw speed
9	pitch1_angle	angle of pitch1
10	pitch2_angle	angle of pitch2
11	pitch3_angle	angle of pitch3
12	pitch1_speed	speed of pitch1
13	pitch2_speed	speed of pitch2
14	pitch3_speed	speed of pitch3
15	pitch1_moto_tmp	temperature of pitch motor1
16	pitch2_moto_tmp	temperature of pitch motor2
17	pitch3_moto_tmp	temperature of pitch motor3
18	acc_x	acceleration in x-direction
19	acc_y	acceleration in y-direction
20	environment_tmp	ambient temperature
21	int_tmp	cabin temperature
22	pitch1_ng5_tmp	ng5 1 temperature
23	pitch2_ng5_tmp	ng5 2 temperature
24	pitch3_ng5_tmp	ng5 3 temperature
25	pitch1_ng5_DC	ng5 1 Charger DC Current
26	pitch2_ng5_DC	ng5 2 Charger DC Current
27	pitch3_ng5_DC	ng5 3 Charger DC Current
28	group	data classification identification

Prior to classification, the relationship between the attributes and group undergoes preliminary analysis. Taking pitch 3_ng5_tmp, Int_tmp, Environment_tmp, and time as examples, Figs. 2, 3, 4 and 5 present the effects of these attributes on the group. The attributes in Table 1 have a certain functional relationship with the classification identifiers and can be used as classification attributes.

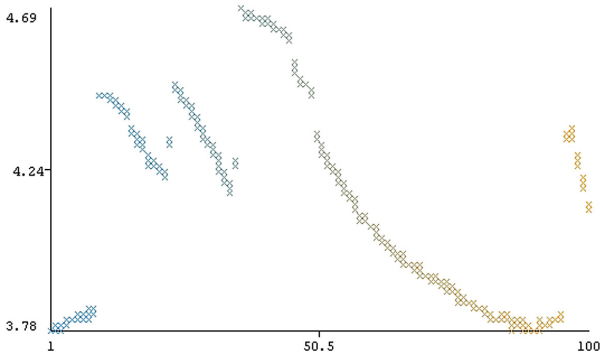


Fig. 2. Relationship between pitch 3_ng5_tmp and group

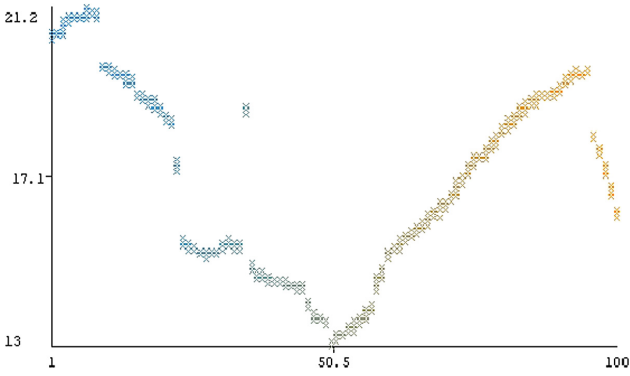


Fig. 3. Relationship between Int_tmp and group

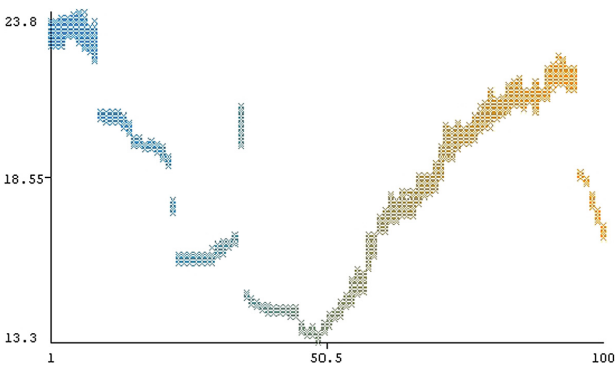


Fig. 4. Relationship between Environment_tmp and group

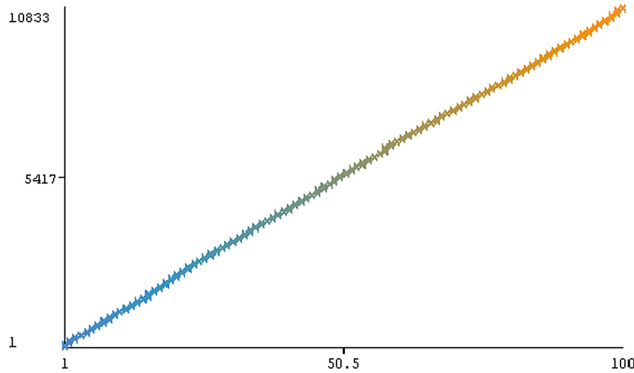


Fig. 5. Relationship between time and group

4.2 Evaluation Indicators

This paper reports the kappa coefficient and accuracy to observe the performance. Kappa coefficient is a statistic that measures inter-rater agreement for qualitative items. It is generally thought to be a more robust measure than a simple percent agreement calculation because it considers the possibility of the agreement occurring by chance [7]. Accuracy refers to the ratio of the number of correctly predicted samples to the total number of predicted samples. In bi-classification, for example, if TP indicates that the forecast result is positive and the actual result is positive, FP represents that the forecast result is positive and the actual result is negative, TN represents that the forecast result is negative and actual is negative, and FN represents that the forecast result is negative and actual is positive. Then, accuracy can be calculated as follows:

$$Acc. = (TP + TN) / (TP + TN + FP + FN) \quad (4)$$

Although this research deals with a non-binary classification problem, Formula (4) describes the calculation method. The difference is that TP , FP , TN , and FN are weighted values here.

4.3 Experimental Verification

To verify the effectiveness of the proposed algorithm, the algorithm is compared with random forest [8], random tree, and naive Bayes; then, the parameters in the experiment are determined via a ten-fold cross-validation process. k denotes kappa coefficient, NB denotes naive Bayes, RF denotes random forest, and RT denotes random tree in the next part.

First Group of Experiments. The number of training samples and test samples selected in this group of experiments is 10,833. Five algorithms are used to observe classification performance. Tables 2 and 3 reflect their performances.

Table 2. Classifier performance when number of instances = 10833

Algorithm	Acc.	k	time(s)
<i>RF</i>	99.16%	0.9915	5.92
<i>RT</i>	96.7968%	0.9676	0.11
<i>RFT</i>	99.16%	0.9915	0.7
<i>NB</i>	90.3166%	0.9022	0.05

Table 3. Performance comparison of RFT with other models when number of instances = 10833

Algorithm	Acc. _{cmp}	k _{cmp}	time _{cmp} (s)
<i>RF</i>	0	0	-88.17%
<i>RT</i>	2.44%	2.47%	5.36
<i>NB</i>	9.79%	9.90%	13

Second Group of Experiments. The number of training samples and test samples selected in this group of experiments is 10,552. Five algorithms are used to observe classification performance. Tables 4 and 5 display their performances.

Table 4. Classifier performance when number of instances = 10552

Algorithm	Acc.	k	time(s)
<i>RF</i>	98.8154%	0.988	5.39
<i>RT</i>	94.475%	0.9442	0.09
<i>RFT</i>	99.0049%	0.9899	0.33
<i>NB</i>	91.7077%	0.9162	0.04

Table 5. Performance comparison of RFT with other models when number of instances = 10552

Algorithm	Acc. _{cmp}	k _{cmp}	time _{cmp} (s)
<i>RF</i>	0.19%	0.19%	-93.88%
<i>RT</i>	4.79%	4.84%	2.67
<i>NB</i>	7.96%	8.04%	7.25

Third Group of Experiments. The number of training samples and test samples selected in this group of experiments is 10,403. Five algorithms are used to observe classification performance. Tables 6 and 7 present their performances.

Table 6. Classifier performance when number of instances = 10403

Algorithm	Acc.	k	time(s)
<i>RF</i>	98.9618%	0.9895	5.78
<i>RT</i>	95.2514%	0.952	0.1
<i>RFT</i>	99.0291%	0.9902	0.31
<i>NB</i>	90.1567%	0.9006	0.04

Table 7. Performance comparison of RFT with other models when number of instances = 10403

Algorithm	Acc._cmp	k_cmp	time_cmp(s)
<i>RF</i>	0.06%	0.07%	-94.63%
<i>RT</i>	3.97%	4.01%	2.1
<i>NB</i>	9.84%	9.95%	6.75

Tables 3, 5 and 7 are performance comparisons between *RFT* and other models. Assuming that all other models are represented by other models, the numerical formulas in these tables are as follows.

$$Acc_cmp = (Acc_{RFT} - Acc_{other\ model}) / Acc_{other\ model} \quad (5)$$

$$k_cmp = (k_{RFT} - k_{other\ model}) / k_{other\ model} \quad (6)$$

$$time_cmp = (time_{RFT} - time_{other\ model}) / time_{other\ model} \quad (7)$$

4.4 Analysis of Experimental Results

As Table 3 shows, the accuracy and kappa coefficient of the *RFT* model are not lower than those of other models. The accuracy of the *RFT* model is 2.44% higher than that of the random tree model and 9.79% higher than that of the Naive Bayes model. In addition, the time loss of the *RFT* model is considerably lower than other benchmark models, except for the naive Bayes model. However, given the low accuracy of naïve Bayes, the *RFT* model is compatible with accuracy and time loss. In summary, the *RFT* model is suitable for industrial data classification, considering time efficiency and classification accuracy.

5 Conclusions

This research proposes a “random tree-based random forest model” for classification of SCADA real-time monitoring data. The model uses the idea of random tree to extract features from attributes after sampling, substantially decreasing the loss time compared

with random forest with higher classification accuracy than single models, such as Naïve Bayes. Experiments show that the *RFT* model can simultaneously meet the needs of industrial data for classification accuracy and classification time efficiency.

References

1. Xu, X., Wei, L., Ran, Q., et al.: Multisource remote sensing data classification based on convolutional neural network. *IEEE Trans. Geosci. Remote Sens.* **PP(99)**, 1–13 (2018)
2. Dörksen, H., Mönks, U., Lohweg, V.: Fast classification in industrial big data environments. In: 19th International Conference on Emerging Technologies & Factory Automation (ETFA 2014). IEEE (2014)
3. Platos, J., Kromer, P.: Prediction of multi-class industrial data. In: International Conference on Intelligent Networking & Collaborative Systems (2013)
4. Chutia, D., Borah, N., Baruah, D., et al.: An effective approach for improving the accuracy of a random forest classifier in the classification of Hyperion data. *Appl. Geomat.* (2) (2019)
5. Tong, L., Jin, L., Liu, Z., et al.: Differentially private Naive Bayes learning over multiple data sources. *Inf. Sci.* **444**, 89–104 (2018). S0020025518301415
6. Augereau, O., Journet, N., Vialard, A., et al.: Improving classification of an industrial document image database by combining visual and textual features. In: IAPR International Workshop on Document Analysis Systems. IEEE (2014)
7. Liu, C., Wang, W., Zhang, Y., et al.: Predicting the popularity of online news based on multivariate analysis. In: 2017 IEEE International Conference on Computer and Information Technology (CIT). IEEE Computer Society (2017)
8. Svetnik, V.: Random forest: a classification and regression tool for compound classification and QSAR modeling. *J. Chem. Inf. Comput. Sci.* **43**(6), 1947 (2003)



A New Non-smart Water Meter Digital Region Localization and Digital Character Segmentation Method

Fei Lei, Zhimei Xiong^(✉), and Xueli Wang

Beijing University of Technology, Beijing, China
{leifei,xlwang}@bjut.edu.cn, xiongzhimei001@163.com

Abstract. The efficient and accurate meter reading method can help us manage water resources more reasonably. Aiming at the image of the non-smart water meter taken by mobile phone photographing, a new method for locating and fragmenting digital area of water meter is proposed in this paper. Firstly, locate the position of the measuring unit in the water meter. Obtain the binary image of the measurement unit and correct the image according to its vertical projection feature, and then locate the number area of the water meter again. The adaptive threshold is used to binarize the digital region, then the median filtering and connected-domain method are used for denoising. Finally, the digital segmentation is completed by finding the circumscribed rectangle of the character. The experimental results show that the method can effectively locate the digital area and segmentation numeric characters for the water meter image with rotation problem and has strong adaptability to the water meter of different water meter companies.

Keywords: Water meter · SIFT · Picture correction · Character segmentation

1 Introduction

Water meter is one of the meters that every household used to record the water consumption. An ideal meter reading method can reduce cost and increase meter reading efficiency at the same time. Today's meter reading methods are mostly manual meter reading, prepaid, and wireless remote meter reading. The latter two methods are not applicable to traditional mechanical water meter and need to replace the water meter which increases the cost of retrofitting. Although the manual meter reading method does not need to replace the water meter, it has problems such as low efficiency and easy to make mistakes [1]. Based on the development of machine vision, there is also recognition of numbers on water meters through processing the images of mechanical water meter which are photographed. However, most of the methods are to install a fixed camera on the mechanical water meter, that is, the digital region of the water meter is also fixed in the picture [2]. At present, almost every household has at least one smartphone. Instead of relying on a camera, we can take water meter photos directly from our mobile phone. However, due to the shooting angle of the phone, there

will be some problems such as picture rotation. It is necessary to correct the water meter image and locate the number area before recognizing the water meter digital.

Aiming at the water meter image obtained by mobile phone photographing, a new method for localization and segmentation of water meter digital region is proposed in this paper. Firstly, the SIFT [3–5] algorithm is used to identify the measurement unit “M” in the water meter. For the rotation problem of the water meter image caused by mobile phone photographing, the water meter picture is corrected by the characteristics of vertical projection histogram after rotating “M”, thereby positioning and cutting the water meter digital area. Then, the adaptive threshold is used to binarize the image of the digital region [6], and the binary image of the digital region is obtained. After median filtering and connected domain denoising [7, 8], digital character segmentation is achieved by taking the circumscribing rectangle of each number in the digital region [9]. The main contributions of this paper are summarized as follows:

- For images that are not taken with fixed camera, we need to correct the image first in order to locate the digital region. This paper proposes a new algorithm to correct the picture and then locate the digital region based on the characteristics of the water meter picture, that is, the measurement unit on the dial of the water meter.
- the image of a digital area cut from a water meter image is processed and then segmented. For the large-area noise, the connected-domain method is used to denoise, and the morphological processing is used to solve the problem of character break after binarization.

The paper is structured as follows: Sect. 2 mainly introduces the SIFT algorithm and propose a new algorithm for image correction. Section 3 introduced the processing of digital area pictures and the segmentation of digital characters. Section 4 showed the experimental results and shortcomings of this paper. Section 5 is the summary for this paper.

2 Digital Region Positioning

The automatic reading of the water meter is mainly to find the digital region of the water meter, and then identify the digit characters in sequence after processing the digital region. For water meter image taken by non-fixed cameras, finding the digital area of the water meter is critical to achieving automatic reading of the water meter. This section describes a new algorithm for locating the water meter reading area [10, 11]. Using the SIFT algorithm to locate the measurement unit “M” on the water meter, then correcting the water meter image based on the vertical projection characteristics of the “M” after rotated, finally determining the position of the digital area.

2.1 Introduction to SIFT Algorithm

The scale-invariant feature transform algorithm [12] was proposed by Professor David G. Lowe of the University of British Columbia in 1999 and was refined in 2004. The algorithm extracts unique and invariant features from the image and is used to match the target or scene between different perspectives. The extracted features are invariant to image scale and rotation and are robust to light and noise. There are several main steps in generating a feature point set.

Scale-Space Extrema Detection. Construct image pyramid and construct Gaussian difference scale space (DOG). $L(x, y, \sigma)$ is defined as an image scale space function, that is produced from the convolution of a variable-scale Gaussian, $G(x, y, \sigma)$, with an input image, $I(x, y)$:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \tag{1}$$

Where $*$ is the convolution operation in $G(x, y, \sigma)$ and $I(x, y)$, x, y represent the horizontal and vertical coordinates of the image, respectively, and σ is the scale space coordinate.

To efficiently detect keypoints in the scale space, it is necessary to construct a Gaussian difference scale space $D(x, y, \sigma)$:

$$\begin{aligned} D(x, y, \sigma) &= (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) \\ &= L(x, y, k\sigma) - L(x, y, \sigma) \end{aligned} \tag{2}$$

Where k is a constant factor of a multiple of two nearby scale spaces, $L(x, y, \sigma)$ represents an image generated by convolving a Gaussian filter with the original image, and $I(x, y)$ represents the original image.

In order to detect the local maximum and minimum values of $D(x, y, \sigma)$, each sample point is compared to its eight neighbors in the current image and nine neighbors in the scale above and below. It is selected only if it is larger than all of these neighbors or smaller than all of them.

Accurate Positioning of Feature Points. The extreme points of discrete space are not true extreme points. The method of using continuous spatial extreme points obtained by interpolation of known discrete spatial points is called sub-pixel interpolation. In order to improve the stability of keypoints, curve fitting of the scale space DOG function is required. The Taylor expansion or fitting function of the DOG function in the scale space is:

$$D(X) = D + \frac{\partial D^T}{\partial X} X + \frac{1}{2} X^T \frac{\partial^2 D}{\partial X^2} X \tag{3}$$

Where $x = (x, y, \sigma)^T$.

Keypoint Direction Allocation. To create a keypoint descriptor, first calculate the gradient size and orientation of each image sample point in the vicinity of the keypoint location. In order to make the descriptors have rotational invariance, it is necessary to utilize the local image properties to assign a consistent orientation to each keypoint. The keypoints descriptor can be related to this orientation and therefore achieve the invariance of image rotation. The image gradient method is used to obtain the stable direction of the local structure. For the keypoints detected in the DOG pyramid, the gradient and direction distribution characteristics of the pixels in the 3σ neighborhood window of the Gaussian pyramid image are collected. The modulus and orientation of the gradient are as follows:

$$m(x, y) = \sqrt{(L(x+1, y) - L(x-1, y))^2 + (L(x, y+1) - L(x, y-1))^2} \quad (4)$$

$$\theta(x, y) = \tan^{-1} \left(\frac{L(x, y+1) - L(x, y-1)}{L(x+1, y) - L(x-1, y)} \right) \quad (5)$$

Where $L(x, y)$ represents an image produced from the convolution of a Gaussian filter with the original image.

After completing the gradient calculation of the keypoints, the histogram is used to calculate the gradient orientations of the pixels within a region. An orientation histogram is formed from the gradient orientations of sample points within a region around the keypoint. The orientation histogram divides the orientations range of 0 to 360° into 36 bins, each of which is 10° . Each sample added to the histogram is weighted by its gradient magnitude and by a Gaussian-weighted circular window with a σ that is 1.5 times that of the scale of the keypoint. The peak of the orientation histogram corresponds to the gradient orientations of pixels within a region around the feature point, with the maximum value in the histogram as the dominant direction of the keypoint. In order to enhance the robustness of the matching, the direction in which the peak value is greater than 80% of the peak value of the dominant direction is retained as the auxiliary direction of the keypoint. Therefore, for keypoint positions of multiple peaks of the same gradient value, multiple keypoints with different orientations will be created at the same location and scale. Only about 15% of the keypoints are assigned multiple orientations, but these contribute significantly to the stability to the matching. In the actual programming implementation, the keypoints are copied into multiple keypoints, and the orientations are assigned to the keypoints after the copying, and the discrete gradient orientation histograms are subjected to interpolation fitting processing to obtain more accurate orientation angle value. Now, keypoints containing position, scale and orientation will be detected.

Keypoint Description. The image gradient magnitudes and orientations are sampled around the keypoint location, and the gradients of the sample points are precomputed. As shown in the Fig. 1, they are illustrated with small arrows at each sample position. The scale of the keypoints is used to select the level of Gaussian blurring of the image. A Gaussian weighting function with σ equal to half the width of the descriptor window is used to assign a weight to the amplitude of each sample point so that the weight can be smoothly reduced. The purpose of this Gaussian window is to avoid sudden changes in the descriptor with small changes in the position of the window, and to give less emphasis to gradients that are far from the center of the descriptor, as these are most affected by misregistration errors.

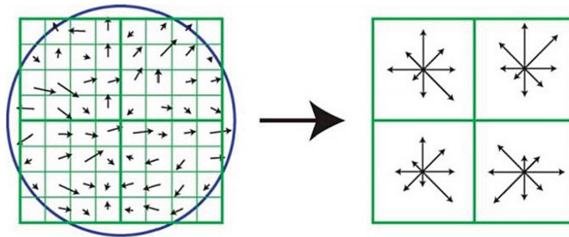


Fig. 1. Image gradients and keypoint descriptors.

The following figure shows a 2×2 descriptor array computed from an 8×8 set of samples, whereas the experiments in this paper use 4×4 descriptors computed from a 16×16 sample array.

In order to ensure that the feature vector has rotation invariance, the angle θ is rotated in the nearby neighborhood centering on the feature point, that is, the gradient orientations are rotated to the keypoint orientations (see Fig. 2).

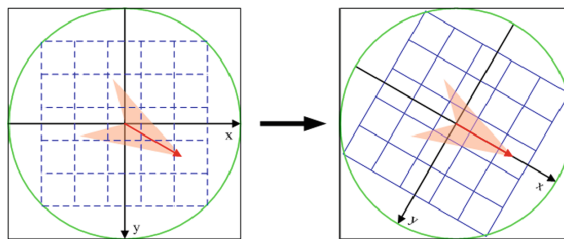


Fig. 2. Rotation diagram.

The new coordinates of the sampling points in the rotated region are as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{6}$$

The rotated region is divided into $d \times d$ sub-regions, and gradient histograms of multiple orientations are calculated in the sub-region, and the accumulated values of the gradient orientations in each orientation are plotted to form a seed point. Lowe’s paper experiments show that the best results are achieved with a 4×4 array of histograms with 8 orientation bins in each, so it is different from the dominant orientation. At this time, the gradient orientation histogram of each sub-region divides $0^\circ\text{--}360^\circ$ into 8 direction intervals, each interval is 45° . That is, each seed point has gradient intensity information of 8 direction intervals. Since there are $d \times d$, that is, 4×4 sub-regions, a total of $4 \times 4 \times 8 = 128$ data is finally formed, forming a 128-dimensional SIFT feature vector.

2.2 Digital Region Positioning

In order to effectively obtain the reading of the water meter, you first need to obtain the digital area of the water meter. The flowchart of digital area positioning is shown in Fig. 3:

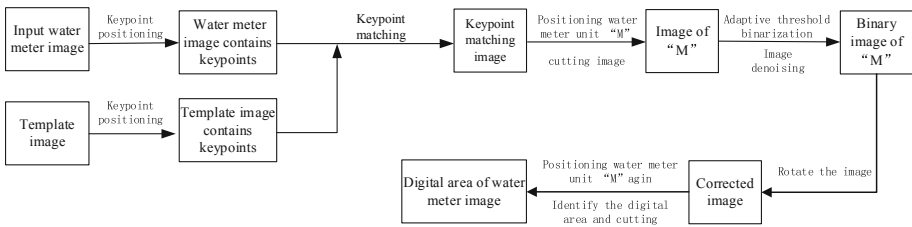


Fig. 3. Digital region positioning flowchart.

Positioning Unit of Measurement. We present a picture of the measurement unit “M” of the water meter as a template picture, obtain the keypoints of the template picture and the water meter image to be detected through the SIFT algorithm, and obtain two keypoint sets SET1 and SET2. For each of the keypoints in SET1, find the best match from SET2 (that is, the one with the smallest Euclidean distance is the best match), and then, in turn, find the best match from SET1 for each keypoint of SET2, only those keypoints that are considered to be the best match for each other are the matching points. Since each keypoint has 128 dimensions, two keypoint vectors are set as $R = (r_1, r_2, \dots, r_{128})$ and $S = (s_1, s_2, \dots, s_{128})$, and the Euclidean distance between R and S can be calculated as follows:

$$d = \sqrt{((r1 - s1)^2 + (r2 - s2)^2 + \dots + (r128 - s128)^2)} \quad (7)$$

The smaller the d value is, the higher the similarity of the two keypoints and the higher the matching degree is.

After using keypoints matching, the effect is shown in the Fig. 4:

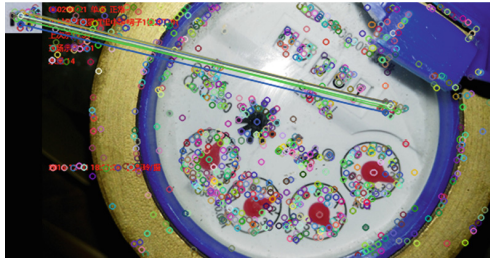


Fig. 4. Keypoint matching.

Image Correction. Through keypoint matching, the measurement unit “M” can be found in the water meter picture. For normal pictures, we know that the position of digital region is at the same horizontal position as “M”, to the left of “M”. But for the rotated water meter picture, we cannot obtain the rotation information of the water meter through keypoint matching. Therefore, it is necessary to correct the water meter picture before processing the digital region [13, 14].

RANSAC algorithm [15] is often used in computer vision, such as solving related problems and estimating the basic matrix of stereo camera at the same time, and calculating transformation matrix when splicing images. General target detection can use the homography matrix calculated by this algorithm to obtain the transformation relationship between the two images, thereby correcting the images. However, in real life, due to different manufacturers, the printing font on the water meter is also different, with the result that the “M” on the water meter is only similar to the template rather than the same, and it is impossible to correct the water meter picture through local transformation matrix. Figure 5 shows the position of the template “M” calculated by this method in the water meter to be tested. As shown in the figure, this method cannot locate “M” correctly, so it cannot correct the water meter picture.

The algorithm steps are as follows:

Algorithm: ImgRotAngleBouNodeExt

Input: all matching points
ct: Mismatch range threshold

Output: final rotation angle

1. sort all matching points in the X direction, take the median point $x1$
 2. sort all matching points in the Y direction, take the median point $y1$
 3. **for** every matching point(x, y) **do**
 4. **if** $abs(x - x1) > ct$ or $abs(y - y1) > ct$
 5. delete the match point
 6. **end if**
 7. **end for**
 8. sort all new matching points in the X direction, take the median point $x2$
 9. sort all new matching points in the Y direction, take the median point $y2$
 10. intercept "M" from the new median point to obtain the water meter unit image *unitImg*
 11. call function *cvtColor()*
 12. call function *adaptiveThreshold()*
 13. call function *medianBlur()* Obtain a binary image of water meter unit *binImg*
 14. **for** every degree **do**
 15. rotate *binImg* and call the vertical projection function
 16. record the maximum peak value *peak[i]* of each vertical projection histogram
 17. find the maximum value *maxPeak* among them;
 18. **end for**
 19. add the corresponding angle with the peak value *maxPeak* to the angle set
 20. calculate the number of directions
 21. take the median of each direction angle as the angle of the direction
 22. **if** only two direction
 23. rotate 90 degrees to get the other two angle
 24. **end if**
 25. **for** four angle **do**
 26. obtain a vertical projection of each angle corresponding to *binImg*
 27. the difference between the first peak and the third peak
 28. sort difference
 29. **end for**
 30. get two angles corresponding to the two smaller difference
 31. **for** two angles **do**
 32. vertical projection after rotating 90 degrees clockwise
 33. calculate the x-axis coordinate corresponding to the maximum peak value
 34. **end for**
 35. select the angle corresponding to the larger one as the final angle
 36. **return final angle**
-

The picture correction is to determine the position of the digital region. In this section, we use the new algorithm to obtain the rotation angle of the image, thereby correcting the image. The position of the digital region can be determined by determining the position of the measurement unit “M” in the correct picture. The intercepted digital region is shown in Fig. 6:

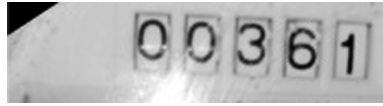


Fig. 6. Digital region.

3 Digital Region Processing and Digit Segmentation

After the digital region of the water meter is acquired, it needs to be processed into a binary image of a single character for easy identification. The acquired image of the multicolor digital region is not convenient for character segmentation, so the digital region image needs to be processed into binary images with as little noise as possible before segmentation. This section describes the methods of digital region image pre-processing and the segmentation of digital characters.

3.1 Digital Region Processing

For intercepted digital pictures. First, it is binarized [17]. When performing binarization, the binarization method of the fixed threshold is to set the pixel value larger than the threshold portion to 255 and the smaller than the threshold portion to 0, and the threshold value needs to be input by the user in advance. Since there is a light difference in the water meter image we obtained, it is obviously unreasonable to adopt a fixed threshold, so the adaptive threshold is used for binarization. In this paper, the digital region image is binarized by the adaptive threshold binarization function *adaptiveThreshold* of *opencv*. It is not to calculate the threshold of the global image, but to calculate the local threshold according to the brightness distribution of different regions of the image. Therefore, different thresholds can be adaptively calculated for different regions of the image, so it is called adaptive threshold method. How to determine the local threshold? The mean or weighted mean of a neighborhood can be calculated to determine the threshold. Weighted mean means that the pixels around (x, y) in the region are weighted according to the Gaussian function according to their distance from the center point. Obviously, the adaptive threshold is more consistent with the different illumination of the water meter image. The effect is shown in Fig. 7:

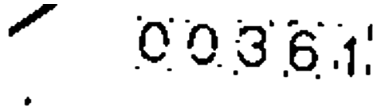


Fig. 7. Binary picture.

There will always be some noises in the binarized picture. The median filtering method is very effective in eliminating salt and pepper noise, some of the small particle noise is removed first by using median filtering [18]. We take a 3*3 matrix in the image which contains nine pixels, sort the nine pixels, and finally assign the median of the nine pixels to the center of the matrix. Traverse the entire image. After the previous processing, there may be a case where the numeric characters are not connected which will affect the subsequent processing. Therefore, we perform the morphological processing [11, 19] on them, and open calculation can connect the disconnected numbers. The effect is shown in the Fig. 9. In the picture of the water meter after binarization, the number of pixels in the digital is within a certain range. For some large noises, the connected domain is used to denoise. Combining the ratio of the digital pixel points in the circumscribed rectangle and the aspect ratio of the circumscribed rectangle can effectively remove noise. The following figure shows the denoising effect after the morphological processing is performed after the denoise is not performed.

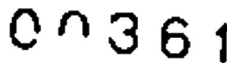


Fig. 8. No morphological treatment.

Figure 8 is a denoising effect diagram without morphological processing. Figure 9 is a denoising effect diagram after morphological processing. As we can see in Fig. 8, the number "0" is not connected; causing the lower half to be removed as noise, and Fig. 9 is connected by morphological processing.

3.2 Digit Character Segmentation

Digit character segmentation usually uses vertical projection segmentation, but some noise that is not completely removed may affect the segmentation effect. In this paper, a new method is adopted to select and intercept the digital regions through the connected domain circumscribing rectangle. In the later recognition, as long as it can determine whether it is a number, it can filter out the influence of the remaining noise and increase the accuracy of digit recognition. The digit segmentation effect is shown in the Fig. 10. In order to better display the segmentation effect, Fig. 10 changes the image background to black.

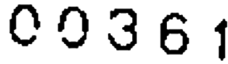


Fig. 9. Morphological treatment.

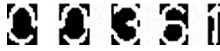


Fig. 10. Digit character segmentation.

4 Experimental Results and Analysis

The algorithm in this paper can correctly locate the digital region of the water meter and obtain a good digit character segmentation effect. Test the collected 100 images and part of the processing results as shown:

It can be seen from the results in the Fig. 11 that the algorithm proposed in this paper can effectively correct the water meter image and correctly locate the digital region. Due to the different printing styles of different water meter manufacturers, the unit “M” of the water meter is not horizontal alignment with the digital region in the water meter, so there will be cases where the actual digital region is on the upper or lower part of the intercepted picture, but this does not affect the subsequent split operation. For images that are tilted at a lesser horizontal angle, as shown in Fig. 11(d) it can also be correctly positioned. The algorithm in this paper is robust to horizontal tilt. In the denoising and segmentation process of the image, the segmenting operation has a good effect on the whole character, but the segmentation effect on the half character is not good, mainly because it is easy to remove the half-character part as noise in the denoising process. The experimental results are shown in Table 1.

The experimental results show that the proposed algorithm can effectively locate the digital region of the water meter image and can correctly split the numbers. For a few images with deviations in correction angle but little deviation, it is also possible to locate and segment the digital area. The algorithm of this paper is very robust to different printing fonts of different water meters, the difference in the light of the captured image, and rotation problems caused by shooting angles.

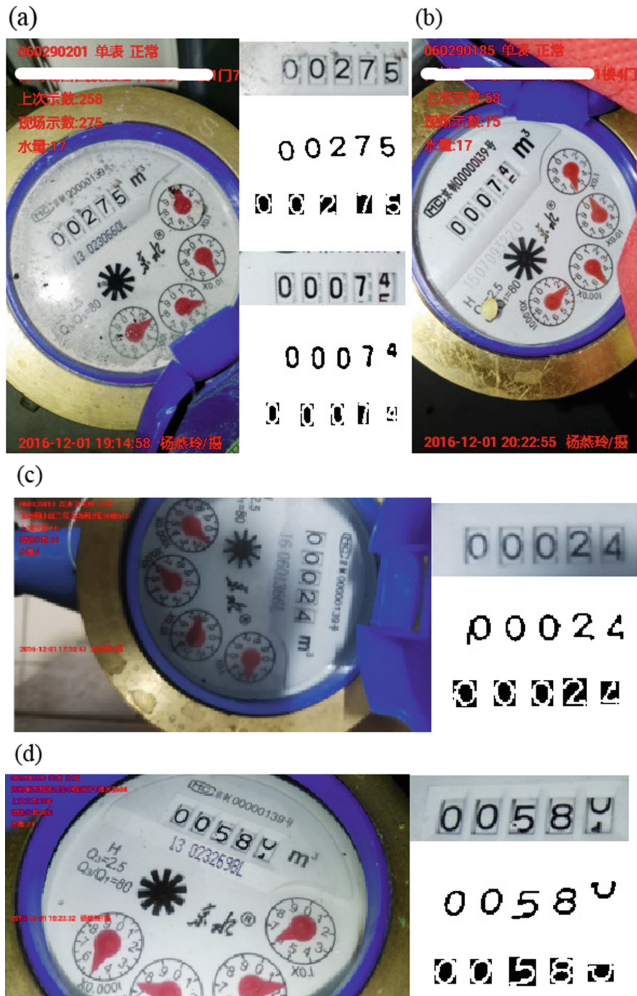


Fig. 11. Partial processing effect.

Table 1. Experimental result

Water meter image	Correct positioning	Correct segmentation	Accuracy %
100	92	89	89%

5 Conclusion

In this paper, the vertical projection feature of the measurement unit “M” on the water meter is used to effectively correct the water meter image, and then determine the position of the digital region on the water meter. It solves the rotation problem of the

water meter image caused by the non-fixed camera shooting. There is also some robustness to the tilt of the small angle of the picture. Denoising by morphological processing and connected-domain method, the interference of the noise is effectively removed while the complete number is retained to achieve the division of the digital characters.

References

1. Li, H., Zhang, L.Z., Tian, Y.: Performance, problems and application prospects of water meter copy in residential areas. *Ind. Des.* **2015**(9), 123 (2015)
2. Zhang, Z., Chen, G., Li, J., et al.: The research on digit recognition algorithm for automatic meter reading system. In: *Intelligent Control & Automation*. IEEE (2010)
3. Zhao, Y.A., Cui, H.: Multi-variable background target recognition based on SIFT algorithm. *Inf. Comput. (Theor. Ed.)* **2019**(01), 85–87 (2019)
4. Lei, B., Jing, Y., Ding, J.: Target localization based on SIFT algorithm. In: Zeng, D. (ed.) *ICAIC 2011, Part I. CCIS*, vol. 224, pp. 1–7. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23214-5_1
5. Narhare, A.D., Molke, G.V.: Trademark detection using SIFT features matching (2015)
6. Luo, B.J.: Binarization and its application in check recognition preprocessing. Southwestern University of Finance and Economics (2007)
7. Liu, X.H., Qian, K., Wang, Y.F., Zhu, X.X., Sun, Z.X.: Research on text recognition algorithm based on connected domain detection in natural scene. *Comput. Technol. Dev.* **25** (05), 41–45 (2015)
8. Gan, L., Lin, X.J.: License plate character segmentation algorithm based on connected domain extraction. *Comput. Simul.* **28**(04), 336–339 (2011)
9. Wang, J.X., Zhou, W.Z., Xue, J.F., et al.: The research and realization of vehicle license plate character segmentation and recognition technology. In: *2010 International Conference on Wavelet Analysis and Pattern Recognition*. IEEE (2010)
10. Liu, Y.L., Cui, L.Y., Shu, J.J., Xin, G.J.: License plate location method based on binary image jump and mathematical morphology. *Int. J. Digit. Content Technol. Appl.* **5**(5), 259–265 (2011)
11. Li, K., Dan, T.: Fast rotation and correction of image algorithm based on local feature. In: *2013 International Workshop on Microwave and Millimeter Wave Circuits and System Technology (MMWCST)*. IEEE (2013)
12. Lowe, D.G.: Distinctive image features from scale-invariant keypoints. *Int. J. Comput. Vis.* **60**(2), 91–110 (2004)
13. Wang, W.: The image correction algorithm based on combined transformation. In: Zhang, Y. (ed.) *Future Communication, Computing, Control and Management*. LNEE, vol. 141, pp. 73–81. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-27311-7_11
14. Li, L., Sang, H., Chang, Y.: Horizontal tilt correction for license plate image (2011)
15. Wang, L.Y., Yin, H.B., Wang, Q.: Application of SURF and RANSAC in image stitching. *Electron. Meas. Technol.* **39**(04), 71–75 (2016)
16. Ostu, N.: A threshold selection method from gray-histogram. *IEEE Trans. Syst. Man Cybern.* **9**(1), 62–66 (2007)
17. Niu, Z., Li, H.: Research and analysis of threshold segmentation algorithms in image processing. *J. Phys. Conf. Ser.* **1237**(2) (2019)

18. Yang, A.: Research on image filtering method to combine mathematics morphology with adaptive median filter. In: 9th International Conference on Optical Communications and Networks (ICOON 2010) (2010)
19. Herry, C.L., Goubran, R.A., Frize, M.: Segmentation of infrared images using cued morphological processing of edge maps. In: Instrumentation and Measurement Technology Conference Proceedings, IMTC 2007. IEEE (2007)



Fault Prediction for Software System in Industrial Internet: A Deep Learning Algorithm via Effective Dimension Reduction

Siqi Yang¹(✉), Shuaipeng Yang¹, Zigang Fang¹, Xiuzhi Yu²,
Lanlan Rui¹, and Yucheng Ma¹

¹ State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing, China
{yangsiqi, yangshuaipeng, 2018140769, llrui,
mayucheng}@bupt.edu.cn

² China Electronics Standardization Institute, Beijing, China
1006564282@qq.com

Abstract. In recent years, as information technology develops, Industrial Internet has become a hot issue in international industry. Because of the use of networked software in Industrial Internet, many machines are software-intensive. But software is a product of human brain thinking activities, with the increase of its scale and complexity, there will inevitably be some software defects caused by human errors in the process of design and development. Nowadays, software fault diagnosis mostly relies on personal experience and lacks effective technology and methods, which seriously affects the ability of software-intensive systems. This paper mainly designed a software system fault prediction model, which can be used by software-intensive system users of Industrial Internet to quickly predict whether software failures occur or not. Different fault prediction methods based on deep learning are introduced. We propose a software fault prediction model based on locally linear embedding (LLE) algorithm and long short-term memory (LSTM) algorithm to train the model. Original data sets are from MDP dataset of NASA. We process original datasets by using LLE algorithm to reduce dimensions of datasets. After processed datasets were trained by LSTM algorithm, the prediction model can be obtained. Compared with single LSTM and principal components analysis-long short-term memory algorithm (PCA-LSTM), the results show that locally linear embedding-long short-term memory algorithm (LLE-LSTM) algorithm has a better performance than other existing algorithms in terms of prediction accuracy, precision, recall, f-measure.

Keywords: Fault prediction · LSTM · LLE · Software

1 Introduction

In recent years, as information technology develops, Industrial Internet has become a hot issue in the international industry. Industrial Internet represents the integration of complex physical machine with networked sensors and software (see Fig. 1). In order

to realize real-time perception, dynamic control of large-scale industrial system, Cyber-Physical Systems (CPS) becomes core technology. CPS is a multi-dimensional complex system that integrates computing, network and physical environment, so machines are software-intensive. But software is a product of human brain thinking activities, with the increase of its scale and complexity, there will inevitably be some software defects caused by human errors. Nowadays, software fault diagnosis mostly relies on personal experience and still lacks effective technology and methods, which seriously affects the normal operation of software-intensive machines. Therefore, establishing a reasonable software fault prediction algorithm to complete the software fault prediction work economically and effectively is important.

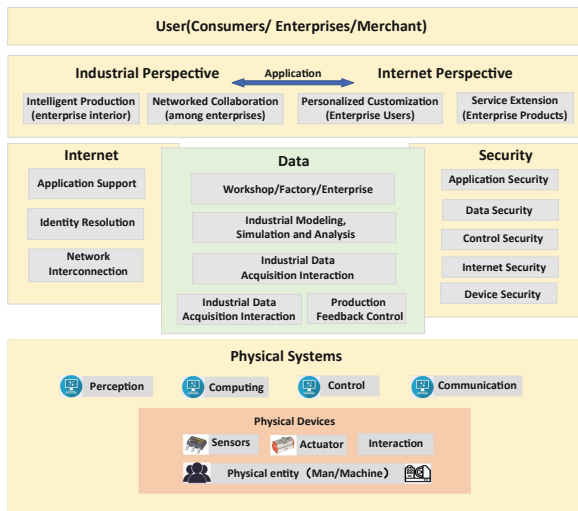


Fig. 1. Industrial Internet architecture

Many fault prediction methods are used in different areas. Wei H proposed a model using neighborhood preserving embedded support vector machine to predict software fault distribution [1]. Wei H proposed a LTSA-SVM algorithm to improve the prediction performance by reducing dimensions of datasets [2]. S. Zhang, Y. Wang, M. Liu and Z. Bao proposed a novel prediction algorithm which is based on LSTM and support vector machine [3]. Tong, HN, Liu, B, Wang, SH proposed SDAEsTSE, which is improved stacked denoising autoencoders (SDAEs) for software fault prediction [4]. C. Guo, Y. Wang and Y. Zhong presented an advanced algorithm based on BP neural network and particle swarm optimization algorithm to predict air conditioner fault [5]. And due to the complexity of software-intensive system, there will inevitably be some data redundancy. Dimension reduction algorithm is used to solve this problem. LLE is a non-linear dimension reduction algorithm [6], which can keep the original manifold structure of the dimension reduction data.

Based on the ideas above, we propose an algorithm based on LLE-LSTM. Our main contributions can be summarized as follows: (1) Locally linear embedding

algorithm is applied in the software fault prediction. Aiming at the problem of dimensional redundancy caused by the increasing attributes of software fault data sets. This paper applies LLE manifold learning algorithm and gives an approach for parameter selection. (2) Long short-term memory algorithm is applied in the software fault prediction. By designing forget gate, input gate and output gate, it can learn long-term dependent information. After processing dataset with LLE, training the dataset by LSTM algorithm, the prediction accuracy, precision, recall and F-measure are improved. (3) Selection of parameters of locally linear embedding algorithm. Different number of neighbors and dimensions have big impact on the final result of model. By comparing the prediction accuracy under different conditions, the parameters are selected.

2 Related Work

2.1 Locally Linear Embedding (LLE)

Local linear embedding is a dimension reduction method. Unlike other linear algorithms, LLE keeps the original manifold structure and maintains the characteristics of samples [7]. And the procedures are shown as follows.

Step 1: K-nearest neighbor algorithm is used to obtain k-nearest neighbor points for each data point. Suppose it is linear, each data point can be expressed by a linear combination of its k-nearest data points, i.e.

$$N_i = KNN(x_i, k), N_i = [x_{1i}, \dots, x_{ki}] \quad (1)$$

Step 2: Get weight coefficient matrix by minimizing the loss function.

$$\arg \min_W \sum_{i=1}^N \|x_i - \sum_{j=1}^k w_{ji} x_{ji}\|_2^2 \quad (2)$$

The notation w_i is a column vector; w_{ji} is the jth row of w_i ; x_{ji} is the jth adjacent point of x_i . This equation can get weight coefficient $w = [w_1, w_2, \dots, w_n]$. There are n data points, that is N column of w_i .

Step 3: LLE algorithm supposes that after reduction, the data set can still be expressed as a linear combination of its k-nearest neighbors, and the combination coefficient remains unchanged. Minimize the loss function again.

$$\arg \min_Y \sum_{i=1}^N \|y_i - \sum_{j=1}^k w_{ji} y_{ji}\|_2^2 \quad (3)$$

2.2 Long Short-Term Memory Algorithm

Long Short-term Memory Algorithm is an improved recurrent neural network (RNN). The nodes of recurrent neural network (RNN) are directionally connected into rings, the current output of a sequence is also related to the previous output [8]. RNN has 3 layers: input layer, hidden layer and output layer (see Fig. 2). Hidden layer will accept the data from the previous hidden layer. Therefore, RNN uses internal memory to process input sequences of arbitrary time series. However, RNN can only memorize part of the sequence and has limited access to contextual information, which results in the decrease of accuracy and vanishing gradient problem. Therefore, LSTM redesigns the memory module, adds input gate and output gate to adjust input data and state information of memory unit, adds the forget gate, clear the useless information, and effectively uses the long-distance sequence information (see Fig. 3).

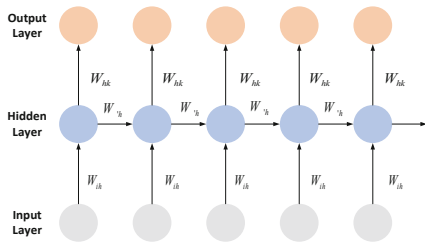


Fig. 2. Simple RNN architecture

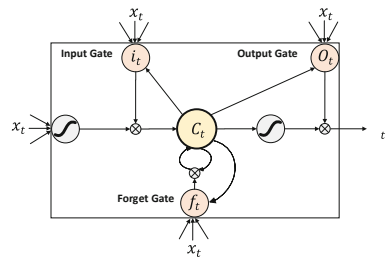


Fig. 3. LSTM memory module

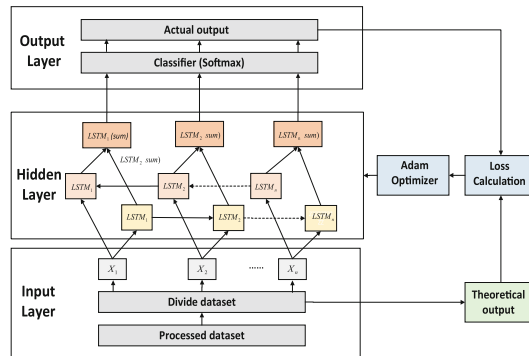


Fig. 4. Architecture of BiLSTM

Because the prediction needs to be decided by the previous input and the latter input together, we choose Bi-directional long short-term memory (BiLSTM) to improve performance. BiLSTM is composed of forward LSTM and backward LSTM [9]. BiLSTM takes into account both past features and future features. Backward process is equivalent to the reverse input of the original sequence into LSTM. BiLSTM

is like two LSTMs. One LSTM uses forward input sequence. The other one uses reverse input sequence. The final result combined the 2 outputs together. Finally, the final output is obtained by combining the output results of forward layer and backward layer at each time (see Fig. 4).

3 The Software Fault Prediction Model

3.1 Software Fault Prediction Model Based on LLE-LSTM

The LLE-LSTM software fault prediction model is designed (see Fig. 5).

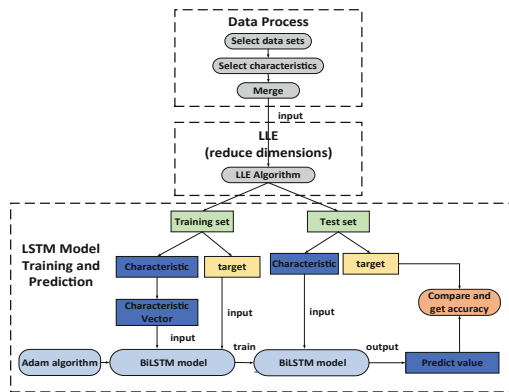


Fig. 5. The overview of software fault prediction model

- Step 1: Obtain and choose data sets.
- Step 2: Use LLE algorithm to process the data sets. LLE algorithm is used to reduce dimensions of the dataset.
- Step 3: Extract characteristics and generate characteristic vector of training set. Train LSTM model by using training set.
- Step 4: Put the characteristics of test dataset into trained LSTM model. Get the predict value.
- Step 5: Compare the target label and predict value to get accuracy.

3.2 Parameter Selection of LLE Algorithm

Because of the characteristics of LLE algorithm, the model needs to select the number of neighbors (k) and the number of embedding dimensions (d). Different value of combination will affect the final results. In this paper, accuracy is used to evaluate the predictive power of model. By generating accuracy with different number of neighbors and different number of dimensions, the optimized parameters can be selected. The optimized result only for the data set and algorithm used in this paper.

Selection of Number of Neighbors. In the process of using LLE algorithm, the impact of k is great. The larger the number of neighbors, the more time it takes to establish the local relationship of samples, but the better the local relationship is. But if the value of K is too large, the smoothness of the whole manifold may be affected and local characteristics cannot be embodied. But if the value is too small, it is difficult for LLE to maintain the topological structure of sample points. By generating datasets with different dimensions and different neighbors, get the relation of accuracy and k , d . According to Fig. 6, the optimized k value is 22.

Selection of Number of Dimensions. The number of dimensions determines whether the local topological structure on the embedded low-dimensional manifold can adequately describe the intrinsic law and essential characteristics of the original high-dimensional space by using LLE algorithm mapping, seek a reasonable and effective low-dimensional visual representation of the original high-dimensional space data by the lowest dimension output after dimensional reduction. If the minimum dimension d is too large, there will be too much noise in the dimension reduction results, and if the value of d is too small, different points may overlap in the low dimension space. According to Fig. 6, the optimized d value is $d = 12$.

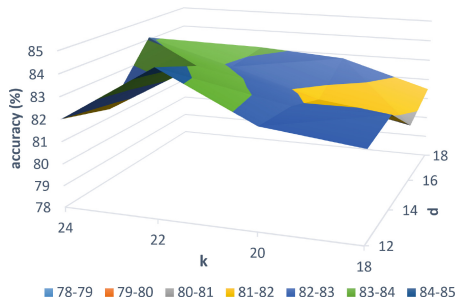


Fig. 6. The relation of accuracy and k , d

4 Results and Discussion

4.1 Selection of Datasets

MDP data sets are widely used in the area of software fault prediction. There are 13 different data sets. They are CM1, JM1, KC1, KC3, KC4, MC1, MC2, MW1, PC1, PC2, PC3, PC4, PC5 [10]. Different data sets have different attributes and fault ratio. Extract the common attributes and put the data sets together. The label of the raw data from NASA is N/Y. In order to train the dataset, we replace N with 0 and replaces Y with 1. Extract characteristics of each sub data set and integrate them.

4.2 Comparison of Different Algorithms

According to the selection of parameters, the optimized number of neighbors is 22 and the optimized number of dimensions is 12. Based on the 2 indexes, we implemented 4 algorithms: single LSTM, SMOTE-LSTM, PCA-LSTM and LLE-LSTM.

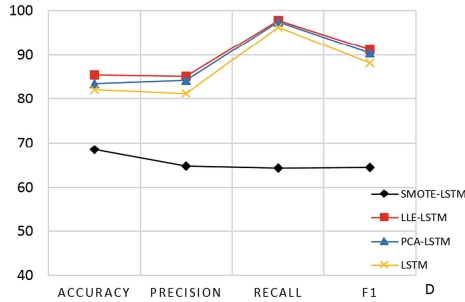


Fig. 7. Comparison of different algorithms

Compared with different algorithms, it shows 2 aspects (see Fig. 7). On one hand, SMOTE algorithm is not applicable in the MDP dataset because of its low accuracy. And the method which synthesis new samples using neighbor points is not applicable. On the other hand, the performance of using dimension reduction algorithm before training is better than that of single LSTM algorithm. Because there are redundant information and noise information in MDP dataset. Dimension reduction removes redundancy features and can solve overfitting problem of software fault dataset MDP.

Compare PCA-LSTM with LLE-LSTM from dimension 8 to 18 (see Figs. 8 and 9). It shows that both PCA-LSTM and LLE-LSTM can predict software faults effectively and improve the performance. The prediction result including accuracy, precision and F1 reaches the highest value when the dimension is 12. When the number of dimensions is between 8 and 18, compared with the single LSTM algorithm, the performance of PCA-LSTM and LLE-LSTM is better.

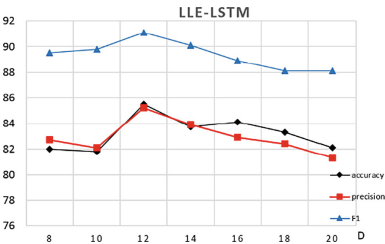


Fig. 8. Result of LLE-LSTM algorithm

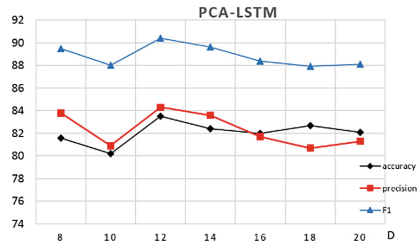


Fig. 9. Result of PCA-LSTM algorithm

Then, we compare PCA-LSTM and LLE-LSTM in terms of accuracy, precision and F1 (see Figs. 10, 11 and 12). The comparison of PCA-LSTM and LLE-LSTM shows that LLE-LSTM has a stable and better performance than traditional linear PCA-LSTM. LLE-LSTM preserves local linear relations in high dimensional space and improves the accuracy, precision and F1 in the prediction process.

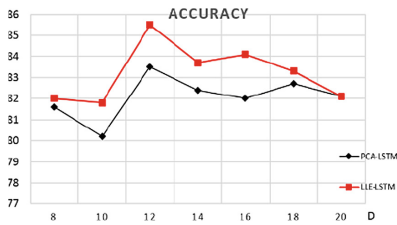


Fig. 10. Comparison of accuracy

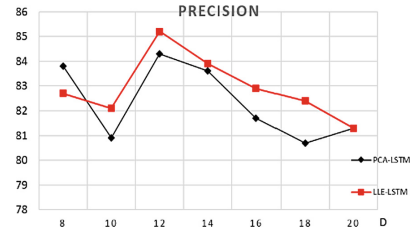


Fig. 11. Comparison of precision

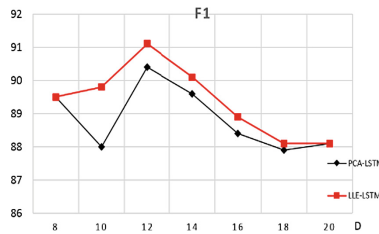


Fig. 12. Comparison of F1

5 Conclusion and Further Work

Fault prediction methods based on deep learning used in software fault prediction are remained to be designed and tested. We give a design of software fault prediction algorithm based on LLE and LSTM algorithm. Compared with the traditional LSTM algorithm, when the dimension varies from 10 to 18, LLE-LSTM algorithm performs better on prediction accuracy, precision, recall and F-measure. And manifold LLE-LSTM algorithm not only solves the data redundancy but also preserves local linear relations in high dimensional space. Some further research work remained to be done: (1) There are many advanced algorithms both in the dimension reduction and prediction. For example, LTSA is an advanced LLE. And the combination of different algorithms may lead to different results. (2) Use cross-validation. Cross-validation can ensure that all data have the opportunity to be trained and validated, make the performance of the optimized model more credible.

Acknowledgements. The work is supported by the Ministry of Industry and Information Technology project entitled “Industrial Internet Platform Standard Management Service Public Support Platform”.

References

1. Wei, H., Shan, C., Hu, C., Sun, H., Lei, M.: Software defect distribution prediction model based on NPE-SVM. *China Commun.* **15**(5), 173–182 (2018)
2. Wei, H., Hu, C., Chen, S.Y., Xue, Y., Zhang, Q.X.: Establishing a software defect prediction model via effective dimension reduction. *Inf. Sci.* **477**, 399–409 (2019)
3. Zhang, S., Wang, Y., Liu, M., Bao, Z.: Data-based line trip fault prediction in power systems using LSTM networks and SVM. *IEEE Access* **6**, 7675–7686 (2018)
4. Tong, H.N., Liu, B., Wang, S.H.: Software defect prediction using stacked denoising autoencoders and two-stage ensemble learning. *Inf. Softw. Technol.* **96**, 94–111 (2018)
5. Guo, C., Wang, Y., Zhong, Y.: Air-conditioning fault prediction about new energy bus based on particle swarm algorithm. *IAEAC* **10**, 211–215 (2017)
6. Lin, P., Chen, Y.M., Zou, Z.Y.: Quick discrimination of rice storage period based on manifold dimensionality reduction methods and near infrared spectroscopy techniques. *Spectrosc. Spectr. Anal.* **36**(10), 3169–3173 (2016)
7. Roweis, S.T., Saul, L.K.: Nonlinear dimensionality reduction by locally linear embedding. *Science* **290**(5500), 2323–2326 (2000)
8. Rather, A.M., Agarwal, A., Sastry, V.N.: Recurrent neural network and a hybrid model for prediction of stock returns. *Expert Syst. Appl.* **42**(6), 3234–3241 (2015)
9. Graves, A., Schmidhuber, J.: Framewise phoneme classification with bidirectional LSTM and other neural network architectures. *Neural Netw.* **18**(5–6), 602–610 (2005)
10. Gray, D., Bowes, D., Davey, N., Sun, Y., Christianson, B.: Reflections on the NASA MDP data sets. *IET Softw.* **6**(6), 549–558 (2012)



An Improved NSGA-II Algorithm and Its Application

Xiaofei Zhang, Zhiqiu Liu^(✉), Chao Wang, and Yalin Shang

School of Automation and Electrical Engineering,
University of Science and Technology Beijing, Beijing 100083, China
g20178606@xs.ustb.edu.cn

Abstract. The NSGA-II algorithm is widely used in multi-objective optimization problems, but the traditional NSGA-II algorithm has some shortcomings such as large computational cost and poor convergence in some complex practical problems. To solve above deflections, an improved NSGA-II algorithm is proposed in this paper. Firstly, the specific crossover and mutation operators are designed. Secondly, a novel elitist strategy is developed as well. Then, the simulations of the standard test functions are carried out, the results illustrate that the improved strategies can effectively enhance the convergence and operation speed of the traditional algorithm. Finally, in order to test the practicality of the algorithm, a multi-objective mathematical model for charge plan of steelmaking is established. Simulation is carried out with real industry data. The results show that the algorithm is practical for charge scheduling.

Keywords: Multi-objective optimization · NSGA-II · Crossover operator · Mutation operator · Charge plan

1 Introduction

Compared to single-objective optimization, multi-objective optimization needs to consider multiple goals simultaneously, which are often contradictory, in addition, the number of solutions is usually more than one, but a set of Pareto optimal solutions composed of multiple non-dominated solutions [1]. Traditionally, the multi-objective problems are mostly solved by a weighted method into a single objective problem. However, there are some limitations in this method, one of disadvantages is that the weight assigned to objective needs the expert background, which is infeasible in many circumstances, another is that only one optimal solution can be obtained in each run. Therefore, the conventional method cannot satisfy the actual needs very well.

In 1994, the non-dominated sorting genetic algorithm (NSGA) proposed by Srinivas and Deb [2] is widely used to solve multi-objective problems [3], which can provide more than one acceptable solution in every run for users to make choices according to their preferences. However, it has some shortcomings, such as high computational complexity, need to set the sharing radius manually, lack of elite protection strategy, etc. In 2002, Deb put forward an improved NSGA-II algorithm [4], using fast non-dominated sorting method to reduce computational complexity,

introduce crowding distance and elitist strategy, it has become one of the most mainstream methods for solving multi-objective problems [5–7].

However, the NSGA-II algorithm has the defections of high computational cost and poor convergence in solving complex nonlinear multi-objective optimization problems. In order to improve above problems, a developed NSGA-II is proposed in this paper. Firstly, the crossover operator is revised to refine the convergence of the algorithm. Secondly, an adaptive differential mutation operator is introduced to enhance the global search ability. Finally, simplify the elitist strategy to accelerate the operation speed.

In order to verify the effectiveness of the proposed strategy, the Generational Distance (GD), Diversity Metric (Δ), and running time are used as indices to compare the performance of the test functions with other algorithms. In the end, a multi-objective mathematical model for charge plan of steelmaking is established, and the proposed algorithm is applied to solve the problem.

2 Improved NSGA-II Algorithm

Aiming at the convergence and operation speed of the original NSGA-II, the following improvements are made in this paper.

2.1 Mixed Crossover Operator

Most of the multi-objective optimization problems use the Simulated Binary Crossover (SBX) suggested by Deb [8] at present. The literature [9] proposed a Normal Distribution Crossover (NDX) based on Gaussian distribution, the NDX operator has a wider search space, it is easier to jump out of the local optimal solution than SBX. These two crossover operators are combined in this paper, in the early stage of the evolution, the location of the optimal solution is unknown, applying the NDX operator to enlarge the search space. At the late stage of iteration, the whole population has tended to be stable, most of the individuals are around the optimal Pareto solution, it is necessary to narrow the search space, SBX crossover operator is used to accelerate the convergence of the algorithm. The formula for the parent individual $x_{1,i}$ and $x_{2,i}$ to generate the child individual $c_{1,i}$ and $c_{2,i}$ is:

$$c_{1,i} = \begin{cases} [(x_{1,i} + x_{2,i}) + 1.481(x_{1,i} - x_{2,i})N]/2 & \text{if } (g \leq G/2) \text{ and } u \leq 0.5 \\ [(x_{1,i} + x_{2,i}) + \beta(x_{1,i} - x_{2,i})]/2 & \text{if } (g > G/2) \text{ and } u \leq 0.5 \end{cases} \quad (1)$$

$$c_{2,i} = \begin{cases} [(x_{1,i} + x_{2,i}) + 1.481(x_{2,i} - x_{1,i})N]/2 & \text{if } (g \leq G/2) \text{ and } u > 0.5 \\ [(x_{1,i} + x_{2,i}) + \beta(x_{2,i} - x_{1,i})]/2 & \text{if } (g > G/2) \text{ and } u > 0.5 \end{cases} \quad (2)$$

where u is the random number generated by uniform distribution on the interval (0,1), N is the value of the random variable of (0,1) Gauss distribution, g is the current evolutionary generations, G is the maximum evolutionary generations, β is a random variable as exhibited below:

$$\beta = \begin{cases} (2u)^{\frac{1}{\eta+1}}, & u \leq 0.5 \\ (2(1-u))^{-\frac{1}{\eta+1}}, & u > 0.5 \end{cases} \quad (3)$$

where η is a constant cross-parameter which set by users.

2.2 Adaptive Differential Mutation Operator

Differential evolution [10] is a random search algorithm based on population evolution. It has good performance in global optimization for using the optimal vector solution in the group for information sharing. In order to enhance the global search ability of the original algorithm, the adaptive mutation operator is designed to replace the polynomial mutation operator. The main idea is enlarging the search step by increasing the value of scaling factor F in the early stage, reduce the value of F to improve the local search ability and accelerate the convergence speed when evolution is coming to an end. The adaptive differential mutation operator expression is:

$$v_i = (1 - q) \cdot x_{best} + q \cdot x + F \cdot (x_{r_2} - x_{r_1}), i = 1, 2, \dots, NP \quad (4)$$

where v_i is the individual after mutation, x_{best} is the best individual at present, x is the individual which needs mutation at present, x_1, x_2 is the two individuals selected randomly from the population size NP , q and F as exhibited below:

$$q = \frac{(G - g)}{G} \quad (5)$$

$$F = \frac{(F_{max} - F_{min})(G - g)}{G} + F_{min} \quad (6)$$

where G is the maximum evolutionary generations and g is the current evolutionary generations.

2.3 Improved Elitist Strategy

The elitist strategy of the original NSGA-II needs to merge the parent and the offspring populations to perform non-dominated sorting again, and select NP individuals to enter the next generation. It is meaningless to calculate the domination level and crowding distance of the abandoned part in the original strategy, furthermore the calculation time will increase when the number of populations is large. To the point, a simplified elitist strategy is developed, when N individuals are selected, the domination level and crowding distance of remaining individuals will not be calculated, as shown in the Fig. 1.

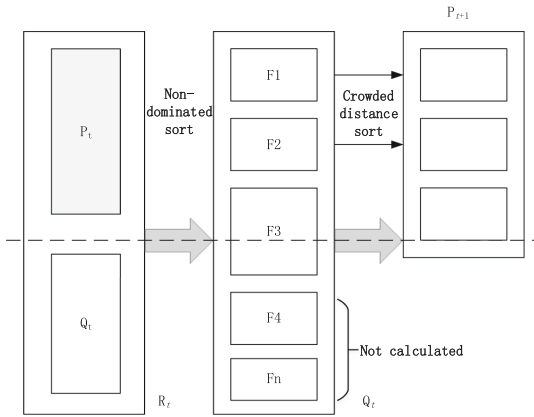


Fig. 1. Improved elitist strategy

2.4 Process of the Improved Algorithm

The steps of improved NSGA-II are as follows:

Step 1: Randomly generates the population P_t with the number of N by real number encoding. Perform non-dominated sorting and calculate the crowding distance on the population.

Step 2: Using binary tournament selecting method to select $N/2$ individuals for crossover and mutation operation, generate the offspring Q_t .

Step 3: Merge P_t and Q_t to get new population R_t , and perform non-dominated sorting on R_t . When the total number of individuals in the first n ranks generated is larger than N , stop calculating the dominance level of the remaining individuals, and use the crowding degree ranking for the first n ranks. Select the best N individuals as P_{t+1} .

Step 4: Selection, crossover and mutation on population P_{t+1} to generate population Q_{t+1} .

Step 5: Stop the loop if the termination condition is met, otherwise, go to Step 2.

2.5 Performance Indices

Convergence and distribution uniformity are two important indices for evaluating multi-objective optimization algorithms. This paper uses the following two indices to evaluate the algorithm.

Convergence. The Generational Distance (GD) [4] is used to reflect the proximity of the non-inferior solutions to the real optimal frontier. The calculation formula is as follows:

$$GD = \frac{\sqrt{\sum_{i=1}^{|Q|} d_i^2}}{|Q|} \tag{7}$$

where Q is the set of the obtained solutions, d_i is the minimum Euclidean distance between the individual i which is the nearest member of the Pareto optimal solution set. The smaller the GD value is, the closer the solution is to the true optimal frontier.

Distribution Diversity. BANOS [11] proposed a diversity index (Diversity Metric, Δ) to evaluate the solution distribution uniformity. The calculation formula is as follows:

$$\Delta = \frac{d_f + d_l + \sum_{i=1}^{N-1} |d_i - \bar{d}|}{d_f + d_l + (n - 1)\bar{d}} \tag{8}$$

where d_f and d_l are the Euclidean distance between the boundary point of the obtained set of non-inferior solutions and the Pareto optimal frontier, d_i is the Euclidean distance between point i and point $i + 1$ in the set of non-inferior solutions, \bar{d} is the average value of d_i . The smaller the Δ value is, the better the distribution uniformity of the optimal solution set is.

2.6 Algorithm Testing

We choose the multi-objective optimization test functions of ZTD1-ZTD4 [12] in Table 1 to test the proposed algorithm.

Table 1. Test problems

Test functions	Expressions
ZDT1	$\begin{cases} f_1(x_1) = x_1 \\ f_2(x) = g(1 - \sqrt{f_1/g}) \\ g(x) = 1 + 9 \sum_{i=2}^m x_i / (m - 1) \\ \text{s.t. } 0 \leq x_i \leq 1, \quad i = 1, 2, \dots, 30 \end{cases}$
ZDT2	$\begin{cases} f_1(x_1) = x_1 \\ f_2(x) = g(1 - (f_1/g)^2) \\ g(x) = 1 + \sum_{i=2}^m x_i / (m - 1) \\ \text{s.t. } 0 \leq x_i \leq 1, \quad i = 1, 2, \dots, 30 \end{cases}$
ZDT3	$\begin{cases} f_1(x_1) = x_1 \\ f_2(x) = g(1 - \sqrt{f_1/g} - (f_1/g) \sin(10\pi f)) \\ g(x) = 1 + 9 \sum_{i=2}^m x_i / (m - 1) \\ \text{s.t. } 0 \leq x_i \leq 1, \quad i = 1, 2, \dots, 30 \end{cases}$
ZDT4	$\begin{cases} f_1(x_1) = x_1 \\ f_2(x) = g(1 - \sqrt{f_1/g}) \\ g(x) = 1 + 10(n - 1) + \sum_{i=2}^n (x_i^2 - 10\cos(4\pi x_i)) \\ \text{s.t. } -5 \leq x_i \leq 5, \quad i = 1, 2, \dots, 10 \end{cases}$

The algorithm is programmed by MATLAB, and runs on 1.8 GHz CPU, 4 GB memory and Windows10 system. The parameters in both algorithms are set to be: the population size is 200; the generation is 500; the crossover probability is 0.8; the mutation probability is 0.1. Each test function runs 20 times to get the average value.

Comparison of Crossover and Mutation Operators. In order to compare the effect of different improved strategies on the traditional NSGA-II, only the crossover and mutation operators have been changed in the simulations, and other settings are the same as the traditional NSGA-II. Table 2 presents the GD and Δ value comparison between the two proposed strategies and the traditional NSGA-II.

Table 2. Comparison of improved strategies

Test functions	Algorithms	GD	Δ
ZDT1	Traditional NSGA-II	0.0026	0.3633
	NSGA-II with mixed crossover	0.0027	0.3251
	NSGA-II with DE mutation	0.0025	0.3755
ZDT2	Traditional NSGA-II	0.0026	0.3812
	NSGA-II with mixed crossover	0.0026	0.3534
	NSGA-II with DE mutation	0.0024	0.3344
ZDT3	Traditional NSGA-II	0.0050	0.5634
	NSGA-II with mixed crossover	0.0050	0.5733
	NSGA-II with DE mutation	0.0049	0.5525
ZDT4	Traditional NSGA-II	0.0378	0.6256
	NSGA-II with mixed crossover	0.0350	0.5733
	NSGA-II with DE mutation	0.0339	0.7974

It can be seen from Table 2 that the two proposed operators can effectively enhance the convergence and distribution performance of traditional NSGA-II. The DE mutation operator has a greater effect on improving convergence than mixed crossover operator, which means that the DE mutation operator can greatly expand the global search ability of the algorithm to search the optimal solutions. In addition, the mixed crossover operator has the best performance on distribution of ZDT1 and ZDT4.

Comparison of Elitist Strategy. Table 3 presents the comparison of the running time between the improved elitist strategy and the traditional algorithm.

Table 3. Comparison of running time

Test functions	Algorithms	T/s
ZDT1	Traditional NSGA-II	21.157
	NSGA-II with improved elitist	17.284
ZDT2	Traditional NSGA-II	20.334
	NSGA-II with improved elitist	16.978
ZDT3	Traditional NSGA-II	52.642
	NSGA-II with improved elitist	46.732
ZDT4	Traditional NSGA-II	30.980
	NSGA-II with improved elitist	18.702

It can be seen from Table 3 that the novel elitism strategy is faster than the original strategy. Compared with NSGA-II, the average operation time of the improved NSGA-II is reduced by 18.3% on ZDT1, 16.5% on ZDT2, 11.2% on ZDT3 and 39.6% on ZDT4. Therefore, the proposed elitist strategy can effectively speed up the running time by reducing unnecessary calculations.

Comparison of Other Algorithms. Traditional NSGA-II and MOPSO [13] are used to compare with the improved NSGA-II. The Pareto optimal fronts we get by using above algorithms are listed in Figs. 2, 3, 4 and 5.

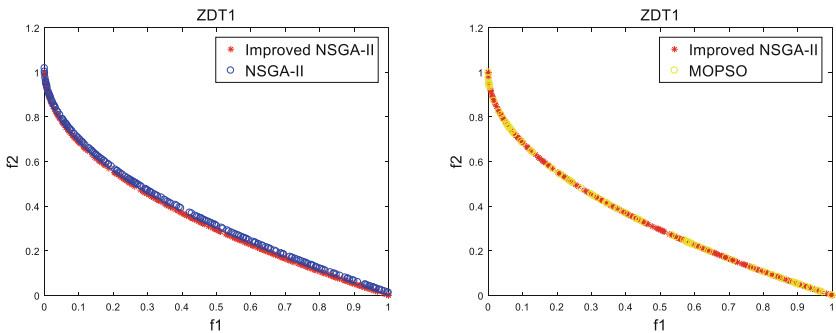


Fig. 2. The Pareto solutions of ZDT1

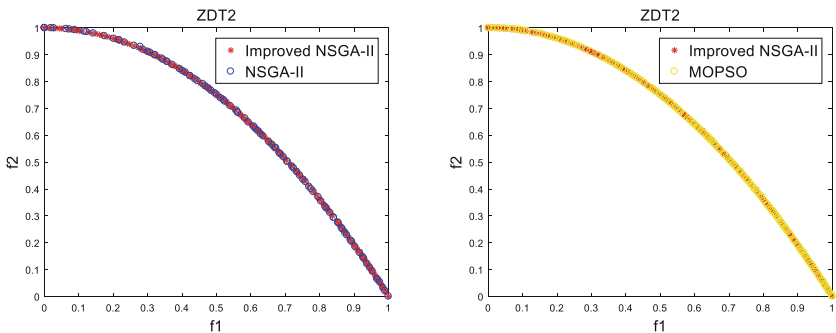


Fig. 3. The Pareto solutions of ZDT2

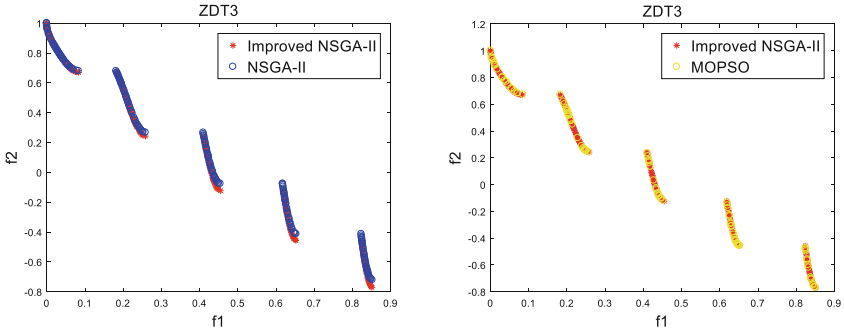


Fig. 4. The Pareto solutions of ZDT3

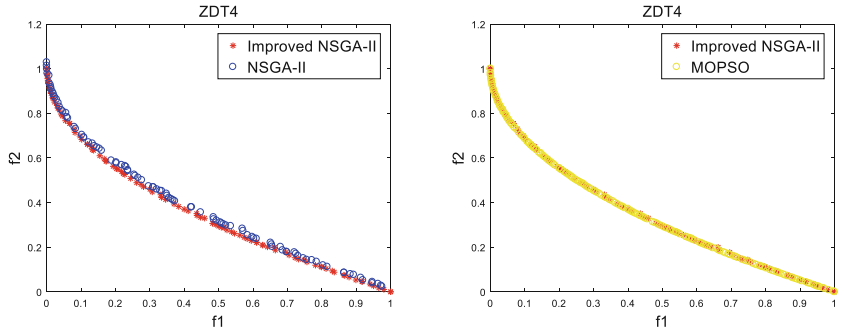


Fig. 5. The Pareto solutions of ZDT4

It can be seen from Figs. 2, 3, 4 and 5 that NSGA-II has a better performance on diversity and distribution in solving four test functions. The Pareto solutions obtained by NSGA-II and MOPSO are very uneven, especially in ZDT1 and ZDT4. The convergence of the solutions obtained by MOPSO is almost the same as that of improved NSGA-II, but NSGA-II has poor convergence in ZDT1 and ZDT4. In order to quantify the comparison results, Table 4 presents three indices obtained by these three algorithms in test functions.

Table 4. Comparison of test results

Test functions	Algorithms	GD	Δ	T/s
ZDT1	MOPSO	0.0031	0.4289	25.524
	NSGA-II	0.0026	0.3633	21.157
	Improved NSGA-II	0.0025	0.3346	17.284
ZDT2	MOPSO	0.0024	0.3167	31.528
	NSGA-II	0.0026	0.3812	20.334
	Improved NSGA-II	0.0023	0.3304	16.978
ZDT3	MOPSO	0.0042	0.5996	68.527
	NSGA-II	0.0050	0.5634	52.642
	Improved NSGA-II	0.0037	0.5397	46.732
ZDT4	MOPSO	0.0167	0.3308	42.672
	NSGA-II	0.0378	0.6256	30.980
	Improved NSGA-II	0.0301	0.4835	18.702

As can be seen from Table 4 that the improved NSGA-II has a better performance in GD and Δ on ZDT1 and ZDT3 than the other algorithms, and improved NSGA-II is the fastest of all comparison algorithms. Although the GD and Δ on ZDT4 is slightly inferior to MOPSO, it is better than NSGA-II. Compared with NSGA-II, the improved NSGA-II algorithm has a 15.4% decrease in GD index, a 12.1% decrease in Δ index and a 21.4% decrease in running time in all test functions. Therefore, the test results demonstrate the superiority of the improved strategy.

3 The Application of NSGA-II

3.1 Model of Charge Planning

Problem Description. The main task of steelmaking is to convert the molten steel from the ironmaking plant into molten iron. The charge is the basic unit of smelting a furnace steel [14]. The size of the furnace determines the weight of each heat, generally in tens to hundreds of tons. An effective charge plan can increase production efficiency, reduce the cost of steel companies, and maximize production capacity. Charge plan is a typical Multiple Knapsack Problem (MKP) [15], as shown in Fig. 4. Different orders differ in steel grades, specifications and delivery dates, only combine these orders with the same or similar indicators can meet the demands of mass production in steel industry (Fig. 6).

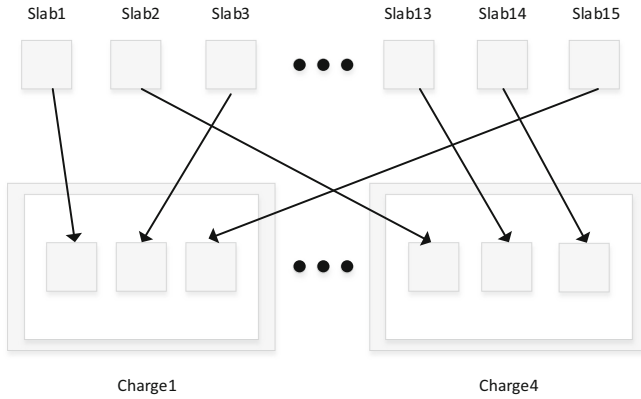


Fig. 6. Equivalent diagram of furnace scheduling

The following goals should be met:

- The difference in steel grade and width in the same charge is the smallest.
- Each slab is assigned to a single charge.
- The total number of charges is the smallest.
- Minimize Non-commissioned materials [16].

Constraints for charge planning:

- Slabs have the same steel grade.
- The thickness and width of the slab are the same.
- The total mass of the slab shall not exceed the maximum production capacity of the steelmaking furnace and not less than 80% of the furnace capacity
- The delivery dates are similar

Model Establishment for Charge Plan. Assuming that the weight of a single slab is less than the furnace capacity, the furnace capacity is constant, the number of slabs to be planned is N , and it is arranged to be produced in m charges. The multi-objective mathematical model of the charge plan is as follows:

Minimize slab steel grade differences in all charges:

$$\text{Min } F_1 = \sum_{j=1}^m \sum_{i=1}^N C_{ij}^1 X_{ij} \tag{9}$$

Minimize slab width differences in all charges:

$$\text{Min } F_2 = \sum_{j=1}^m \sum_{i=1}^N C_{ij}^2 X_{ij} \tag{10}$$

Minimize total remaining capacity:

$$\text{Min } F_3 = mU - \sum_{j=1}^m S_j \tag{11}$$

Subject to:

$$\sum_{j=1}^m X_{ij} = 1, \quad i \in \{1, 2, \dots, N\} \tag{12}$$

$$S_j = \sum_{i=1}^N W_i X_{ij} \leq U, \quad j \in \{1, 2, \dots, m\} \tag{13}$$

$$X_{ij} \in \{0, 1\} \quad i = 1, \dots, N \quad j = 1, \dots, N \tag{14}$$

Where:

$$C_{ij}^1 = \begin{cases} +\infty & \text{Steel grade of slab } i \text{ and furnace } j \text{ is different} \\ K_1 |ST_i - ST_{maxj}| & \text{others} \end{cases} \tag{15}$$

$$C_{ij}^2 = \begin{cases} +\infty & |WD_i - WD_{maxj}| > 100 \\ K_2 |WD_i - WD_{maxj}| & \text{others} \end{cases} \tag{16}$$

The parameters in the above formulas are expressed as follows:

- U Upper limit of furnace capacity;
- W_i Weight of i^{th} Slab;
- S_i Total weight of slab in the i^{th} charge;
- ST_i Steel grade of the i^{th} slab;
- WD_i Width of the i^{th} slab;
- C_{ij}^1 i^{th} slab merged into the j^{th} charge steel grade cost factor;
- C_{ij}^2 i^{th} slab merged into the j^{th} charge steel width cost factor;
- K_1 Steel grade difference penalty coefficient;
- K_2 Width difference penalty coefficient;
- ST_{maxj} The highest steel grade quantitative index of slab in the j^{th} charge;
- WD_{maxj} The max width of slab in the j^{th} charge;
- $X_{ij} = \begin{cases} 1 & \text{merge } i^{th} \text{ slab into } j^{th} \text{ charge} \\ 0 & \text{others} \end{cases}$

Constraint (4) means that each slab can be uniquely grouped into the charge plan; Constraint (6) means that the total slab weight of each charge cannot exceed the maximum furnace capacity; Constraint (7) is the decision variable range of values.

3.2 Case Analysis

The actual production data of a steel company in the literature [17] is used to test the practicality of improved NSGA-II. Randomly select 15 slab orders, and the parameters are set as follows.

The furnace capacity is 100 ton; the penalty coefficients K_1 and K_2 are 20 ¥/t, 10 ¥/m² × t, respectively; the population size is set to 50; the generation is 200; the crossover probability is 80%; the mutation probability is 0.1%.

In the MATLAB 2016 environment, running 200 generations. One of the running results as follows.

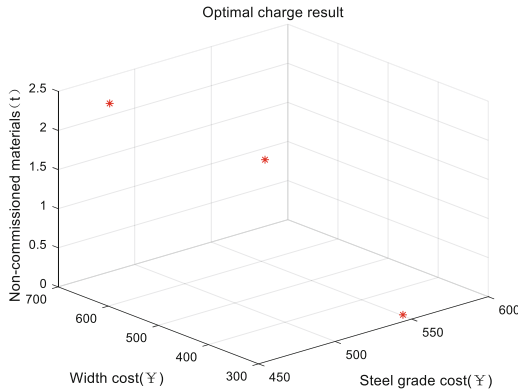


Fig. 7. Spatial distribution map of optimal solution

From the Fig. 7, it can be seen that three solutions are obtained in one run which have a good distribution in the function space. In order to illustrate the difference between the solutions clearly, Table 4 presents the cost of each plans under different goals. The obtained plans are presented in Table 5.

Table 5. Cost of each scheme

Schemes	Steel grade cost (¥)	Width cost (¥)	Non-commissioned materials (ton)
1	457.49	620.00	2.50
2	460.78	320.00	2.50
3	550.84	320.00	0

Table 6. Result of charge scheduling

Schemes	Charge 1	Charge 2	Charge 3	Charge 4
1	(9,10,11)	(1,7,12,14)	(5,8,13,15)	(2,3,4,6)
2	(2,5,6,7)	(9,10,11)	(1,3,4,12)	(13,14,15)
3	(2,9,13)	(4,8,11,12)	(3,10,14,15)	(1,5,6,13)

It can be seen from Table 4 that the values of the individual objective functions of a scheme fluctuate within a certain range. The results demonstrate the plans obtained by improved NSGA-II have diversity and practicality. Decision makers can select the most suitable scheme from Table 5 according to actual situations.

At the end of the experiment, the traditional NSGA-II is used to solve the model, although the results are the same as the improved NSGA-II, the main difference is in the running speed. Table 6 presents the average running time after ten runs with NSGA-II and NSGA respectively.

Table 7. Comparison of running time

Algorithm	T/s
Improved NSGA-II	13.42
NSGA-II	18.72

It can be seen from Table 6 that improved NSGA-II reduces operation time by 28%. Therefore, the improved algorithm can effectively enhance the efficiency of charge planning (Table 7).

4 Conclusions

In this paper, the improvement on the original NSGA-II is illustrated in details, by introducing the developed mix crossover operator and an adaptive DE mutation operator enlarges the search range of the original algorithm, the experimental results prove that the improved NSGA-II is better than original NSGA-II in distribution uniformity and convergence of population, and the novel elitist strategy is helpful to enhance the speed of operation. Therefore, this proposed algorithm has certain superiority by comparison with original algorithm.

In the end, the simulation results of charge plan are diverse and satisfy the actual situation, demonstrate the practicability of the improved NSGA-II.

References

1. Chen, G.: Multi-objective optimization method based on agent model and its application in vehicle body design. Hunan University (2012)
2. Srinivas, N., Deb, K.: Multiobjective Optimization Using Nondominated Sorting in Genetic Algorithms. MIT Press, Cambridge (1994)
3. Alikar, N., Mousavi, S., Ghazilla, R., et al.: Application of the NSGA-II algorithm to a multi-period inventory-redundancy allocation problem in a series-parallel system. *Reliab. Eng. Syst. Saf.* **160**, 1–10 (2017)
4. Deb, K., Pratap, A., Agarwal, S., et al.: A fast and elitist multiobjective genetic algorithm. *IEEE Trans. Evol. Comput.* **6**(2), 0–197 (2002)

5. Mason, S.J., Kurz, M.E., Pfund, M.E., et al.: Multi-objective semiconductor manufacturing scheduling: a random keys implementation of NSGA-II. In: IEEE Symposium on Computational Intelligence in Scheduling. IEEE (2007)
6. Ma, E.J., Chai, T.Y., Bai, R.: The optimization methods based on non-dominated sorting genetic algorithm for scheduling of material flow in mineral process. In: IMACS Multiconference on Computational Engineering in Systems Applications. IEEE (2006)
7. Chen, X., Zhao, L., Liang, H., et al.: Matching patients and healthcare service providers: a novel two-stage method based on knowledge rules and OWA-NSGA-II algorithm. *J. Comb. Optim.* (2017)
8. Deb, K., Goyal, M.: A combined genetic adaptive search (GeneAS) for engineering design. *Comput. Sci. Inform.* **26**(4), 30–45 (1996)
9. Zhang, M., Luo, W.J., Wang, X.F.: A normal distribution crossover for ϵ -MOEA: a normal distribution crossover for ϵ -MOEA. *J. Softw.* **20**(2), 305–314 (2009)
10. Storn, R., Price, K.V.: Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces. *J. Glob. Optim.* **11**(4), 341–359 (1997)
11. Veldhuizen, D.A., Lamont, G.B.: Evolutionary Computation and Convergence to a Pareto Front, pp. 221–228. Stanford University Bookstore (1998)
12. Zitzler, E., Deb, K., Thiele, L.: Comparison of multiobjective evolutionary algorithms: empirical results. *Evol. Comput.* **8**(2), 173–195 (2000)
13. Coello, C., Pulido, G.: Handling multiple objectives with particle swarm optimization. *IEEE Trans. Evol. Comput.* **8**(3), 256–279 (2004)
14. Hu, K.-Y., Gao, Z.-W., Wang, D.: Optimal multi-objective model and algorithm for order matching problems in iron & steel plants. *J. Northeast. Univ.* **25**(6), 527–530 (2004)
15. Yang, J., Wang, B., Zou, C., et al.: Optimal charge planning model of steelmaking based on multi-objective evolutionary algorithm. *Metals* **8**(7), 483 (2018)
16. Yu, S., Lv, R., Zheng, B., et al.: Simulation system for logistics in steelmaking process based on Flexsim. In: CCDC (2009)
17. Xue, Y., Zheng, D., Yang, Q.: Optimal furnace scheduling for steelmaking and continuous casting based on improved discrete particle swarm optimization. *Comput. Integr. Manuf. Syst.* **17**(07), 1509–1517 (2011)



Correction to: Wear Debris Classification and Quantity and Size Calculation Using Convolutional Neural Network

Hongbing Wang, Fei Yuan, Liyuan Gao, Rong Huang,
and Weishen Wang

Correction to:
Chapter “Wear Debris Classification and Quantity and Size Calculation Using Convolutional Neural Network”
in: H. Ning (Ed.): *Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health*, CCIS 1137,
https://doi.org/10.1007/978-981-15-1922-2_33

The original version of this chapter contained an error in Table 10. The values in the last three rows of the table have been modified. The table has now been corrected.

Table 10. R-FCN detection results compared with Faster RCNN

Detect model	<i>mAP</i>	Fatigue	Severe sliding	Cutting	Spherical	Copper	Test time (sec/img)
Faster RCNN+ ReNet50	0.7793	0.7920	0.8428	0.7734	0.6543	0.8338	0.391
Faster RCNN + ReNet101	0.7700	0.7677	0.8571	0.8465	0.5293	0.8496	0.180
Faster RCNN+ ReNet101+ FPN+ OHEM	0.8297	0.8426	0.8868	0.8844	0.6522	0.8823	0.179
R-FCN+ ReNet50 + FPN + OHEM	0.8319	0.7491	0.8512	0.8252	0.8555	0.8787	0.178

The updated version of this chapter can be found at
https://doi.org/10.1007/978-981-15-1922-2_33

Author Index

- Abdelrahman, Ra'ed Bani II-149
Abuassba, Adnan Omer I-349
Ahmed, Zahoor II-138
Al-Aqrabi, Hussain II-149, II-169
Ali, Hazrat I-349
Aslam, Muhammad Muzamil II-38, II-138
Azeem, Hassan II-38, II-138
Azeem, Muhammad I-175
- Batbayar, Delgerbat I-199
Bo, Wen I-249
Bulbul, Mohammad Farhad I-349
- Cao, Huimei II-407
Cao, Jian II-504
Cao, Shuai I-141, I-187
Cao, Yang I-141
Cao, Zongfu I-214
Chai, Yuke II-389
Chen, Haowei II-3
Chen, Liming II-205
Chen, Pan II-130
Chen, Reed II-328, II-345
Chen, Rongrong I-94, I-130
Chen, Shuhong I-94
Chen, Tianen I-357
Chen, Xianzhong I-284
Chen, Xinlei II-513
Chen, Xinli I-296
Chen, Xuehong I-547
Cheung, Jason Pui Yin II-431
Chow, K. P. I-3
- Dai, Fei II-92
Dai, Qinglong II-105
Dai, Wei I-413
Deng, Bangfei I-379
Diao, Jin I-487
Ding, Jinshun II-504
Ding, Lin I-161
Ding, Yi II-3
Dong, Guannan II-51
- Dou, Jinhua I-502
Du, Liping II-38, II-138
- Fang, Bin I-379
Fang, Weiqing II-504
Fang, Weiwei II-3
Fang, Zigang I-572
Farha, Fadi II-205
Fasko Jr., Michael II-328, II-345
Feng, Chen I-107
Feng, Shaobin II-452
Feng, Xialing II-241
- Gai, Keke I-335
Gao, Liyuan I-470
Gao, Yang I-321
Gaye, Babacar I-231
Geng, Yunxiao I-214
Guo, Bin II-272
Guo, Wenjie I-335
Guo, Wuwu I-119
Guo, Xi I-73
Guo, Xiaoyong II-431
Guo, Yu I-265
- Han, Yu I-265
Hao, Xuekun II-65
He, Jie I-141
He, Ye I-309
Helal, Sumi I-187
Hill, Richard II-149, II-169
Hu, Wen I-534
Hu, Yong II-431
Huang, FangLiang I-518
Huang, Qihe II-92
Huang, Rong I-470
Huang, Xingzhe I-38
Huangfu, Wei II-389
- Ikram, Muhammad II-38, II-138
- Jia, Hunfu I-187
Jia, Zhai I-107

- Jiang, Aiwen II-79
 Jiang, Yatong I-214
 Jiao, Yanbin II-121
 Jing, Yuhai I-534

 Karim, Feroz I-349

 Lane, Phil II-169
 Lei, Fei I-557
 Li, Changyun I-94
 Li, Guoyan II-65
 Li, Haihua I-296
 Li, Huan II-21
 Li, Hui II-65
 Li, Jiangyun I-284
 Li, Jiansheng II-407, II-542
 Li, Jianwu II-105
 Li, Jianyuan I-321
 Li, Jun I-547
 Li, Li I-296
 Li, Liangyan I-249
 Li, Qian II-130
 Li, Qingjuan II-205
 Li, Tian II-65
 Li, Tingting II-312
 Li, Weimin II-92
 Li, Xiang II-21
 Li, Xiaojun I-242
 Li, Xueni II-417
 Li, Ya I-518
 Li, Yang I-199
 Li, Zezhou II-228
 Li, Zhaotong I-403
 Li, Zhimin II-272
 Li, Zhuang II-441
 Lin, Hongyi I-357
 Lin, Junting I-433
 Lin, Wenmin II-92
 Liu, Caiyun I-547
 Liu, Fangfang I-56
 Liu, Jianwei I-214
 Liu, Jingyi I-296
 Liu, Meiliang I-199
 Liu, Mengran II-3
 Liu, Mengyi II-301
 Liu, Xia I-403
 Liu, Xiaoxiao II-105
 Liu, Xin I-141, I-187, I-335
 Liu, Yan I-357

 Liu, Yongqing II-121
 Liu, Zhiqiu I-581
 Lu, Siyuan II-216
 Lu, Yang I-518
 Lu, Zhihai II-216, II-360
 Luo, Xiong I-321, II-328, II-345
 Lv, Jinxin I-296

 Ma, Jia I-450
 Ma, Yucheng I-572, II-121
 Manning, Kyle II-466
 Mi, Zhenqiang I-265
 Miao, Xue I-73
 Mughal, Muhammad Arif II-38

 Nie, Li II-528
 Ning, Huansheng II-205, II-389, II-452,
 II-528

 Qi, Lianyong II-92
 Qian, Jide I-379
 Qian, Jin II-105
 Qian, Jiye I-379
 Qin, Hao II-121
 Qin, Jingyan II-441
 Qin, Shengzhi I-3
 Qureshi, Junaid Javed I-349

 Ran, Na I-20
 Ren, Pengcheng I-119
 Rui, Lanlan I-572, II-121

 Shang, Tao I-214
 Shang, Yalin I-581
 Shen, Mengyu I-199
 Shen, TongPing I-518
 Shen, Yan I-56
 Shen, YuLian I-518
 Shi, Zhiguo I-450, II-285, II-417, II-487
 Siegler, Dylan II-328, II-345
 Song, Shangxiu I-413
 Sun, Jincheng I-357
 Sun, Jingying II-285
 Sun, Rong I-413
 Sun, Yan I-547
 Sun, Yueqi II-272

 Tan, Min-Sheng I-161
 Tan, Tianran II-228, II-241
 Tian, Shu I-309

- Ullah, Ata I-175, II-38
- Wan, Ming II-301
- Wan, Yadong II-441
- Wang, Chao I-581
- Wang, Dongdong I-130
- Wang, Hong I-284
- Wang, Hongbing I-296, I-470
- Wang, Leiyu II-51
- Wang, Liang II-272
- Wang, Meng II-51
- Wang, Rui II-130, II-185
- Wang, Weiping I-321, II-105
- Wang, Weishen I-470
- Wang, XiuQing II-256
- Wang, Xueli I-141, I-557
- Wang, Ying I-335
- Wang, Yixin II-504
- Wang, Yizhong II-431
- Wang, Yunpeng II-3
- Wang, Zhaoshun I-73
- Wang, Zhu II-272
- Wei, Shuqi I-296
- Wen, Yueran I-413
- Wu, Di II-21
- Wu, Xinghao II-521
- Wu, Yuezhong I-94
- Wulamu, Aziguli I-73, I-231
- Xiao, Jiaojiao I-249
- Xiao, Wendong II-521
- Xie, Gangwen I-379
- Xin, Li I-107
- Xing, Yongli I-487
- Xiong, Zhimei I-557
- Xu, Dong I-242
- Xu, Hairui II-301
- Xu, Liang I-119, I-390, I-403
- Xu, Lingyu I-130
- Xu, Qian I-433
- Xu, Suxia II-431
- Xu, Tao I-413
- Xu, Xiaolong II-92
- Xue, Shengjun II-79
- Yan, Huiran II-185
- Yang, Chun II-487
- Yang, Hongju I-249
- Yang, Jie I-161
- Yang, Shuaifeng I-547
- Yang, Shuaipeng I-572
- Yang, ShunKun II-256
- Yang, Shunkun II-328, II-345, II-452, II-528
- Yang, Siqi I-572, II-121
- Yang, Yang I-265
- Yao, Xuanxia I-199
- Ye, Jihua II-79
- Ye, Xiaozhen II-528
- Yi, Dong I-107
- Yin, Changqing II-228, II-241
- Yin, Xu-Cheng I-309
- Yu, Jie I-130
- Yu, Lei I-518
- Yu, Wangyang II-466
- Yu, Xiuzhi I-572
- Yu, Zhiwen II-272
- Yu, Zhi-Xuan I-309
- Yuan, Fei I-470
- Yuan, Hongfei I-413
- Yuan, Jiangru I-119
- Yuan, Yizhe II-228, II-241
- Yue, Xinwei II-65
- Zeng, Xingjie I-119
- Zhai, Tongtong II-371
- Zhai, Xiaojun II-466
- Zhang, BenHong I-518
- Zhang, Changyou I-249
- Zhang, Haixia II-51
- Zhang, Jianlong II-21
- Zhang, Lei I-38
- Zhang, Peiying I-38
- Zhang, Ruicong I-119
- Zhang, Weishan I-38, I-119, I-141, I-187, I-390, I-403
- Zhang, Xiaofei I-581
- Zhang, Xiaotong II-441
- Zhang, Yuanjie I-390
- Zhao, Dongmei II-389, II-452
- Zhao, Dongming II-513
- Zhao, Hongwei I-403
- Zhao, Hui I-335
- Zhao, Jun I-413, II-105
- Zhao, Qi II-371
- Zhao, Wangqilin II-521
- Zhao, Wenbing I-321, II-328, II-345
- Zhao, Xin-dong I-413
- Zhao, Yile II-360
- Zhao, Yu II-205

Zheng, Jiaqi [I-487](#)

Zheng, Liang [I-141](#), [I-187](#)

Zheng, Zongchao [I-390](#)

Zhi, Ruicong [II-301](#), [II-312](#)

Zhong, Wei [II-513](#)

Zhong, Xiaowei [II-550](#)

Zhou, Caixia [II-312](#)

Zhou, Jiehan [I-119](#), [I-187](#), [I-390](#), [I-403](#)

Zhou, Xin [I-379](#)

Zhou, Zhangbing [I-487](#)

Zhu, Chao [I-309](#)

Zhu, Tao [II-205](#)

Zhu, Zhixin [II-542](#)

Zong, Haoyu [I-413](#)