Journal of Real-Time Image Processing (2019) 16:559–563
https://doi.org/10.1007/s11554-019-00881-y

GUEST EDITORIAL

Special issue on real-time image watermarking and forensics in cloud computing

Chuan Qin[1] · Zhenxing Qian[2] · Guorui Feng[3] · Xinpeng Zhang[2]

Published online: 14 May 2019

1 Introduction

Nowadays, the transmission, storage and processing for multimedia data have been increasingly performed with ease due to the advancements of the technologies of Internet and cloud computing. The fact that multimedia data, especially digital images, can be easily copied, modified or tampered has led to the development of watermarking and forensics image processing techniques. Considering that the ownership and copyright of digital images may be impinged and confused due to such attacks, it is necessary to ensure that digital images which are received or downloaded are not faked. Hence, the techniques of image watermarking and forensics have been developed to overcome the deficiency of traditional cryptography for the scenario of image protection, which are becoming increasingly important and attracting the public attention.

There are still some notable disadvantages in current research methodologies for image watermarking and forensics, which are commonly based on the strict conditions that are not possible to satisfy for real-time applications. Furthermore, high computational complexity of current schemes makes it difficult to cope with big data in computer networks and cloud computing. These drawbacks limit the applications of image watermarking and forensics techniques in practice, and thus requiring in-depth investigations and studies.

This special issue aims to bring together the latest research works in the related areas of real-time image watermarking and forensics. It addresses novel and efficient techniques that have potential to be applied to cloud computing with privacy preserving. According to a rigorous review procedure, each manuscript submitted to the special issue was reviewed by at least three anonymous experts. Based on the reviews done, a total of 21 papers have been selected to be included in this special issue, which fall into the following five major categories: (1) watermarking and steganography (5 papers), (2) steganalysis (3 papers), (3) reversible data hiding (5 papers), (4) image forensics (3 papers), (5) image encryption (2 papers), and (6) other emerging techniques (3 papers). In what follows, an overview of these papers is provided.

2 Watermarking and steganography

The paper entitled "Dynamic Multi-watermarking and Detecting in DWT Domain", co-authored by Youcai Gao, Jinwei Wang, and Yun-Qing Shi, proposes an efficient, dynamic multi-watermarking scheme, which embeds different watermarks into DWT coefficients according to two secret keys. In this scheme, dynamic detectors, i.e., optimum and locally optimum, are derived from additive approximation and multiplicative approximation, respectively, and then the optimal Lagrange algorithm is applied to calculate embedding strength factors with the given PSNR for the strongest robustness. This scheme can be effectively used for the applications of copyright protection and traitor tracing.

The paper entitled "Exploiting Error Control in Matrix Coding-based Data Hiding over Lossy Channel" is

✉ Chuan Qin
qin@usst.edu.cn

Zhenxing Qian
zxqian@fudan.edu.cn

Guorui Feng
grfeng@shu.edu.cn

Xinpeng Zhang
zhangxinpeng@fudan.edu.cn

[1] School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China

[2] School of Computer Science, Fudan University, Shanghai 200433, China

[3] School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China

authored by Ching-Nung Yang, Yung-Shun Chou, Yanxiao Liu, and Cheonshik Kim. The authors focus on a steganographic scheme, i.e., the matrix coding-based data hiding (MCDH), which is constructed from covering function to enhance embedding efficiency. It is claimed that MCDH may be compromised under the condition of steganography over lossy channel, and one-bit error in MCDH may change to multi-bit errors during extraction of the embedded data. In their proposed scheme, the constant weight code is used to overcome error spreading problem, and the small lookup table is adopted to reduce the computational complexity for real-time application.

Besides embedding capacity and visual quality of stego image, computational complexity is also an important criterion to evaluate the performance of a data hiding scheme. As an effective technique, the turtle shell matrix is extensively used in data hiding, however, leading to lower computational efficiency. In the paper entitled "Fast Turtle Shell-based Data Embedding Mechanisms with Good Visual Quality", Ching-Chun Chang and Yanjun Liu propose two real-time data hiding schemes based on turtle shell matrix. In the first scheme, 3×3 squared associate sets, rather than irregular ones, are chosen to hide an 8-ary digit into a cover pixel pair. In the second scheme, each edge digit in the turtle shell matrix is added with eight, and 5×5 squared associate sets are then adopted to hide a 16-ary digit at a time. Experimental results show that the proposed schemes can effectively decrease computational complexity and achieve better visual quality of stego images than some reported schemes.

In another paper entitled "Efficient Halftone Image Steganography Based on Dispersion Degree Optimization", Yingjie Xue, Wanteng Liu, Wei Lu, Yuileong Yeung, Xianjin Liu, and Hongmei Liu present an efficient block-based steganographic method for halftone images, in which optimal dispersion degree is utilized to measure texture complexity. Image blocks consisting of complex texture are chosen as cover data based on dispersion degree, and the secret bits are hidden through flipping the pixels subject to minimizing the changes of textural structure. This scheme can achieve large embedding rate and good image quality with acceptable statistical security.

High-dynamic range (HDR) images have become more and more popular in recent years. The existing RDH schemes for HDR images may cause the problem of stream expansion, leading to the expansion of storage size for original HDR image. The paper titled "A Fast Coding Method for Distortion-free Data Hiding in High Dynamic Range Image", co-authored by Yue Guo, Weiming Zhang, Dongdong Hou, Yuanzhi Yao, and Shuangkui Ge, proposes an efficient coding method called reverse-Golomb code for data embedding in all-zero cover to decrease the number of changed pixels, which can reduce the stream expansion of cover HDR images effectively. In addition, the operation of reducing stream expansion in this method can be implemented in shorter time compared with the syndrome trellis coding (STC).

3 Steganalysis

The paper entitled "Faster and Transferable Deep Learning Steganalysis on GPU", co-authored by Dengpan Ye, Shunzhi Jiang, Shiyu Li, and Changrui Liu, proposes a new architecture to combine batch normalization with shallow layers, which can accelerate the convergence of the network. To decrease the loss of tiny information in steganalysis, the depth is reduced and the width of networks is increased by abandoning the max-pooling layers. In addition, to improve the efficiency of the training process, two transfer-learning schemes based on parameter multiplexing and fine tuning are presented. Extensive results provided demonstrate that this scheme can acquire acceptable performance on SRM and YE.net in some specific hiding payloads and high efficiency in deep learning steganalyzers.

Another paper entitled "Deep Neural Networks for Efficient Steganographic Payload Location", co-authored by Yu Sun, Hao Zhang, Tao Zhang, and Ran Wang, presents a tailored deep neural network (DNN) with the improved feature of mean square of adjacency pixel difference, which outperforms some state-of-the-art MAP methods for payload location under the condition of insufficient images. Two key stages of this method include the extraction for training and testing features and the training for a DNN model. The DNN model plays the role of a classifier and transforms feature vectors of each pixel location into output probabilities for each class, and the class information of a given pixel location is inputted into DNN as its label for supervised learning. In addition, payload locations of testing images are independent from those of training images.

The extraction for embedded data, i.e., extraction attack, is the ultimate objective of steganalysis. For steganography using a stego key, the extraction attack is equivalent to the stego key recovery. The paper entitled "Efficient Stego Key Recovery Based on Distribution Differences of Extracting Message Bits", co-authored by Jiufen Liu, Junjun Gan, Junchao Wang, Che Xu, and Xiangyang Luo, focuses on the stego key recovery of random LSB steganography in JPEG domain. Based on the distribution differences of extracting bits from the correct and incorrect keys, stego key recovery is transformed into a problem of hypothesis test for the message-bits distribution. Stego key recovery methods based on nonparametric hypothesis test and parametric hypothesis test are presented. The stego key corresponding to the minimum of the Chi-square statistic is regarded as the correct key. The message-bits distribution extracted with the

incorrect key is approximately the same as the distribution of available coefficients in stego images. Experiments of stego key recovery were conducted on OutGuess 0.13b, OutGuess 0.2, JPEG-domain random LSB matching steganography and random F3 steganography. The results show that the proposed method can recover stego key successfully.

4 Reversible data hiding

The paper entitled "Real-time Reversible Data Hiding Based on Multiple Histogram Modification", co-authored by Tong Zhang, Xiaolong Li, Wenfa Qi, Wei Li, and Zongming Guo, presents an effective reversible data hiding scheme for high-capacity embedding, in which multiple pairs of expansion bins are used in each histogram and a greedy searching method is designed to adaptively decide the pair number of expansion bins and corresponding values. This scheme can eliminate the gap between one-pair-based method and multi-pair-based method for multiple histogram modification, and makes the latter feasible in computation. Experimental results show that the scheme achieves high visual quality of embedded image and good real-time performance.

Another paper entitled "A Real-time Dual-image-based Reversible Data Hiding Scheme Using Turtle Shells", co-authored by Jiangyi Lin, Yanjun Liu, and Chin-Chen Chang, focuses on the dual-image-based reversible data hiding using turtle shells. Through designing a turtle shell-based reference matrix, one secret bit is embedded into the first shadow image and four secret bits are embedded into the second shadow image. Based on the orientation relationship between the pixel pairs from the two shadow images, the embedded bits can be extracted and the original image can be recovered reversibly. Experimental results show that this scheme can obtain an embedding rate of 1.25 bpp with satisfactory quality of shadow images. Also, this scheme has good performance of security to resist static attacks on pixel-value differencing histogram.

In the paper entitled "Improved Reversible Data Hiding Based on PVO and Adaptive Pairwise Embedding", Haorui Wu, Xiaolong Li, Yao Zhao, and Rongrong Ni improve the pixel-value-ordering-based reversible data hiding method through observing the modification for two prediction errors is independent without exploiting the correlation in each block. In their improved method, the two prediction errors of each block are utilized as a pair, and the pairs are modified for data embedding according to adaptive two-dimensional histogram modification. Based on the experimental results, the proposed method can achieve superior rate-distortion performance compared with the original PVO-based method and some of its improved versions.

In recent years, signal processing in encrypted domain (SPED) has attracted considerable attention due to the requirement of privacy preserving in cloud computing. The paper entitled "Real-time Reversible Data Hiding in Encrypted Images Based on Hybrid Embedding Mechanism", co-authored by Wei Zhang, Ping Kong, Heng Yao, Yu-Chen Hu, and Fang Cao, focuses on separable reversible data hiding in encrypted images, which includes the stages of image encryption, data embedding, data extraction and image recovery. In their proposed scheme, non-overlapping blocks are encrypted by stream cipher and permutation, and encrypted blocks are classified into smooth region and complex region adaptively. MSB layer of a part of pixels in blocks of smooth region is embedded with secret data, and LSB layers of other pixels are collected and compressed to generate a room for embedding the secret data again. Separable operations of data extraction, image decryption and recovery can be realized. Experimental results show the effectiveness and low computation efficiency of this scheme.

In the paper entitled "Real-time Reversible Data Hiding with Shifting Block Histogram of Pixel Differences in Encrypted Image", Zhenjun Tang, Shijie Xu, Dengpan Ye, Jinyan Wang, Xianquan Zhang, and Chuanqiang Yu propose an efficient reversible data hiding scheme for encrypted images in the homomorphic encrypted domain, in which a block-based encryption method with additive homomorphism is utilized to maintain spatial correlation of plaintext image in encrypted domain. Also, block histogram shifting is applied to realize data embedding with high-capacity and reversible image recovery. Comparison results demonstrate that the proposed scheme outperforms some state-of-the-art schemes with respect to embedding rate, image quality and computational complexity.

5 Image forensics

The paper entitled "A Multi-purpose Image Forensic Method Using Densely Connected Convolutional Neural Networks", co-authored by Yifang Chen, Xiangui Kang, Yun-Qing Shi, and Z. Jane Wang, proposes a multi-purpose method based on densely connected convolutional neural networks (CNNs), which can realize the simultaneous detection for 11 different types of image processing operations. In this scheme, a CNN architecture is designed for image forensic purposes based on different architecture components, in which a small receptive field is applied throughout the architecture to learn forensic-related features. In addition, the dense connectivity pattern is introduced to increase variations in the input of subsequent layers through feature reuse, which has better parameter efficiency than the traditional pattern and alleviates the vanishing-gradient problem. This method can achieve better performances than the compared methods with respect to multiple operation detection tasks, especially for small image patches.

In recent years, many forensic methods have been studied to determine the processing history of multimedia data. However, due to the interaction caused by tampering operations, some fundamental limitations about the determination of tampering order and type still exist. The paper entitled "Real-time Detecting One Specific Tampering Operation in Multiple Operator Chains", co-authored by Shangde Gao, Xin Liao, and Xuchong Liu, proposes an efficient theoretical framework to solve this problem, in which the operation detection problem is analyzed from the perspective of set partitioning and detection theory. Based on certain detectors, conditional probability criterions are exploited to quantify the identification of one specific operation, and MLE is utilized to obtain the best detectors. Simulations show that this proposed framework and constraints are effective for operation detection.

In the paper entitled "An Approach to Detect Video Frame Deletion Under Anti-forensics", Haichao Yao, Rongrong Ni, and Yao Zhao propose an effective anti-forensic scheme, which is inter-frame interpolation at the frame deletion point (FDP). Taking advantages of the two frames on both sides of FDP, the interpolated frames are produced to repair the inter-frame continuity. Additionally, a global and local joint feature is presented to differentiate the interpolated frames and the pristine frames, which can avoid the problem of weak residual in HEVC videos and guarantees real-time detection simultaneously. Experimental results demonstrate that this scheme can detect frame deletion under anti-forensic operation effectively.

6 Image encryption

In the paper entitled "Efficient Image Encryption and Compression Based on a VAE Generative Model", Xintao Duan, Jingjing Liu, and En Zhang focus on the image encryption based on variational auto-encoder (VAE) generation model. The random gradient method is applied to train the VAE generation model, and iteration times of the model are decided by the training time, loss function and reconstructed image. PSNR and MSE are utilized to measure compression performance of the model. Then, two trained image data divisions are used to change the data of the generated model and produce the encrypted image. Experimental results demonstrate that this method is fast and easy to implement, and the distortions of decrypted image with respect to original image is low.

How to ensure the correctness of the image content if an encrypted image is performed by active attack is an important issue. The paper entitled "Robust Real-time Image Encryption with Aperiodic Chaotic Map and Random-cycling Bit Shift", co-authored by Fengyong Li, Haibin Wu, Gang Zhou, and Weimin Wei, tackles this recent challenge in real-time image encryption. In the proposed scheme, original image is first permuted with an aperiodic generalized Arnold transform, and then, cycling bit shift is randomly performed on each pixel of the scrambled image by changing the pixel values at bit level. As a result, the encryption procedure is finished by conducting XOR operation between the scrambled image and a secret matrix produced by the chaotic map. This scheme has better performances in terms of low computation complexity and robustness compared with some state-of-the-art schemes.

7 Other emerging techniques

In the paper entitled "Privacy Protection Based on Binary Fingerprint Compression", Sheng Li, Jiajun Su, Zichi Wang, and Xin Chen propose a real-time system to protect fingerprint database through compressed binary fingerprint images, which can be used to store private data with high capacity. In this system, fingerprint image is first transformed into a binary bitstream, and then, is compressed with run-length coding and Huffman coding to create a sparse space to accommodate private data. At last, the image constructed by the obtained binary bitstream is encrypted for security. After fingerprint matching is passed with the decrypted and decoded binary fingerprint, the private data can be extracted. If fingerprint matching is failed, private data cannot be extracted. Even if a leakage of the encryption key occurs, the system can still protect the user privacy based on the existence of the data-embedding key.

The paper entitled "Efficient Image Compression Based on Side Match Vector Quantization and Digital Inpainting", co-authored by Qing Zhou, Heng Yao, Fang Cao, and Yu-Chen Hu, proposes two efficient image compression methods based on an adaptive selection mechanism for vector quantization (VQ), side match vector quantization (SMVQ), and image inpainting. In both two methods, image blocks in pre-specified locations are first encoded with VQ. For each residual block, the optimal compression scheme is chosen through computing the mean square error (MSE) between the original block and its inpainted version, and then comparing it with a pre-determined threshold. If MSE is greater than the threshold, image inpainting is utilized to encode the current block. Otherwise, the compression mode of VQ or SMVQ is adaptively decided to replace image inpainting to obtain better visual quality. With the assist of transmitted indicators, the receiver can implement image inpainting and image decompression effectively and efficiently.

Visual secret sharing is an effective technique for the protection of data transmission. To enhance the security, the data hiding-based visual secret sharing (DH-VSS) methods are emerging and have attracted considerable research attentions recently. In the paper entitled "Real-time Adaptive

Visual Secret Sharing with Reversibility and High Capacity", Ching-Chun Chang, Yanjun Liu, and Kaimeng Chen propose a high-capacity (2, 2) DH-VSS method based on the LSB substitution technique, which includes two stages, i.e., shadow creation and secret extraction, and image reconstruction. In the first stage, original cover image is divided into eight bit planes and secret data are embedded in the 4-LSB bit planes to generate two shadow images. In the second stage, both the embedded data and the cover image can be correctly recovered with two shadows. Experimental results demonstrate that this method has satisfactory performance of computational complexity and embedding capacity.

The publication of this special issue has been made possible due to contributions made by many people, in particular by authors and reviewers. We wish to thank all the authors for the submission of their excellent works and also appreciate the technical reviews provided by the reviewers. We do hope that the papers published in this special issue would be of great benefit to the readers of Journal of Real-Time Image Processing. At the end, we would like to thank Prof. Matthias F. Carlsohn and Prof. Nasser Kehtarnavaz, Editors-in-Chief of Journal of Real-Time Image Processing, and the Springer staff for their great support and help from the beginning to the eventual publication of this special issue.

Chuan Qin received the B.S. degree in electronic engineering and the M.S. degree in signal and information processing from Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. Since 2008, he has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently a Professor. He was with Feng Chia University at Taiwan as a Postdoctoral Researcher from July 2010 to July 2012. His research interests include image processing and multimedia security. He has published over 110 papers in these research areas.

Zhenxing Qian received both the B.S. and the Ph.D. degrees from University of Science and Technology of China (USTC) in 2003 and 2007, respectively. Since 2009, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University. Now, he is a Professor of Fudan University. He has published over 80 peer-reviewed papers on international journals and conferences, and has managed more than 10 projects including three projects of National Science Foundation of China and the Shanghai Rising-Star Project. His research interests include information hiding, image processing and multimedia security.

Guorui Feng received the B.S. and M.S. degrees in computational mathematic from Jilin University, China, in 1998 and 2001, respectively. He received Ph.D. degree in electronic engineering from Shanghai Jiaotong University, China, 2005. From January 2006 to December 2006, he was an assistant professor in East China Normal University, China. During 2007, he was a research fellow in Nanyang Technological University, Singapore. Now, he is with the School of Communication and Information Engineering, Shanghai University, China, where he is currently a Professor. His current research interests include image processing, image analysis and computational intelligence.

Xinpeng Zhang received the B.S. degree in computational mathematics from Jilin University, China, in 1995, and the M.E. and Ph.D. degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively. Since 2004, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University. Now, he is a Professor of Fudan University. He was with the State University of New York at Binghamton as a visiting scholar from January 2010 to January 2011, and Konstanz University as an experienced researcher sponsored by the Alexander von Humboldt Foundation from March 2011 to May 2012. He is an Associate Editor for the IEEE Transactions on Information Forensics and Security. His research interests include multimedia security, image processing, and digital forensics. He has published more than 200 papers in these areas.