Opportunities and Challenges for Biometrics

Zhenan Sun, Qi Li, Yunfan Liu, and Yuhao Zhu

Abstract Biometrics refers to the science and technology of automatic identification achieved by computers through acquiring and analyzing physiological and behavioral characteristics of human body. The purpose of biometrics research is to give computers advanced intelligence to automatically detect, capture, process, analyze, and identify digital biometric signals, that is, make machines "can see and hear". This is one of the basic functions of machine intelligence as well as one of the most significant challenges in theoretical and applied research human beings face. In conclusion, biometrics research is important in terms of both academic significance and practical value. In recent years biometrics has become an important part of national strategies such as the "Internet + Action Plan" and the "Development Plan on the New Generation of Artificial Intelligence". At the same time, it has already become a new growth point for strategic high-tech and electronic information industry in the field of national and public security. This paper introduces research progress of several common biometric modalities such as face, iris, fingerprint and gait, summarizes development trends and opportunities of current biometrics technology, and analyzes main challenges on the road to the development of a new generation of biometrics. Finally, this paper provides some suggestions regarding the future development of biometrics.

Keywords Biometrics · Face recognition · Iris recognition · Fingerprint recognition · Gait recognition

1 Introduction

Identification is the key technology to protect national and public safety, to maintain economic and social order, and to ensure the security of personal information. Traditional identification methods are based on specific knowledge (such as passwords, codes, questions, answers, etc.) and physical objects (such as keys, ID cards,

Z. Sun (✉) · Q. Li · Y. Liu · Y. Zhu
National Laboratory of Pattern Recognition, Center for Research on Intelligent Perception and Computing, Institute of Automation, Chinese Academy of Sciences, Beijing, China
e-mail: znsun@nlpr.ia.ac.cn

China's e-Science Blue Book 2020,
https://doi.org/10.1007/978-981-15-8342-1_6

USB shields, etc.). They have inherent defects such as being cracked, forgotten, and stolen, and it is difficult to meet the requirement on reliability, security, and convenience. Biometric identification (referred to as Biometrics) is based on the identification of physiological or behavioral characteristics of individuals. It has the unique advantage of being distinct, stable, reliable, and portable. Common biometric modalities include fingerprints, iris, face, palm print, hand shape, veins, handwriting, gait, voice, etc. (Fig. 1). Biometrics is an interdisciplinary field: acquisition devices at the hardware level involve optical engineering, mechanical engineering, and electronic engineering; recognition algorithms at the software level involve key problems in fields of pattern recognition, machine learning, computer vision, artificial intelligence, digital image processing, signal analysis, cognitive science, neural computing, human–computer interaction, and information security.

Biometrics refers to the science and technology of automatic identification achieved by computers through acquiring and analyzing physiological and behavioral characteristics of human body. The purpose of biometrics research is to give computers advanced intelligence to automatically detect, capture, process, analyze, and identify digital biometric signals, that is, make machines "can see and hear". This is one of the basic functions of machine intelligence as well as one of the most significant challenges in theoretical and applied research human beings face, which is of great scientific significance.

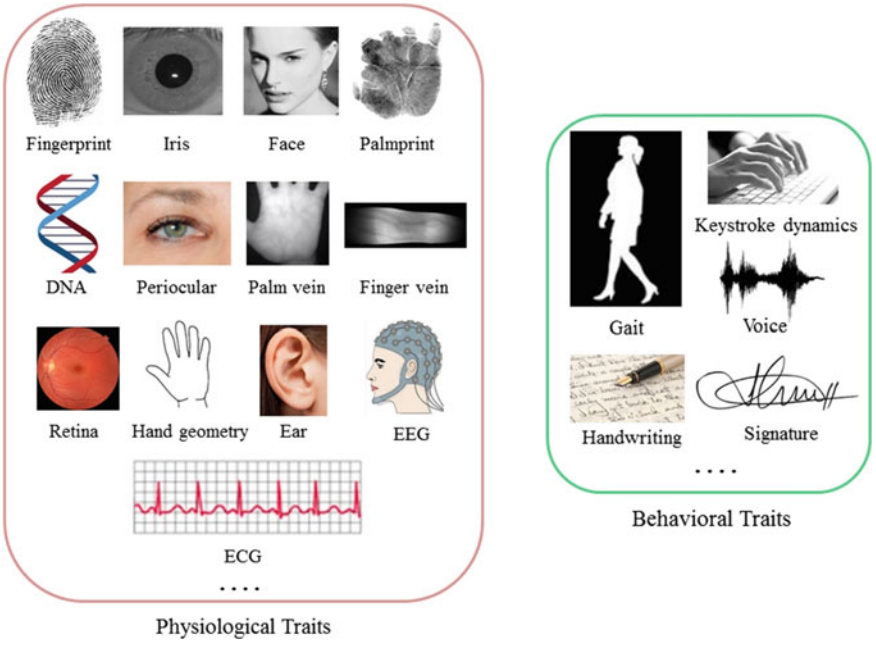

Fig. 1 Representative modalities of biometrics

Biometrics has complex patterns (points, lines, regions, textures, etc.), various types (faces, irises, fingerprints, gait, handwriting, etc.), diverse categories (up to tens of millions of people per class), rich information (statistical and structural information, local and global information), and subtle differences. They could be reflected and described in various signal forms such as images, videos, and speech, so biometric recognition is a typical and complex problem involving pattern recognition, computer vision, and neural computing, setting a challenging goal for these disciplines, building a good basic experimental platform for related researchers for trying out new methods, validating new theories, and explaining new phenomena. Since the 1960s, basic problems of biometric recognition have always been inspiring the development of disciplines such as pattern recognition, computer vision, cognition and neural computing. Biometric recognition has also been at the forefront of the development of disciplines such as pattern recognition. Therefore, the in-depth research and final solution to the problem of biometric recognition can greatly promote the maturity and development of these disciplines.

Alibaba DAMO Academy claims that "digital identity will become the second ID card" is one of the top ten technology trends in 2019 [1]. From mobile phone unlocking, community access control to cashiers of restaurants and supermarkets, and then to stations of high-speed rail and airports, the era of face recognition and iris recognition is accelerating to come. We commented on the statement in major media such as the Xinhua News Agency, saying that "biological features, such as faces and irises, will become a key for people to enter the connected world and enjoy digital life" [54]. It can be seen that biometric recognition, such as face recognition and iris recognition, is a popular technology at the moment, and has attracted much attention from fields of political, industrial, academic, and research applications. The "Internet +" action plan [2] and "new-generation artificial intelligence development planning" [3] and other national strategies have clearly proposed to focus on supporting the development of biometric identification technology. Biometrics is not only an important academic frontier of pattern recognition and computer vision, but also one of the main directions for the fastest implementation of artificial intelligence and the largest commercial market. Biometric technology has been widely used in important areas of the country such as public security and anti-terrorism, financial payment, social security certification, and security clearance, creating a market with a size of tens of billions of dollars. In addition, face recognition involves issues of public interest such as privacy, ethics, and law, which has also caused widespread concern in the community.

2 The Development Status of Biometric Recognition Technology

2.1 Overview

The research of computer-based automatic biometric recognition started in the 1960s. Fig. 2 shows the development history of biometric identifications. With the development of basic disciplines including pattern recognition, computer vision, digital image processing, and signal processing, the research level of biometric recognition algorithms has rapidly improved; with the development of biometric sensor technology and computer technology, rapid implementation and low-cost promotion have become possible; with the increasing emphasis on security management and the increasing demand for automatic identity authentication, biometric systems have been widely used in households, workplaces and public areas.

Therefore, in recent years, biometric identification has become a popular direction in both academia and industry. Driven by the broad prospect of practical applications, biometric recognition has become a hot research topic in the fields of pattern recognition, image processing, and computer vision. New modalities, new devices, new theories, and new methods have emerged endlessly to guide and promote the rapid development of related disciplines.

The National Science Foundation (NSF) funded biometrics as a key direction, and also held biometric disciplinary development seminars. The Center for Identification Technology Research, an institute dedicated to researching biometric recognition, was established in conjunction with 14 universities, including Michigan State University, West Virginia University, Rice University, and the University of Chicago. The National Science and Technology Council (NSTC) is a cabinet-level committee chaired by the president, members of ministers, and heads of major federal agencies related to science and technology policy, which is in charge of the decision-making process related to scientific and technical issues.

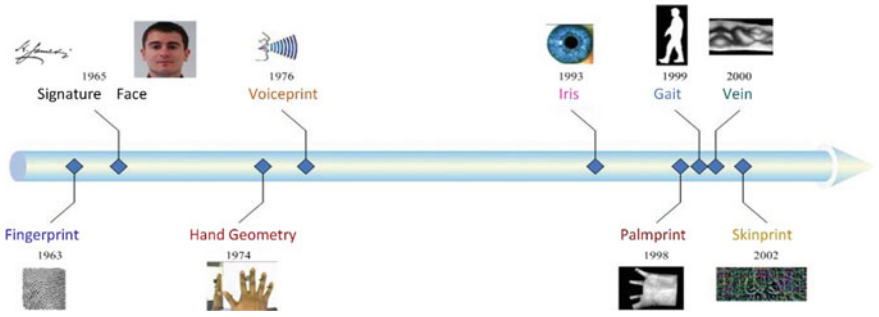

Fig. 2 The history of biometric identification

NSTC attaches great importance to promoting the development and application of biometric identification technology in the United States. It has specifically established a biometric identification committee and has released a series of biometric identification technology development planning reports, such as "Biometrics in Government Post 9–11-Advancing Science, Enhancing Operations, NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards, The National Biometrics Challenge, and more.

In order to enhance the ability to protect US defense and important civilian facilities and prevent attacks from terrorists, the US Department of Defense Advanced Research Projects Agency (DARPA) launched the Human ID (Human Identification at Distance) program to develop multi-modal long-range identification of human biological characteristics. It aims to realize the technology to detect, classify and identify individuals or groups of people in all weather conditions, and provide early warning for military protection, national defense, combating terrorist acts, preventing criminals and other man-made sabotage activities.

The EU framework plans take biometrics as the focus of funding, and have organized a series of large-scale research projects such as BIOSEC, BIOSECURE, TURBINE, ACTIBIO, HIDE, MOBIO, HUMABIO, 3DFACE, MTIT, BITE, etc., collaborating with some key European universities to study critical issues in the field of biometrics, such as basic databases, test platforms, mobile biometrics, multimodal biometrics, etc.

A large number of academic papers on biometrics has been published in conferences in fields of pattern recognition, image processing, signal processing (such as CVPR, ICCV, ICB, ICPR, ICIP) and journals (such as IEEE Transactions on PAMI/IP/IFS, PR, IVC, CVIU). Some systematic in-depth works, such as Handbook of Biometrics, Handbook of Multi-biometrics, Handbook of Face Recognition, and Handbook of Fingerprint Recognition have also been published. Many universities and research institutes have engaged in the study of biometric recognition, and new biometric identification products are also emerging.

Biometric identification is not only a major appliable technology oriented to the national strategic needs, but also at the forefront of the development of pattern recognition disciplines. Therefore, the sources of biometrics research power include universities, research institutes, companies, and government agencies.

Due to the importance of biometrics for homeland security, financial security, and cybersecurity, government departments in many countries are very concerned about the research progress of biometrics. FBI and NIST have been researching fingerprint recognition technology since 1967, and have built the largest fingerprint database of tens of millions of people in the world. The United States Department of Defense (DOD) established a biometric management office and biometric fusion center in 2000, and started the face recognition scientific research project (FERET) from 1993.

The US government organizes the Biometrics Consortium every year and organizes various algorithm evaluations through NIST. Moreover, the US Department of Homeland Security, the Central Intelligence Agency, and some military research

institutions are also organizing the development of large-scale biometric identification projects. As biometric identification is a major challenge to the traditional social lifestyle, it will cause many new problems to be solved, such as privacy, ethics, law, etc. Judicial departments in many countries are also tracking the research and application status of biometric systems to guide the development of relevant laws and policies.

The development of standards for biometrics has started. Specialized agencies have already been established, such as the joint technical committee established by the ISO (the International Organization for Standardization) and the IEC (the International Electrotechnical Commission). There is a branch, SC 37 Biometrics, which is responsible for formulating relevant standards for biometric technologies. Some developed countries have also established designated departments to develop biometric standards.

The following sections mainly introduce the research progress of main biometric recognition technologies, including human face, iris, fingerprint, and gait.

2.2 Face Recognition Technology

Human face is one of the most traditional and intuitive biological features. It has received full attention and has important applications in a variety of identity authentication scenarios due to its good user acceptance and simplicity of collection. In addition, the analysis and synthesis of human faces and the emerging problems of liveness detection in face images and videos have also attracted increasing attention from both academics and industry.

In the early stage of the development of artificial intelligence, face recognition was studied as a general pattern recognition problem. At this stage, face recognition technology is mainly implemented by expert systems that rely on manual features. Its robustness and generalization are poor, and it has not achieved widespread practical application.

With the rapid development of statistical learning, many face recognition algorithms based on statistical models have been proposed. The "EigenFace" model proposed by the Massachusetts Institute of Technology is one of the most important research results at this stage [4]. This method introduces a statistical-based machine learning method to the face recognition task, and derives a series of subspace analysis methods and improved strategies based on kernel learning, such as FisherFace [5]. The introduction of statistical learning theory has also improved the performance of classifiers. Among them, Support Vector Machine (SVM) has become the first choice for classifiers due to its simple and intuitive theoretical basis and excellent adaptability to high-dimensional large sample data. Feature extraction techniques have also been developed rapidly during this period. For example, both Gabor filters and LBP filters were proposed at this time. Therefore, early face recognition methods mainly depended on the combination of artificially designed features and machine learning technology. During this period, manually designed features were not able to

cope with different changes (lighting conditions, occlusions, etc.) in unconstrained environments. Since 2011, with the rapid development of deep learning theory and the widespread application of related algorithms in the field of computer vision, deep neural network-based face recognition technology has become the mainstream. With its hierarchical structure characteristics, deep neural networks could mine higher-level information that is more representative, so that it could achieve much better discriminative performance than shallow classifiers, and could surpass the accuracy of human recognition on commonly used databases.

During this period, studies on face recognition focused on the design of loss functions. Facebook published its research results in 2014, where the DeepFace algorithm based on the softmax loss function [6] had reached 97.35% on the LFW (Labeled Face in the Wild) landmark database, reducing the error rate of existing best face recognition by 27%. Google proposed the FaceNet algorithm based on the triplet loss function in 2015 [7], relying on millions of training data, and achieved 99.63% accuracy on LFW. After that, center loss [8] and large margin softmax loss function [9] were proposed to train face recognition networks. The above-mentioned loss functions usually adopt the Euclidean distance metric. SphereFace [10] first proposed the use of cosine distance instead of Euclidean distance for face recognition training and testing, and its performance surpassed the previous method. Both post-CosFace [11] and ArcFace [12] use an improved cosine distance.

In the process of moving from the laboratory to practical applications, adaptability to large-scale face data is the primary challenge face recognition technology confronts. In 2015, the research team of the University of Washington proposed the MegaFace dataset containing millions of face images, and held a recognition competition [13], aiming to improve the recognition accuracy in the case of large-scale face data. As of 2019, research results from companies such as Tencent, SenseTime, and Sogou have topped the competition. The United States National Bureau of Standards and Technology has restarted FRVT face recognition evaluation in recent years [14], and many companies in China, such as Yitu, have achieved good performance in FRVT. In addition to the scale of the dataset, lighting conditions and poses are also important factors affecting the performance of face recognition technology. To solve these problems, 3D face recognition and cross-modal face recognition have gradually become the main research hotspots in recent years.

Face generation technology is another research hotspot that comes with the rising of big data, which could help solve the problems of large poses and age gaps in face recognition. In addition, editing attributes of face pictures, such as age, expression, hair color, etc., have great practical values in webcasting and photo retouching. Making artificial intelligence algorithms to create faces with various styles like painters also has great application prospects in the entertainment industry. High-quality artificial intelligence paintings are also considered to have high artistic value, and there have been cases of auctions in the international market. The fundamental theory behind face generation technology is Generative Adversarial Networks, which have made great breakthroughs in face frontalization [15] and face aging [16].

As one of the most common biological characteristics, face recognition has become the most widely used method of identity authentication due to its advantages

such as high accuracy and low requirements on user cooperation. The FaceID technology, released by Apple in 2017, uses structured light to capture three-dimensional information on the user's face. It can successfully solve the problems in face recognition technology such as lighting and posture, and has been applied to various identity authentication services across the entire product line. The facial recognition technology of domestic companies such as CloudWalk, Megvii, SenseTime, and Yitu has been widely used in many aspects, including face payment, bank intelligent outlets, security control in key areas, and intelligent medical care. Based on face recognition, technologies such as face liveness detection and pedestrian trajectory analysis have also emerged in smart finance and intelligent transportation.

Although face recognition technology is now developing rapidly, it is still a problem that has not been completely solved. For example, accurate face recognition in surveillance scenes and large scale data, for people with dark skins, and for face images with large age gaps. There is a lot of room and potential for face recognition technologies to be improved.

2.3 Iris Recognition Technology

The industry is the main research force of iris image acquisition devices. LG, Panasonic, IrisGuard, IrisKing and other companies have designed a series of close-range iris image acquisition equipment. In order to improve the convenience of iris imaging and to expand the application range of iris recognition, an increasing number of institutions have started research on long-range iris image acquisition. The InSight system of AOptix in the United States implements clear imaging of iris from 1.5–2.5 and 2.4–3 m away. Carnegie Mellon University is currently developing a device with an imaging distance of 12 m. OKI's IRISPASS-M and Panasonic's BM-ET500 use PTZ gimbals to adjust the camera's pitch angle to accommodate users of different heights. At the same time, the iris imaging device gradually has become more and more lightweight to be used in practical situations. In 2013, AOptix developed a mobile phone external iris, face, fingerprint image acquisition module, which can be seamlessly connected with the iPhone. In May 2015, Fujitsu released a smartphone that can use iris recognition to unlock, log in to online accounts, and pay. IrisKing officially released the first domestic iris recognition mobile phone in early 2016. In 2017, Samsung S8, Note7 and other smartphones began to add iris recognition modules.

As shown in Fig. 3, two main steps for iris recognition on given iris images are iris region segmentation and iris texture feature analysis. The iris region segmentation can be roughly divided into two categories: boundary localization based methods [17, 18] and pixel classification based methods [19, 20]. The iris texture feature analysis includes feature expression and comparison. The feature expression method extracts discriminative information from complex texture images that can be used for identity recognition. Representative feature expression method include Gabor phase-based methods [17], multi-channel texture analysis-based methods [21], correlation

filters-based method [22], and sequential measurement-based method, etc. [23]. The stability and discrimination of eigenvalues are the main factors affecting the accuracy of feature comparison.

Traditional iris recognition algorithms mostly use artificially designed logic rules and algorithm parameters, resulting in poor generalization performance of the algorithm, which cannot meet the need of large-scale application scenarios. Data-driven machine learning methods automatically learn the optimal parameters from a large number of training samples, which can significantly improve the accuracy, robustness and generalization performance of the iris recognition algorithm [24]. Large-scale iris recognition applications have brought many new challenges. Fast retrieval of iris features [25], and robust recognition of multi-source heterogeneous iris images [26] have become current research difficulties and hot issues of iris recognition.

The current mainstream iris imaging methods fail to consider subsequent image processing steps, while emerging computational imaging methods (such as wavefront coding and light field cameras) consider both imaging and image processing at the same time, which is expected to break through the existing technology bottleneck and significantly increase the imaging range. In terms of algorithms, the research team of the Institute of Automation, Chinese Academy of Sciences, inspired by the human visual mechanism, proposed the use of sequential measurement filters to describe the local texture of the iris, and designed multiple feature selection methods to determine the optimal parameters of the filter [27]. For the first time, they applied deep learning to iris recognition, and proposed a multi-scale full convolutional neural network-based iris segmentation method [28] and a convolutional neural network-based iris feature learning method [24]. They also explored the complementary relationship between deep learning features and sequential measurement features [29].

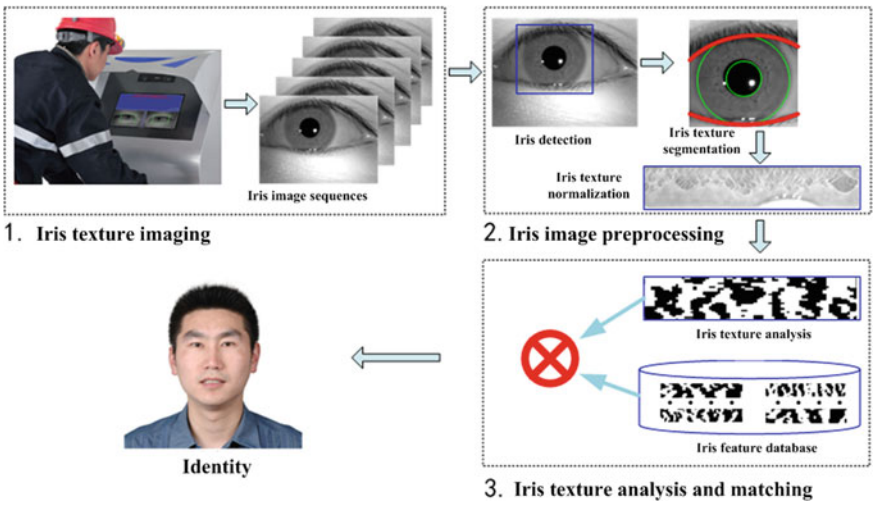

Fig. 3 The pipeline of iris recognition

Fig. 4 The development path of Chinese iris recognition technology

In addition, they systematically studied the iris image classification method based on a hierarchical visual dictionary, which significantly improved the accuracy of iris feature retrieval, ethnic classification and living body detection [25]. The development roadmap of iris recognition technology of the Institute of Automation, Chinese Academy of Sciences is shown in Fig. 4.

2.4 Fingerprint Recognition Technology

Fingerprint recognition technology is one of the most common and earliest biometric identification technologies for civilian use. In 1892, Galton and others pointed out that as a unique and stable biological feature, fingerprints can be used for identity authentication, marking the beginning of fingerprint identification technology.

Fingerprint recognition technology mainly includes three aspects, namely fingerprint image acquisition, fingerprint image enhancement, and fingerprint feature extraction and matching. After the electronic computer was invented, optical-based fingerprint collection devices have replaced traditional inks, which greatly improved the efficiency of fingerprint collection, identification, and storage. Subsequently, capacitive sensor-based fingerprint collectors were invented [30], and have been widely used in user identity authentication systems for mobile terminal devices such as Apple phones. There are mainly two types: pushing based and scratching-based. In addition, fingerprint acquisition technologies based on temperature sensors, ultrasonic waves, and electromagnetic waves have also been proposed, each with its own strengths. In recent years, non-contact 3D fingerprint acquisition systems have also been proposed to improve user experience and recognition accuracy [31].

Fingerprint image enhancement mainly includes image smoothing (de-noising and texture stitching), image binarization (separation of foreground and background), and refinement (fingerprint skeleton acquisition). Traditional image processing methods such as frequency domain filtering, Gabor transform, and matched filter [32] can effectively remove noise from fingerprint images. They can also detect, complete and refine breakpoints in fingerprint lines. With the development of deep learning, deep convolutional networks have been widely used in fingerprint image enhancement related problems, such as warped fingerprint image correction [33] due to their strong feature extraction capabilities.

Fingerprint image feature extraction and matching methods can be broadly divided into two categories: directional field-based methods and feature point-based methods. The directional field depicts ridges and valleys of the fingerprint image, which is an important basis for fingerprint image matching. Many methods have been proposed to reduce the influence of noise on the calculation of the directional field, and improve the operation efficiency. Feature points refer to the common patterns of fingerprints, including arches, account bows, left loops, right loops, and thread patterns. The characteristics of regional distribution and rotation invariance of feature points are also often used to improve the robustness of recognition algorithms. With the application of fingerprint recognition technology in different scenarios, the quality of collected fingerprint images is uneven, and sometimes even complete fingerprints cannot be obtained. Therefore, partial fingerprint image recognition problem is currently a research hotspot [34]. In addition, for protecting the safety of users' personal property, the problem of liveness detection in fingerprint recognition technology is also a research focus. In order to solve this problem, on the one hand, additional sensors can be added to the fingerprint acquisition system from the hardware perspective to detect the evidence of liveness, such as the temperature of the finger [35], color, and blood flow. On the other hand, the quality of capture fingerprint images could be considered as an evaluation metric to obtain high-quality live fingerprint data [36].

2.5 Gait Recognition Technology

Gait can be defined as a combination of action cycles that lead to motion [37]. Under this definition, biped or quadruped walking, running, climbing, jumping, and swimming can be considered as a kind of gait. In the current stage of research, the research on gait is more focused on the scope of "human walking". Gait recognition aims to use people's walking gestures to recognize identities, which is a very challenging research topic. In view of the long-distance and non-aggressive perceptual characteristics of gait, the research of gait recognition has a good application prospect and research value, especially for long-range and large-scale visual surveillance applications. Since the United States Defense Advanced Research Projects Agency (DARPA) proposed the Long-range Human Identification Program (HumanID) in 2000, a large number of research institutes and universities worldwide have joined

the research wave of "gait recognition", including Massachusetts Institute of Technology (MIT), Carnegie Mellon University (CMU), Georgia Institute of Technology (GIT), Chinese Academy of Sciences Institute of Automation (CASIA) and other world-class research institutions.

Generally, a gait recognition system takes a gait sequence as input, obtains gait features through a feature extractor, and compares the extracted features with features in the gait database to give the identity of the target person. As the key of gait recognition systems, the innovation of gait feature extraction algorithm has always been the focus of researchers. The earliest gait recognition algorithm was based on the analysis of spatiotemporal information [38]. By establishing the XYT spatiotemporal coordinate system, the sagittal angle of the target's direction is considered as the feature for identification. In [39], the optical flow method was introduced for gait feature modeling, and the best recognition results at the time were successfully obtained. Finally, the feature space transformation (EST) [40] was proposed, terminating the study on small-scale gait datasets with a 100% recognition rate. With the proposal of more gait datasets with much larger scales, modern gait feature extraction algorithms can be divided into two broad categories by whether explicit kinematic modeling is performed.

For gait feature extraction algorithms that do not require a kinematics model, most of them rely on the analysis of the spatiotemporal information of the contour of the target person. Almost all gait feature extraction algorithms without kinematics models require preprocessing such as background extraction and contour extraction. The Institute of Automation of the Chinese Academy of Sciences (CASIA) has proposed a gait recognition algorithm that analyzes contour edge information [41]. The introduction of Dynamic Time Warping (DTW) and Hidden Markov Model (HMM) [42] further improves the recognition accuracy of algorithms without kinematic models. The proposition of Gait Energy Image (GEI) [43] and Gait Flow Image (GFI) [44] has once again pushed forward the research in this direction, and a series of steps based on this method has been derived. Gait feature extraction algorithms based on kinematics use more accurate spatiotemporal information to perform motion analysis on human joints. The focus of its research is to accurately model the structure of the human body. Compared with algorithms without kinematics models, this type of algorithm achieves better robustness and recognition accuracy at the expense of algorithm complexity. Earlier methods used 16 points to approximate the human body, and with the advent of Microsoft's depth camera Kinect, depth information helped to model the human body more accurately [45].

Deep learning has become the mainstream method of gait recognition in recent years and has made breakthroughs in cross-view gait recognition. CASIA has developed a framework based on deep convolutional neural networks to learn the similarity between paired GEIs and automatically learn valuable static and dynamic features for gait recognition, and the use of "positive–negative pair"-based training methods to expand the sample size can also achieve high accuracy on small sample training databases. This method based on dual-channel mid-level gait feature fusion solves the difficulty of cross-view gait features matching in traditional methods. It achieves an average accuracy rate of more than 94% across perspectives on large-scale gait

database CASIA-B, reaching the international leading level. Related results have been published in IEEE-TPAMI [46] and IEEE-TMM [47]. Recently, the team further proposed an acceleration idea of full-graph segmentation based on convolutional neural network, which accelerated the previous algorithm by nearly 1000 times. They also built the world's largest outdoor gait database, which contains 760,000 gait sequences. The long-distance gait recognition system developed by the Institute of Automation, Chinese Academy of Sciences, won the second prize of Beijing Municipal Science and Technology Invention 2018, and it performed well on CCTV's "Smart Wisdom" program and was rated as the "wisdom pioneer". Embedded gait recognition has been applied in the field of home appliances in the United States. Gait recognition has been used in public security systems for more than 1,000 h and participated in the detection of more than 20 cases.

Although many breakthroughs have been made in gait recognition in recent years, the recognition performance is far from being saturated. In general, the current research hotspots focus on (1) improving the robustness of the algorithm in the case of clothing changes, different travel speeds, and perspective changes, (2) improving the algorithm's accuracy in long-interval gait recognition, and (3) improving the accuracy of person re-identification and other directions. Few researchers have been involved in studying the influence of factors such as race, injury, fatigue, weight-bearing, and self-control on gait recognition, which are difficult points in gait recognition research. In the next few years, the research on gait recognition will also continue the current research hotspots, and gradually expand the research direction into the above-mentioned difficult areas. As a bridge connecting current and future research fields, the research of gait-based pedestrian re-identification algorithms is expected to bring new opportunities and inspirations for research breakthroughs in gait recognition from multiple levels and perspectives.

2.6 Other Biometric Recognition Technologies

2.6.1 Palmprint Recognition Technology

Compared with other biological features, palmprint recognition has the advantage of convenient collection, good privacy, and high user acceptance. Palmprint recognition is widely used in high-level access control, public security criminal investigation, medical social security, network security, attendance and other fields. Palmprint recognition currently has two application areas: detection-oriented and civilian-oriented. Palmprint recognition based on law generally requires high-resolution palmprint images. Palmprint images based on commercial applications can generally be low-resolution grayscale images. In addition, related researches on three-dimensional palm print images and non-contact collected palm print images are also being carried out.

2.6.2 Voiceprint Recognition Technology

Voiceprint recognition is a technology that automatically recognizes a speaker's identity based on speech parameters that reflect the physiological and behavioral characteristics of the speaker in the speech waveform. Voiceprint recognition uses sound as a recognition feature and can be collected in a non-contact manner. The collection method is more concealed, the collection space is wider, and it is easier for users to accept. The technology was developed by Bell Labs in the late 1940s and is mainly used in the field of military intelligence. With the gradual development of voiceprint recognition technology, the technology was used in the fields of forensic evaluation and forensic evidence in the United States in the late 1960s. At present, voiceprint recognition technology has important applications in the fields of information, financial security, justice, security and document anti-counterfeiting, military and national defense.

2.6.3 Eyeprint Recognition Technology

Eyeprint recognition is a technology for individual identity verification through the unique vein pattern on the white region (sclera) of the human eye. People's eye conditions are not static, eye congestion could be caused by allergies, red eyes, or hangovers all night, but this will not affect the pattern of eyeprint and blood vessels in the eye. This shows that the eyeprint features are stable enough to be used for authentication. Compared with other biometric recognition technologies, eyeball reflection, blinking, eyelashes and other factors will seriously interfere with the accuracy of eyeprint recognition, resulting in high thresholds and challenges for its research and development.

In addition, the field of biometrics continues to explore emerging information modalities for identity verification, such as veins [48], knuckles [49], human ears [50], EEG/ECG signals [51], eye movements [52], screen swiping patterns [53], etc.

3 Development Trends and Opportunities of Biometrics

By analyzing the policy environment, market size, application platform and subject development of biometrics, we believe that biometrics are currently in an opportunity period of great strategic importance.

3.1 Regulatory and Policy Support

At present, the important role of biometric identification technology has been highly recognized by governments and the general public, providing a loose policy environment for the widespread application of biometric identification technology. The United States successively signed the Patriot Act, the Border Visa Act, and the Aviation Security Act after "911", all requiring the use of biometric technology as a guarantee of legal implementation, requiring biometric features such as fingerprints and irises to be added to passports. In 2006, ICAO mandated that facial features must be stored in electronic passports, with fingerprints and irises as options. Also, more and more countries and regions have added biometrics to their ID cards. For example, the Indian government has launched a national identification and management UID project and has collected more than 1.2 billion people's iris, face and fingerprint information.

Biometric identification technology has been highly valued by various sectors of society such as government, industries, universities, research institutes, and other industries. For example, the annual biometric forum in the United States brings the Department of Security, the Department of Justice, the Department of Defense, FBI, CIA, NIST, universities, research institutes, and thousands of companies together to discuss biometric technology, industry, and the unprecedented policy opportunities of it.

3.2 Growing Biometric Market

Bill Gates, the CEO of Microsoft, had predicted in 2004 that biometrics would become an important change in the IT industry in the next few years. In August 2012, Gartner published a report about technology hype cycles of the year 2012–2013 which shows biometric authentication has now entered a bright period and reached its peak as one of the 48 emerging technologies. Currently, biometric technology and products are now available for public security areas such as border clearance, residence permits, public security and justice, financial securities, e-commerce, social security benefits, information networks and other civil areas such as access control or attendance in schools, hospitals, venues, supermarkets, etc., which is to say biometrics has been widely used and formed a new industry of information technology.

Faces, irises and other identifying information have become the portal of the "Interne+" era and the intelligent era, which has broad development capacity. For example, iPhone X and Samsung S8 use face recognition and iris recognition technology as mobile phone login methods, respectively. According to a forecast from the BCC market research company in January 2016, the global biometrics market size will grow significantly in the next few years. It estimates that from 2015 to 2020, the global biometrics market will reach a compound annual growth rate (CAGR) of 22.7%, and the global biometrics market will reach 41.5 billion by 2020.

3.3 Inter-Connected Application Platform

Biometric technologies may be useful as long as there is a space for human existence on whether physical space or virtual space. At present, the development of mobile internet, IoTs, and social networks provide a new application platform for the development of biometrics. With the in-depth development of information technology in human society, the biometric sensors (audio and video) of mobile internet and IoTs are showing a general development trend. At the same time, the scale of audio and video data on the internet is growing explosively, which provides a new development opportunity for biometric identification technologies.

Many countries have deployed tens of millions of high-definition monitoring terminals all over the country where personal activities are the major monitoring content and biometrics is an important technology to determine the identity of individuals. The high-definition cameras on hundreds of millions of new smartphone and tablet computer growth each year have built a ubiquitous mobile visual perception platform. Such iPhone and other smartphones are equipped with voice interaction technology, which provides a new way to collect the biometrics of face, iris, voiceprint, and other modes; the booming social networking sites generate massive user data every day, in which a large number of images and videos involve biometric information such as faces, irises, and voices can be collected. In addition, some somatosensory game platforms, such as Kinect, can obtain depth and color image information at the same time, providing new opportunities for 2D and 3D face fusion recognition. Besides, augmented reality and virtual reality (AR/VR) scenes would use biometric technology either.

3.4 Upgrading Technology

After more than 40 years of development in the field of biometrics, researchers have accumulated a wealth of theories and methods, and the proposed technologies can basically correctly identify highly coordinated users under strictly controlled conditions. However, biometric images are subject to internal physiological changes and external environmental changes, in turn, the performance of biometrics declined sharply, which leads these technologies cannot meet the needs of identification in the complex environment of the real world. Many basic scientific problems need further study in terms of ease of use, robustness, real-time, security, and wide-area perception, which have severely restricted the subject progress, technology promotion and industrial development of biometrics. Therefore, with ubiquitous biometric sensors, biometric recognition technology is facing a historical opportunity from applied only at controlled conditions to complex real-world environments.

In order to meet the growing practical application needs in the field of information security, we must innovate existing biometric recognition models and propose a set of innovative technologies, systems, and applications to form a systematic solution,

handling biometric image acquisition, living detection, pattern recognition, security protection; break through the various bottlenecks of the existing biometric recognition system in ease of use, accuracy, robustness, real-time, and security; and build convenience, automation, intelligence, networking, safe and reliable biometric identification system for massive users. Therefore, we are facing the historical opportunity to seize the commanding heights of the new generation of biometrics technology, which is of strategic significance for the scientific progress of biometrics, technology promotion and industrial development.

4 Major Challenges in Developing Next-Generation Biometrics

The core concept of the new generation of biometric recognition technology is "people-oriented", and it is necessary to break through many technical bottlenecks to achieve the leap-forward development from controlled and restricted scenarios to ubiquitous biometric recognition cases. For one object to be identified, a more intelligent biometric image acquisition device and computer vision software will realize a new model of biometrics that transitions from "humans cooperate with machines" to "machines actively cooperate with people": the requirements on location, distance, posture, and expression of this object will be more relaxed. Biometric systems can complete the identification process and complete visual monitoring tasks such as detection, tracking, and trajectory analysis in a relatively relaxed environment without explicit user's cooperation. Indeed, there are many technical challenges for the new generation of biometric recognition technology in every step from biometric information acquisition to information processing, from real-time response to security assurance and from physical space to cyberspace.

4.1 The Ease of Acquisition

The biometric information acquisition device is a front-end module of any biometric identification system and is also a major bottleneck that affects the popularization of biometrics. Therefore, the necessity and significance of developing a convenient biometric acquisition device are self-evident. The convenient acquisition of biometric information involves a series of core technologies such as human–computer interaction, target detection, quality evaluation, and integration of optical-mechanical–electrical computing. In terms of biometric information acquisition, potential research directions include long-distance iris-face integrated imaging, multispectral biometric imaging (such as visible light fingerprint/palmprint image, near-infrared finger vein/palm vein image acquisition, near-infrared human face imaging, etc.), non-contact fingerprint/palmprint imaging, facial depth image acquisition which is similar

to Kinect technology, etc. In practical application scenarios where the environment has complex lighting conditions, various environmental backgrounds, crowd movement, mutual occlusion, and small biological targets such as iris, face, and palmprint, the key issue remains to be solved that how to automatically capture multi-modal organisms with dynamic changes over long distances. In addition, there are also many important challenges in obtaining high-quality voiceprint information in noisy environments.

4.2 Recognition Robustness

The algorithm part of biometrics is undoubtedly the core module of any biometric system. This part aims to analyze and extract robust biometrics from the biometric information collected by the biometric acquisition device to achieve accurate and reliable individual matching and recognition. This process involves preprocessing, feature analysis, feature extraction, and feature matching for identification as well as information fusion of multi-modal biological characteristics.

Due to the complexity of the imaging environment under complex conditions such as lighting condition, distance, pose, expression, blurriness, deformation, glasses, occlusion, noise, and other factors will cause large intra-class differences between biometric images collected at different times. It is a challenging pattern recognition problem that how to propose an image feature expression and analysis method which is robust to these external factor changes while ensuring inter-class separability. Recently, the academic community has proposed theories and methods such as sparse representation and deep learning as new tools for solving the robustness problem of biometric recognition.

Biometrics in complex environments includes both active and passive identity authentication. In the traditional active identity authentication mode, users need to cooperate actively and the image quality needs to be relatively good. Different from the active authentication, the identified objects in the passive identity authentication do not necessarily be willing to pass the authentication, and may even adopt resistance strategies, such as makeup and non-cooperation. In order to achieve passive identity authentication, we must study automatic biometrics in non-cooperative situations, and we must tackle key issues such as robust biometric identification.

In the case of face recognition, the accuracy rate of identity authentication currently exceeds 99% under controlled conditions. But in video surveillance scenarios, the accuracy rate quickly drops below 80%; in addition, the low-resolution facial images, incomplete fingerprints and palmprints pose a major challenge to the robustness of biometrics. Thus, there is still a long way to go for robust biometric recognition.

4.3 Real-Time Matching

With the declining cost of biometric imaging and the urgent need for governmental high-performance identity authentication technology, biometrics will be widely utilized. For example, biometrics has begun to be promoted in national and industry level applications such as electronic passports, ID cards, suspect investigations, identification of missing persons, banking, e-commerce, medical treatment, insurance, social welfare, etc. At this time, the scale of the biometrics template in the central database is bound to reach a huge amount (ten million or even hundreds of millions), and the cost of time to identification will be unbearable. This is one of the three major issues in the field of biometric recognition: the problem of scale. In complex application environments such as airports, stations, and docks, it is often necessary to screen certain preset special groups (such as those in the "blacklist" of the Ministry of Public Security and the Ministry of Security), which requires real-time efficiency large-scale biometric data retrieval technology breakthroughs.

4.4 Credibility and Security

A biometric system is a security system. Like other information security technologies, it may be attacked by various kinds of attacks, and threatened by hackers. Besides the forgery the biometric samples of others, many other possible attacks include: modifying the sample data on the communication link between the acquisition device and the server; modifying the recognition results; replacing the matching program; attacking the biometric template database, etc. The safety factor of the biometric system depends on the weakest part since each joint is equally essential. To make biometric technologies can be applied in the situation of high-security requirements, besides algorithm design, it is also very important to protect the security of the system itself and improve the resistance to various hacker attacks. In order to prevent malicious hackers from forging and stealing other's biometrics for identity authentication, the biometric system must have the functionality of living detection, that is, to determine whether the biometric images come from living individuals. For all kinds of potential attack methods against biometric systems in an open environment are unpredictable, it is very difficult to design a strict and foolproof security protection system for biometric systems. At present, the security of a biometric system has been highly valued by the academic and industrial communities. For example, Trusted Biometrics, the seventh framework research project of the EU, specializes in the security and anti-counterfeiting of biometric systems.

4.5 Coordinated Identification in Physical and Cyberspace

Cyberspace, as the expansion and extension of human society's living space in the era of information, is closely related to the traditional social space of human existence as a supplement. The rapid development of public transportation and information networks has made social individuals increasingly active in physical and cyberspace, placing huge challenges to public safety and social management. Therefore, how to realize coordinated identification in physical and cyberspace is an important problem with many challenges. For example, in recent years, Google and Facebook have acquired some face recognition companies and developed several biometric applications for the network environment, illustrating the development prospects of biometric recognition technologies. Basically speaking, it is a new research problem on how to make use of social network relationships, integrate the network audio and video information and the IoT monitoring biometric information to achieve a coordinated identification system across physical and cyberspace.

4.6 Evaluation and Certification

From a perspective of research, the performance evaluation of biometric recognition algorithms can follow the latest progress in academic research, explore the inherent potential of recognition algorithms, compare the pros and cons of different algorithms, and propose algorithm optimization solutions based on deficiencies, such as feature selection, parameter adjustment, etc., so as to push forward the research of biometric recognition algorithms. From the perspective of industry and applications, if there is no standard technical supervision and performance evaluation system in the field of biometric identification, the entire industry will be in a state of chaos and disorder, which will bring many fatal hidden dangers to the public and personal security systems.

In the face of the booming biometric recognition technology, countries around the world have set up specialized evaluation centers. For example, the United States has the National Institute of Standards and Technology NIST and the National Biometric Test Center relies on San Jose State University. In addition, the United States Department of Defense has established a Department of Defense & Federal Biometric System Protection Profile which conducts a rigorous evaluation of all biometric systems that enter the US military and federal government. The British government's information security technology authority CESG has proposed a Biometric Evaluation Methodology under the framework of the Common Criteria for general information security products. Korea established the National Biometric Test Center (K-NBTC), built a large-scale database, and carried out testing services for standards compliance, identification performance, and security performance.

In summary, there many problems with how to evaluate next-generation biometric technologies that are still unsettled, including evaluation data (how to quantify the

representative, quality and scale of test data, etc.), evaluation models (how to statistically analyze test results and how to predict actual application performance based on test results, etc.) and evaluation software (how to build automatic, configurable, and integrated evaluation system).

5 Development Strategies on Biometric Technologies

Focus on the challenges encountered by biometric applications in complex environments, those many aspects like human–computer interaction, information acquisition, preprocessing, feature analysis, pattern matching, large-scale retrieval and comparison, multimodal information fusion, security, anti-counterfeiting, and application mode in biometrics need innovations on friendly interfaces, accurate identification, and reliable systems that can do real-time comparisons. The improved intelligence, automation, and informatization level of biometric identification system are required to achieve environments and users adaption, improve the user experience and satisfaction so as to complete the technical transition of biometrics from "humans cooperate with machines" to "machines actively adapt to people", realize the applied biometric technologies from a controlled environment to a complex environment, develop a biometric industrial cluster with independent intellectual property rights (including core chips, acquisition devices, recognition algorithms, and application systems), and create a large scale biometric technology and product certification system. Through technological breakthroughs of biometrics in complex environments, it will greatly expand the scope of biometrics in the real world, promote the revitalization of the biometrics industry, and increase the international market share of biometric identification products. Achievements in scientific research with independent intellectual property rights through collaborative innovation of industries, universities, and research institutions will be the core factor to enhance the biometric industries, to create domestic biometric brands, to satisfy the urgent public security needs.

5.1 Overall Solution for Large-Scale Biometric Applications

At present, many countries have determined to embed biometric information in the new generation of ID cards and e-passports. These ID cards are widely used in education, social security, finance, customs clearance, telecommunications, transportation, tourism and other fields by the supports of an inseparable national biometric infrastructure platform. Therefore, it is important and urgent to study architecture and key technologies of the ultra-large-scale biometric application system with independent intellectual property rights.

5.2 Biometrics' IntelliSense and Human–Computer Interaction

Focus on developing biometric imaging devices such as non-interfering face and iris image acquisition devices; non-contact fingerprint, palmprint, and vein acquisition devices at a medium-and-long distance; acquisition devices which can endure object motioning; and large depth of field acquisition devices based on the new photoelectric principles.

5.3 Robust Biometric Identification Method

The researches should focus on human face, gait, and iris recognition technologies in video surveillance scenes, incomplete fingerprints in the field of criminal investigations in public security, palmprint recognition technology, and multi-source heterogeneous biometric recognition methods.

5.4 Biometric System Security Protection

Construct a comprehensive biometric identification security protection system based on multispectral imaging, live detection, cryptography, information hiding and other technologies to solve the security problem of biometric identification.

5.5 Coordinated Biometrics Across Physical and Cyberspace

Focus on the researches of cross-camera identification technology in the large-scale monitoring scene of physical space, the identification technology based on social networks, and the identification technology of the fusion of physical space and cyberspace.

5.6 Biometric Evaluation and Certification Platform

The evaluation and certification of biometric performance are related to national security, industrial development, and academic progress. Therefore, it is necessary to study the standards and technical systems of biometric evaluation and certification, including not only biometric accuracy and robustness but also security tests. It also

needs to establish an expert system that guides the optimization of algorithms based on the evaluation information and make better evaluations with better algorithms.

6 Conclusion

With the rapid development of artificial intelligence technologies, such as adversarial generative networks, automated machine learning (AutoML), neural network architecture search (NAS), etc., and emerging sensing devices, such as light-field cameras, 3D imaging, multispectral imaging, etc., biometric technologies and its applications could have a broad developing capacity. Biological features such as faces, irises, fingerprints, veins, voiceprints, and gait in the era of artificial intelligence are more convenient to collect and can be identified more accurately and safely in wider applications. Such biological features now have become the identity token for people to go through security checks, customs clearance, door opening, withdrawal, payment, social insurance, examination, medical treatment, and attendance in physical and cyberspace. New technologies, applications, and industries of biometrics have become new driving forces for social progress and human civilization.

References

1. Alibaba DAMO Academy (2019) The top ten technology trends in 2019 by Alibaba DAMO Academy [EB/OL]. https://damo.alibaba.com/events/50
2. The Central People's Government of the People's Republic of China (2015) Guiding opinions of the state council on vigorously advancing the "internet plus" action [EB/OL]. https://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm
3. The Central People's Government of the People's Republic of China (2017) Notice of the state council on issuing the development plan on the new generation of artificial intelligence [EB/OL]. https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm
4. Turk MA, Pentland AP (1991) Face recognition using eigenfaces. IEEE, The United States
5. Belhumeur PN, Hespanha JP, Kriegman DJ (1997) Eigenfaces versus fisherfaces: recognition using class specific linear projection. IEEE Trans Pattern Anal Mach Intell 19(7):711–720.
6. Taigman Y, Yang M, Ranzato M, Wolf L (2014) Deepface: closing the gap to human-level performance in face verification. IEEE, The United States
7. Schroff F, Kalenichenko D, Philbin J (2015) Facenet: a unified embedding for face recognition and clustering. IEEE, The United States
8. Wen Y, Zhang K, Li Z, Qiao Y (2016) A discriminative feature learning approach for deep face recognition. Springer, Switzerland
9. Liu W, Wen Y, Yu Z, Yang M (2016) Large-margin softmax loss for convolutional neural networks. PMLR.
10. Liu W, Wen Y, Yu Z, Li M, Raj B, Song L (2017) Sphereface: deep hypersphere embedding for face recognition. IEEE, The United States
11. Wang H, Wang Y, Zhou Z, Ji X, Gong D, Zhou J, Li Z, Liu W (2018) Cosface: large margin cosine loss for deep face recognition. IEEE, The United States
12. Deng J, Guo J, Xue N, Zafeiriou S (2019) Arcface: additive angular margin loss for deep face recognition. IEEE, The United States

13. Kemelmacher-Shlizerman I, Seitz SM, Miller D, Brossard E (2016) The megaface benchmark: 1 million faces for recognition at scale. IEEE, The United States
14. National Institute of Standards and Technology (NIST) (2020) Face Recognition Vendor Test (FRVT) [EB/OL]. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt
15. Huang R, Zhang S, Li T, He R (2017) Beyond face rotation: global and local perception gan for photorealistic and identity preserving frontal view synthesis. IEEE, The United States
16. Liu Y, Li Q, Sun Z (2019) Attribute-aware face aging with wavelet-based generative adversarial networks. IEEE, The United States
17. Daugman J (1993) High confidence visual recognition of persons by a test of statistical independence. IEEE Trans Pattern Anal Mach Intell 15:1148–1161
18. He Z, Tan T, Sun Z, Qiu X (2009) Toward accurate and fast iris segmentation for iris biometrics. IEEE Trans Pattern Anal Mach Intell 31(9):1670–1684
19. Proenca H (2010) Iris recognition: on the segmentation of degraded images acquired in the visible wavelength. IEEE Trans Pattern Anal Mach Intell 32(8):1502–1516
20. Tan CW, Kumar A (2012) Unified framework for automated iris segmentation using distantly acquired face images. IEEE Trans Image Process 21(9):4068–4079
21. Ma L, Tan T, Wang Y, Zhang D (2003) Personal identification based on iris texture analysis. IEEE Trans Pattern Anal Mach Intell 15(11):1148–1161
22. Thornton J, Savvides M, Kumar V (2007) A bayesian approach to deformed pattern matching of iris images. IEEE Trans Pattern Anal Mach Intell 29(4):596–606
23. Sun Z, Tan T (2009) Ordinal measures for iris recognition. IEEE Trans Pattern Anal Mach Intell 31(12):2211–2226
24. Liu N, Zhang M, Li H, Sun Z, Tan T (2016) DeepIris: learning pairwise filter bank for heterogeneous iris verification. Pattern Recogn Lett 82(2):154–161
25. Sun Z, Zhang H, Tan T, Wang J (2014) Iris image classification based on hierarchical visual codebook. IEEE Trans Pattern Anal Mach Intell 36(6):1120–1133
26. Liu N, Liu J, Sun Z, Tan T (2017) A Code-level approach to heterogeneous iris recognition. IEEE Trans Inf Forensics Secur 12(10):2373–2386
27. Sun Z, Wang L, Tan T (2014) Ordinal feature selection for iris and palmprint recognition. IEEE Trans Image Process 23(9):3922–3934
28. Liu N, Li H, Zhang M, Liu J, Sun Z, Tan T (2016) Accurate iris segmentation in non-cooperative environments using fully convolutional networks. IEEE, The United States
29. Zhang Qi, Li H, Sun Z, Tan T (2018) Deep feature fusion for iris and periocular biometrics on mobile devices. IEEE Trans Inf Forensics Secur 13(11):2897–2912
30. Marco T, Guerrieri R (1997) A 390 dpi Live Fingerprint Imager based on Feedback Capacitive Sensing scheme. IEEE, The United States
31. Galbally J, Bostrom G, Beslay L (2017) Full 3D touchless fingerprint recognition: sensor, database and baseline performance. IEEE, The United States
32. Lawrence O, Nickerson JV (1988) Matched filter design for fingerprint image enhancement. IEEE, The United States
33. Dabouei A, Kazemi H, Iranmanesh S, Dawson J, Nasrabadi N (2018) Fingerprint distortion rectification using deep convolutional neural networks. IEEE, The United States
34. Roy A, Memon N, Ross A (2017) Masterprint: exploring the vulnerability of partial fingerprint-based authentication systems. IEEE Trans Inf Forensics Secur 12(9):2013–2025
35. Komeili M, Armanfard N, Hatzinakos D (2018) Liveness detection and automatic template updating using fusion of ECG and fingerprint. IEEE Trans Inf Forensics Secur 13(7):1810–1822
36. Park E, Cui X, Nguyen T, Kim H (2019) Presentation attack detection using a tiny fully convolutional network. IEEE Trans Inf Forensics Secur 14(11):3016–3025
37. Boyd JE, Little JJ (2005) Biometric gait recognition. Springer, Switzerland
38. Niyogi SA, Adelson EH (1994) Analyzing and recognizing walking figures in xyt. IEEE, The United States
39. Little J, Boyd J (1998) Recognizing people by their gait: the shape of motion. Videre: J Comput Vis Rese 1(2):1–32.

40. Huang P, Harris C, Nixon M (1999) recognizing humans by gait via parametric canonical space. Artif Intell Eng 13(4):359–366
41. Wang L, Tan T, Hu W, Ning H (2003) Automatic gait recognition based on statistical shape analysis. IEEE Trans Image Process 12(9):1120–1131
42. Cuntoor N, Kale A, Chellappa R (2003) Combining multiple evidences for gait recognition. IEEE, The United States
43. Han J, Bhanu B (2006) Individual recognition using gait energy image. IEEE Trans Pattern Anal Mach Intell 28(2):316–322
44. Lam TH, Cheung KH, Liu JN (2011) Gait flow image: a silhouette-based gait representation for human identification. Pattern Recogn 44(4):973–987
45. Kastaniotis D, Theodorakopoulos I, Theoharatos C, Economou G, Fotopoulos S (2015) A Framework for gait-based recognition using kinect. Pattern Recogn Lett 68(2):327–335
46. Wu Z, Huang Y, Wang L, Wang X, Tan T (2017) A comprehensive study on cross-view gait based human identification with deep CNNs. IEEE Trans Pattern Anal Mach Intell 39(2):209–226
47. Wu Z, Huang Y, Wang L (2015) Learning representative deep features for image set analysis. IEEE Trans Multimedia 17(11):1960–1968
48. Zhou Y, Kumar A (2011) Human identification using palm-vein images. IEEE Trans Inf Forensics Secur 6(4):1259–1274.
49. Kumar A, Ravikanth C (2009) Personal authentication using finger knuckle surface. IEEE Trans Inf Forensics Secur 4(1):98–110
50. Yan P, Bowyer KW (2007) Biometric recognition using 3D ear shape. IEEE Trans Pattern Anal Mach Intell 29(8):1297–1308
51. Marcel S, Millan JDR (2007) Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. IEEE Trans Pattern Anal Mach Intell 29(4):743–752
52. Rigas I, Komogortsev OV (2014) Biometric recognition via probabilistic spatial projection of eye movement trajectories in dynamic visual environments. IEEE Trans Inf Forensics Secur 9(10):1743–1754
53. Frank M, Biedert R et al (2013) Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans Inf Forensics Secur 8(1):136–148
54. http://www.xinhuanet.com/fortune/2019-01/02/c_1123938779.htm

Zhenan Sun received the B.E. degree in industrial automation from the Dalian University of Technology, China, in 1999, the M.S. degree in system engineering from the Huazhong University of Science and Technology, China, in 2002, and the Ph.D. degree in pattern recognition and intelligent systems from the Institute of Automation, Chinese Academy of Sciences, China, in 2006. He is currently a Professor with the Center for Research on Intelligent Perception and Computing, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, and also with the School of Artificial Intelligence, University of Chinese Academy of Sciences, China. He has authored/coauthored over 200 technical papers. His research interests include biometrics, pattern recognition, and computer vision. He is the Chair of Technical Committee on Biometrics, International Association for Pattern Recognition (IAPR) and an IAPR fellow. He serves as an Associate Editor for the IEEE Transactions on Biometrics, Behavior, and Identity Science.