A Review of Recent Advances in Identity Identification Technology Based on Biological Features

Jianan Tang[1], Pengfei Xu[1], Weike Nie[1](✉), Yi Zhang[2], and Ruyi Liu[3]

[1] School of Information Science and Technology, Northwest University,
Xi'an, China
weikenie@163.com

[2] School of Electronic and Information Engineering, Xi'an Jiaotong University,
Xi'an, China

[3] School of Computer Science and Technology, Xidian University, Xi'an, China

Abstract. With the development of social informatization technology, the problems of individual information security are becoming serious. Nowadays identity identification has been required essentially in government and business field. In this paper, we summarize and analyze the identification principles and identification methods based on biometrics, including the present researches fingerprint, palmprint, iris, human face, vein, gait and signature, and make comparative analysis of the differences of the error recognition rate, stability, acquisition difficulty and counterfeiting degree. Finally, the prospects of biometric recognition technologies are discussed additionally.

Keywords: Biometric recognition · Identity authentication · Fingerprint
Palmprint · Face · Vein

1 Introduction

Identity is the basis of individual life in the society. It is not only a sign of the difference among individuals, but also it gives individuals a lot of social attributes. The generalized identity identification refers to the individual identity by means of ID card and fingerprint. In the Internet field, identity authentication refers to the process of confirming the identity of the operator in the computer network system. The problems of personal identification can be divided into two categories: Verification and Recognition. Verification refers to verifying that the user is the identity he/she claims. Recognition refers to determining the specific identity of the user.

Personal verification or identification is an important part of the information security field, which greatly affects the privacy of individuals. With the rapid development of all kinds of information technology, modern life has put forward higher requirements for the practicability and reliability of user identification. For traditional authentication methods, such as passwords and passwords, authentication is theoretically relatively safe as long as the password strength is high enough. However, because people's memory is limited, the chosen password is usually not so complicated, so that

Z. Xu et al. (Eds.): Big Data 2018, CCIS 945, pp. 178–195, 2018.
https://doi.org/10.1007/978-981-13-2922-7_12

people can log in again. Although this method is convenient, it is easily stolen by others. Once the intruder breaks the security line, it is easy to get the user's information.

An actual biometric system should: (1) Achieve acceptable recognition accuracy and speed with reasonable resource requirements; (2) Be harmless to people and be accepted by people; (3) For various types of fraud, the method has sufficient robustness. Biometrics is the most convenient and secure authentication technology. It does not need to remember complex passwords, and does not need to carry keys, smart cards and the like. Biometrics recognizes people themselves, which directly determines that this type of certification is safer and more convenient. Because each person's biometrics have uniqueness different from others and constant stability within a certain period of time, it is not easy to forge and counterfeit. Therefore, biometric identification technology is used for identity identification, which is safe, reliable and accurate. In addition, biometric technology products are realized by means of modern computer technology, and it is easy to integrate with computers and security, monitoring, and management systems to achieve automated management.

Biometrics provide a more reliable and efficient way to authenticate. Specifically, each person has a unique physical feature or behavior that can be automatically measured or identified, called a biological feature, which can be divided into physiological features (such as fingerprints, facial images, irises, palm prints, etc.) and behavioral features (such as gait, sound, handwriting, etc.). Biological characteristics are relatively stable over a period of time, so they do not disappear and are difficult to forge. So far, various biometric technologies [1] have been developed for many years.

At present, biometrics has three main application directions in life: 1. As an important means of criminal investigation and identification; 2. To meet the needs of enterprise security and management. For example, physical access control, logical access control, attendance, patrol and other systems have fully introduced biometric technology; 3. self-service government services, immigration management, financial services, e-commerce, information security (personal privacy protection).

The development potential of biometric applications is mainly reflected in the following aspects: First, there are many sources of human identity information and a large amount of data. Whether it is static management or dynamic control, identity is the primary factor. Second, with the development of economic globalization, large factories can use automatic identity authentication instead of manual labor to manage. In addition, economic globalization has a more direct impact on the need for frequent personal identification. The prevalence of biometric authentication in e-commerce and e-government is also the best solution at this stage for the foreseeable future.

In this paper, the authors conducted a comprehensive analysis of current biometric-based recognition methods. Compared to existing articles on biometric identification methods, our differences lie in the detailed description of various biometric methods and the summary of some improved algorithms in recent years. In addition, the results of 3D technology and the rapid development of deep learning networks in the field of identity identification are briefly introduced (Fig. 1).

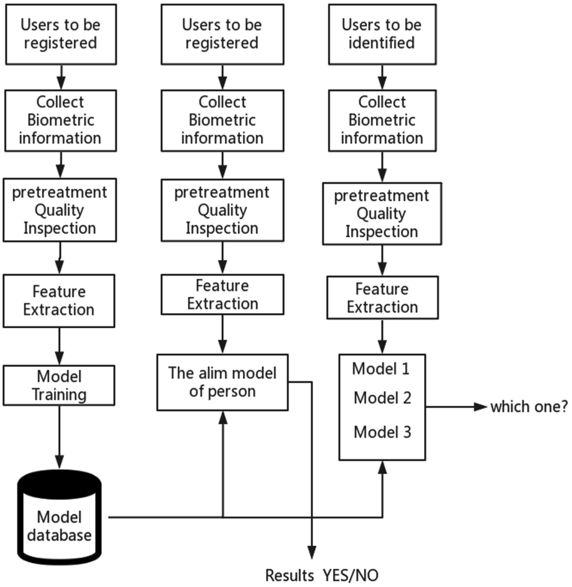

Fig. 1. The process of verification/recognition

2 Biometric Feature Recognition Technology

2.1 Fingerprint Recognition

Fingerprint recognition is one of the most widely used biometric technologies. Fingerprints have two important characteristics: uniqueness and stability [2, 3]. Almost no two fingerprints are identical. Galton first estimated the unique level of fingerprints as 1.45×10^{-11}, which provides a theoretical basis for a series of fingerprint identification studies [4]. At the same time, the characteristics of each fingerprint from birth, its shape may remain unchanged for life, unless it is seriously affected or diseased.

The whole process of fingerprint recognition technology is divided into four steps: fingerprint acquisition, fingerprint preprocessing, feature extraction and fingerprint matching. The development of fingerprint collection has gone through the original ink printing stage. Most existing fingerprint identification systems are equipped with contact-based two-dimensional sensors, such as China's second-generation ID card and optical fingerprint collector for company attendance. Solid-state fingerprint sensors installed on mobile electronic devices, including fingerprint smart phones and other mobile electronic devices. With the rapid development of 3D scanning and reconstruction technology, non-contact 3D fingerprint reconstruction and recognition technology is used to solve the shortcomings of contact-based 2D fingerprint recognition system and improve recognition accuracy [5].

Fingerprint preprocessing and feature extraction are important components of fingerprint recognition. After processing the fingerprint image by denoising and refining, the original fingerprint image is converted into a refinement map of the pixel range. The task of feature extraction is to extract the main feature points of the fingerprint in the refinement graph, including two singular points (center point and triangle point) and two points (bifurcation point and end point) with higher probability of occurrence. In addition, we need to match the directional field distribution around each point [6] and the type of feature points. This information will be built into the feature vector and stored in the data (Fig. 2).

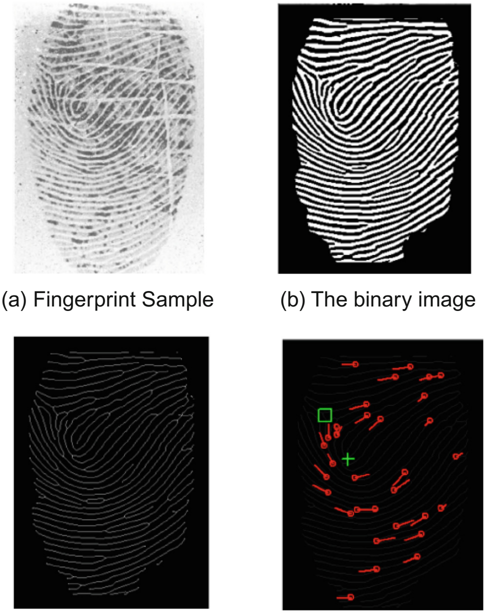
(a) Fingerprint Sample
(b) The binary image
(c) Detail of image
(d) Singular point

Fig. 2. The process of fingerprint recognition

Fingerprint matching is a pattern recognition process based on fingerprint pattern classification. At present, there are three different types of recognition methods according to the selected feature types: 1. Detailed feature recognition method [7], in which the details of the fingerprint information are extracted and detailed feature vectors are constructed to match. This method requires high quality images and a certain amount of feature information. Finally, the threshold is used to determine whether the collected fingerprints are from the same finger; 2. The structural pattern recognition method [8], which pays more attention to the overall distribution of fingerprints, including the pattern. This method can better resist noise, but the description of the fingerprint is rough and cannot be unique. 3. The method of combining the structure mode and the detail mode first narrows the matching range according to the classification of the fingerprint, thereby reducing the matching time and improving the matching efficiency. However, since the current fingerprint classification method is not highly accurate, the failure rate of this method is also high.

At present, in view of the great success of the CNN method, Lin et al. [9] proposed to develop a non-contact 3D fingerprint identification method to solve the limitations of the existing method by integrating the 3D fingerprint information of the side view. By integrating the 3D fingerprint information of the side view and the top view with the corresponding 3D contour map, the depth feature representation of the global shape and texture information can be enriched.

2.2 Palmprint Recognition

Palmprint recognition has many special advantages. Palm prints have a larger area and richer information than fingerprints. A high-performance palmprint recognition system can be built using only lower resolution acquisition devices.

The main features of the palm print include the main line, folds, triangle points and detail points. All of the above features can be extracted in a high-resolution palmprint image, while for low-resolution images, only mainline features and wrinkle features (collectively referred to as line features) can be extracted. The process of palmprint recognition is similar to fingerprint recognition, which mainly includes the acquisition of palmprint images, the preprocessing of palmprint images and feature extraction, and the matching of palmprint images.

The pretreatment of palm prints is mainly carried out in three aspects. First, due to the uncertainty of the position of the palm, it is necessary to maintain all images in a substantially uniform position and orientation with varying degrees of translation and rotation. Second, palmprint images mostly contain images of some or all of the fingers, but palmprint image recognition focuses only on the central region of the palm, so we need to segment the palmprint image and extract and normalize the central region of the palmprint image. In addition, due to the different sizes of the palms, it is necessary to standardize the images.

Palmprint feature extraction methods can be divided into four categories: 1. Structure-based feature extraction: Extracting line features and point features; 2. Feature extraction based on time-space domain transform: Transforming the original space palmprint image into the frequency domain and defining several feature vectors in the frequency domain, which can reflect the texture in the palmprint density and depth. 3. Statistical feature extraction: Redefine the original image with a stochastic model composed of statistical features; 4. Subspace-based feature extraction: Convert the image into a low-dimensional vector or matrix. The palm print is represented and matched in a low dimensional space.

The basic idea of Do Gcode [10] proposed by WU.XQ is to use the reciprocal of Gaussian function as the horizontal and vertical filter of the image. Then we use the Do G code as the extracted feature. When matching, the approximate degree of the image is determined by calculating the distance between the Hamming images. Compared with 2D image feature matching, 3D palm print is more favorable. In [11], the l1 norm or l2 norm regularized 3D palmprint recognition based on the cooperative representation (CR) framework is proposed.

2.3 Face Recognition

Face recognition technology, as a technique based on physiological feature recognition in the field of biometric recognition, extracts facial features by computer and performs identity verification based on these features.

At present, face recognition research mainly includes five aspects: (1) face detection: finding the coordinates of the face and the area occupied by the face in different situations; (2) face representation: extracting the facial features of the person Determine the detected face and the existing face description in the database. (3) Face matching. The object to be tested is compared with the existing face image of the database, and the result is obtained. The key to this step is to select the appropriate face expression method and matching algorithm. (4) Facial table analysis. The computer analyzes and understands the meaning of the person's emotions by recognizing the expression of the face and face. (5) Physiological classification: A careful analysis of the physiological characteristics of the human face, and information about the gender, age, race, occupation, etc. of the person.

Common algorithms for face recognition include: (1) Face recognition based on geometric features first proposed by Bledsoe [12]. The facial feature vectors (such as eye, nose, mouth position coordinates, and width distance) are obtained by recognizing the relative distance between the face feature points of the face. Find the best matching faces by performing vector comparisons. (2) Identification based on feature faces. The subspace pattern is formed by extracting statistical features of the face. The principal component analysis method is mainly used for orthogonal transformation. (3) Face recognition based on template matching requires a face template of some different standard samples to be given in advance. First, a global range search is performed on the face to be measured, and the similarity between the faces of the target person is compared according to the templates. It is judged whether the image window contains the target face by using the size of the image window. (4) The face recognition method based on Markov model is represented by the corresponding set of characteristic values for the five most important areas of the face (forehead, eyes, nose, mouth, and chin). (5) Face recognition based on elastic matching method is an algorithm based on dynamic link structure. It uses the sparse degree of the lattice to represent the facial image. The feature vector mark is obtained by the representation node in the sparse graph by performing Gabor wavelet decomposition on the image position, and the edge of the sparse graph is marked by the distance vector of the connected node. (6) The face recognition method based on neural network is currently popular, mainly using BP algorithm for face facial feature extraction. Through the learning process, we can get the invisible expression of the rules and rules of face recognition, which is more adaptable and the processing speed is very fast. With the further development of deep learning, it provides a new idea for the solution of the face recognition problem.

In 2014, Facebook proposed DeepFace [13], which uses convolutional neural networks and large-scale face images for face recognition. It achieves 97.35% accuracy on LFW, and performance is comparable to manual recognition. The VGG [14] network achieved a depth of 98.95% with a deep network topology and a large input image. The DeepId [15–18] network proposed by the Chinese University of Hong

Kong has made a series of improvements to the convolutional neural network. The accuracy is increased to 99% by combining local and global features, using joint Bayesian processing convolution features, and training using both identification and authentication information. With the expansion of the face data set, the face recognition accuracy has also been improved accordingly. In 2015, Google's FaceNet [19, 20] achieved an accuracy of 99.63%. It uses TripletLoss as its supervisory information and uses 200Mllion images for training. After that, Baidu even got an accuracy of 99.77% [21]. In addition, DCNN's network structure is getting bigger and deeper: VGGFace has 16 layers, FaceNet has 22 layers, 2015 ResNet [22] has reached 152 layers.

In view of the large amount of data required in face training, the literature [24] proposed the idea of artificially synthesizing a large amount of training data, and the face synthesis from three directions: perspective, shape, expression. Recently, different kinds of generation tasks can be completed by using Generative Adversarial Networks (GAN), which can generate real-life pictures. Google's new BEGAN model is used for face data sets, and the author focuses on image generation tasks. Even at even higher resolutions, new milestones in visual quality have been established. Deep learning can also achieve very good results on smaller data sets. Lightened CNN [23] uses a new activation function MFM function and uses a small network structure to achieve an accuracy of 98.13%. Caffe-Face achieved an accuracy of 99.28% using the Center Loss function.

With the development of science and technology, face automatic recognition technology has made great achievements, but it still faces difficulties in practical application. It not only requires accurate and rapid detection and segmentation of face parts, but also effective compensation, feature description and accurate classification effect. The following aspects need to be emphasized and improved: 1. The combination of local and global information can effectively describe the characteristics of human face, and the method based on hybrid model is worthy of further study. 2. Multi-feature fusion and multiple classifier fusion methods are also a means to improve recognition performance. 3. Because the human face is not rigid, the similarity between human faces and the influence of various factors lead to the difficulty of accurate face recognition. In order to meet the real-time requirements of automatic recognition, it is necessary to study the fusion method of face and fingerprint, iris and speech recognition technology. 4.3D deformation model can deal with many kinds of change factors and has a good development prospect. The method of simulation or compensation is adopted to achieve a better recognition effect. Three-dimensional face recognition algorithm is still being explored, which needs to be improved and innovated on the basis of traditional recognition algorithm. 5. Surface texture recognition algorithm is a kind of newest algorithm, which waits for us to continue to study.

In a word, face recognition is a challenging subject. It is difficult to achieve good recognition effect by using only one existing method. How to combine with other technologies, improve the recognition rate and speed, reduce the calculation amount, improve the robustness, adopt the embedded and hardware realization and practical is worth studying in the future.

2.4 Iris Recognition

The iris recognition performs the authentication or recognition of the user identity by extracting the texture features in the test iris image and comparing the feature with the feature template pre-stored by the user.

The pre-processing of the image includes positioning of the inner and outer boundaries of the iris, normalization and image enhancement, and denoising operations. Iris feature extraction uses texture extraction algorithm, such as the classical Gaobor filter method, to extract iris texture features from the uniformized normalized iris image, and performs binary coding to obtain a feature template composed of 0 and 1. Pattern matching can use a normalized Hamming distance to align feature templates of two iris images for identification (Fig. 3).

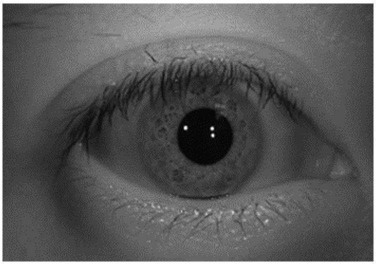

Fig. 3. CASIA iris database sample

The matching is mainly to separate and encode the texture features in the iris by performing pre-analysis, and then compare the obtained data with known samples in the database. According to the analysis similarity, it is diagnosed whether the two irises match, and thus the identity detection is realized. At present, iris-based identity checking methods are developing rapidly. The more classical algorithms are as follows: (1) Texture-based feature recognition algorithm. The most classic is the iris image of four different resolutions based on the Gauss-Laplace pyramid structure proposed by Wildes [25]. The iris was first analyzed and clustered using the Fisher linear criterion, and then the correlation between the iris images was compared; (2) Iris recognition method based on zero-crossing detection. The most representative method of iris recognition based on zero-crossing detection is the algorithm proposed by Boles [26] et al. The core idea uses four-scale wavelet to decompose the one-dimensional signal of the iris image, and then selects the zero-crossing point as the iris recognition standard. According to different two functions, the iris is further classified and matched to achieve identity detection; (3) Phase-based identification method. Daugman [27] 's iris recognition method is representative of the phase-based recognition method. Its core idea is to use a multi-scale Gabor filter to analyze the iris image. The features are separated and processed by phase encoding. Finally, iris matching is realized by Hamming distance. (4) Multi-channel Gabor filter bank and Daubechies-4 wavelet identification algorithm. The method is an iris recognition system independently developed by the Chinese Academy of Sciences. The core idea is to use multi-channel

Gabor filter filtering and two-dimensional wavelet transform for the iris image after normalization. In the feature matching stage, the variance reciprocal weighted Euclidean distance algorithm is used. The experiment proves that the method can obtain better identification results.

2.5 Retinal Identification

Retinal recognition is accomplished by extracting retinal vascular features and comparing them to pre-stored retinal data to confirm identity. The retina is composed of complex blood vessels distributed around the tiny nervous system at the back of the eyeball. It can remain unchanged for life without damage or disease. At the same time, it is also the most difficult system to be deceived, so retina recognition can be said to be one of the most reliable biometric technologies.

Retinal image acquisition is the first step in achieving retinal recognition. In a real environment, a professional fundus camera is generally used to scan a human retina to obtain a retinal image. The quality of the acquired image will affect the later recognition.

At present, methods for feature extraction of retinal blood vessels fall into two broad categories. One type is to extract the gray scale information of the retinal blood vessels and the characteristic information around the optic disc from the whole image, and the other is to extract the feature points from the shape of the blood vessel by the blood vessel segmentation and refinement.

With the research and development of retinal recognition technology, three matching methods are gradually formed: 1. Image-based matching method. Two typical methods: the American professor Rahman [28] proposed to use the overall gray information of the retinal blood vessel image and the statistical features around the optic disc to identify; Norwegian professor Ashokkumar [29] uses the visible spectrum for retinal recognition. The main disadvantage is that the structural characteristics of the blood vessels are neglected, resulting in insufficient matching accuracy. And the positioning of the disc itself becomes a problem. There is also a literature [30] that proposes the entire retinal vessel tree as a matching feature. 2. Node-based matching method. First, the blood vessels in the retinal image are segmented, and then nodes (cross points, bifurcation points) are selected from the segmented blood vessel network as feature points for one-to-one comparison. The advantage of this method is that the accuracy of the matching is higher, but the amount of calculation is relatively large. 3. Retinal vascular morphology recognition method based on structural features. Based on the fact that the mutual position between the nodes and the nodes is fixed, the matching feature of the retinal vascular structure is extracted by using the nearest neighbor triangle, which can effectively reduce the influence of image rotation and scaling.

2.6 Vein Recognition

Vein recognition uses the veins of the venous vessels to achieve identity authentication. Images are typically acquired using near infrared imaging.

Vein recognition mainly includes four stages: image acquisition, preprocessing, feature extraction and matching. For the acquisition of vein images with insufficient quality, the corresponding pre-processing techniques are needed for image localization and normalization. The extracted features mainly include vein grain features, texture features, minutiae features, and features obtained through learning. The grain features are a good representation of the topology of the entire vein network. Texture features are often expressed using local two-code values (gray value comparison), which are the bifurcation points, endpoints, etc. of the blood vessels. The features obtained through learning are the component features obtained by dimensional reduction after principal component analysis. The last step is matching. Matching refers to one of the basic technical aspects of vein recognition. In the case that a user registers multiple templates, a multi-template matching method is generally used to improve the matching precision, including a fuzzy fusion matching method of a three-valued template; matching method based on pixel matching rate, Hamming distance matching, and pixel non-matching rate fusion; a hierarchical strategy based on multiple templates.

In view of the problem that the finger vein image pixels are low and easy to extract errors during the extraction process, the literature [31] proposed the local binary pattern (LBP) and a local derivative pattern (LDP) algorithm for vein recognition. Rosdi et al. proposed using a new LBP algorithm local a line binary pattern (LLBP) for identification.

In 2016, Matsuda [32] evaluated a new method of finger vein authentication based on feature point matching. He proposed matching the feature points of irregular shadow and vein deformation, and extracting features using the curvature of the intensity image section. In order to increase the number of feature points, the points extracted from any position are non-linear. In addition, a finger shape model and a non-rigid matching method are proposed, which have a higher recognition success rate.

2.7 Gait Recognition

Gait characteristics are an emerging behavioral feature that mainly refers to people's habitual walking style. Gait characteristics are unique to everyone. Since each person has a different physiological structure and walking habits, it is difficult to find two identical gaits. Gait is the only feature of all current biometrics that is suitable for long-range observations at present.

A complete gait recognition system usually consists of three parts: gait contour extraction, gait feature extraction, and gait classification. The gait contour is extracted using motion detection algorithms to extract moving objects from gait video images. If there is more than one moving object in the video, you need to classify the moving targets. After the motion object is extracted, it needs to be filtered by noise and scaled to a standard size to obtain a gait contour. Gait features contain two important components: structured components and dynamic components. The structured component captures the individual's body shape, height, limb length, step size, etc. The dynamic component captures the motion characteristics of the human body during walking, such as the swinging of the arms, hips, and legs.

The current gait recognition methods can be roughly divided into two categories: one is a model-based approach. This type of method identifies individuals by modeling the anatomy and extracting image features to map the gait features into structural components of the model, or to derive motion trajectories from the human body. The other type is the non-model approach. This type of method acquires a compact representation of the motion characteristics by characterizing the entire motion pattern of the human body, so there is no need to consider the underlying structure of the human body. After the gait features are extracted, the classification algorithm classifies and identifies its features. The classification algorithms currently used in the field of gait recognition include neighborhood classification, support vector machine, hidden Markov model, multivariate discriminant analysis, linear discriminant analysis, tensor analysis, etc. In addition, principal component analysis is in gait. Identification is often used to preprocess feature matrices.

In the existing literature, there are many researches on the gait recognition algorithm of human body parameters. The literature [33] is based on the vibration model commonly used in physics to build a model of human body posture and shape, and uses self-learning algorithm to update in real time. In literature [34], based on the particle filter algorithm, the gait shape tracker is designed to realize the gait recognition and tracking algorithm based on the overall contour data of the step. The literature [33, 34] is a more representative gait recognition algorithm based on human contours.

2.8 Signature Recognition

Signature recognition is a technique for biometric recognition based on human behavior characteristics. It is a widely used biometric recognition technology. It can be divided into two modes according to the timing of the signature: offline mode (off-line) and online mode (on-line). Online signatures retain more valuable information. The movement speed, acceleration, pressure and other information of the nib make the recognition rate higher. For offline signature recognition, the written dynamic information is almost completely lost. It can only rely on the static information (handwriting features) of the signature image to reflect the signature writing style and habits, so identification is more difficult (Fig. 4).

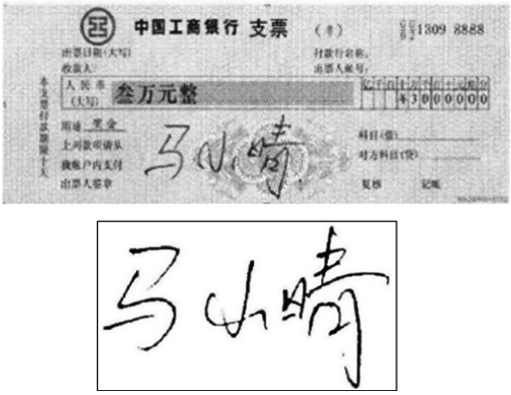

Fig. 4. Signature sample

Domestic and foreign scholars have gradually deepened and developed research on the field of signature recognition, and many new theories and methods have appeared in this field. Ferrer [35] proposed three kinds of gray feature fusions: Local binary pattern, Local directory pattern and Local derivative pattern. The LS-SVM was used for classification and identification, and verified on GPDS and MCYT databases. Kaur et al. [36] used the SURF algorithm on the pre-processed pictures and then classified them using HMM. Abdoli et al. [37] proposed a signature recognition system for feature extraction of Geodesic derivative pattern (GDP), which uses KNN as a classifier to compare feature vectors with each other. Shekar [38] applied Discrete Cosine Transform (DCT) to the binary image of the signature image, achieving a recognition rate of 92.74%. Vargas [39] uses the combination of gray level co-occurrence matrix and LBP, and uses SVM to identify. Wen [40] extracted the probability density function based on the structural distribution of the signature image and achieved good results. Azmi [41] proposed a signature verification system. The Freeman Chain Code (FCC) is used as the representation of the signature feature to extract a total of 47 dimensions, which is identified by the ANN classifier. Das [42] uses Gabor filtering technology to extract the topological features and statistical features of signature images, and forms the signature recognition system through the attribute reduction of rough set theory. Hatkar [43] extracted the geometric features of the image and used neural networks for classification and recognition.

As a deep learning method, DBN is a combination of multiple RBNs. The method solves the problem that the traditional neural network training method is not suitable for the training of the multi-layer network, and shows certain advantages in the field of handwritten digit recognition. By preprocessing the signature image and eliminating the interference, the local binary pattern (LBP) texture features of the handwritten signature image are extracted and used as the input of the DBN to construct the deep belief network model. It can automatically learn different levels of abstract features from the bottom up, and finally obtain a structural description of the signature image features, and classify at the top.

2.9 Other Biometric Feature Recognition Techniques

Biometrics technology is far more than the above mentioned, and more biometrics technologies have been proposed to meet the market needs of different fields. Each biometric identification technology has certain advantages over other biometric identification technologies in its application field, because no biometric identification technology can meet all real security requirements.

1. Non-contact recognition method

The characteristics of the human ear are unique, including shape, earlobe, skeletal structure, size, and the like. Therefore, ear shape recognition is also a non-contact biometric technology. With the popularity of computer technology, the use of keyboards has become the basic skill of work. Keyboard built-in sensors capture keystroke dynamics for authentication. When he or she frequently uses the keyboard, the user's identity can be authenticated by detecting the speed, pressure, time, and time the user clicks on each keystroke.

Voiceprint recognition converts a sound signal into an electrical signal that is then recognized by a computer. The voice spectrum of any two people is different. The acoustic characteristics of each person's voice are relatively stable but easy to change. This change may come from physical, pathological, psychological, etc., but it is also related to environmental disturbances. However, because each person's pronunciation is different, people can still distinguish the voice of different people or judge whether it is the voice of the same person.

2. The identification based on medical technology

Gene identification identifies a particular human identity by using a gene fragment having biological characteristics on the DNA sequence. The identification device is costly, the recognition algorithm is complex, and the identification method is difficult to implement quickly. It is now only used for a few specific applications.

In addition, the researchers found that everyone's heart is not exactly the same. It can be identified by ECG differences. Each value in the ECG wave has a profound meaning. These values change when a heart attack changes, but the sub-mode in which the value is shared with the value does not change. Because different hearts correspond to different ECGs, we can use this feature for identity authentication. However, the ECG acquisition process is more complicated than other methods, and the equipment requirements are higher. A non-contact heartbeat method has been successfully developed that uses radar remote scanning to analyze the shape and size of the heart and its geometric features, such as fluctuations in heart recognition.

There is also a method of identifying through the skin. The identity of a person is identified by illuminating infrared light into a small piece of skin to measure the wavelength of the reflected light. The theoretical basis is that each human skin with different skin thickness and subcutaneous layer has its own special mark. Because of the personality and specificity of the skin, cortex and different structures, these reflect light of different wavelengths. This method requires less computing ability.

3 The Comprehensive Comparison and Analysis of Several Biometric Identification Techniques

Each biometric technology has its own characteristics. In general, recognition techniques based on physiological logic features require near-end acquisition. Its stability is generally safer and more reliable than behavior-based identification techniques. But because it requires near-end collection, it is often inconvenient to use in remote authentication situations, and there is a risk of being easily imitated. However, behavioral characteristics are not easily imitated. We compared the advantages and disadvantages of each of the above biological features. These advantages and disadvantages determine their application in different fields, and also put forward new requirements for future research and development.

Fingerprint functionality is usually unique. The greater the number of features, the higher the accuracy of fingerprint recognition. On the one hand, current fingerprint readers are not expensive and can be scanned very quickly. However, because of the need to artificially limit fingerprint acquisition data, the location of each constraint is not exactly the same. Differences in focus can also lead to varying degrees of distortion, which makes high-precision fingerprint recognition not meet the original requirements; on the other hand, fingerprints are often used for criminal records, which makes some people afraid to “record” fingerprints.

The advantage of face recognition lies in its nature and the characteristics that are not easy to be detected by the participants. Humans usually confirm each other’s identities according to their faces. The human face has the similarity of structure. Even for different individuals, the structure is still very similar. This characteristic is advantageous to the localization human face, but is disadvantageous to the human face distinction. The shape of the human face is also very unstable. The change of facial expression is very easy to change the character of face, and the image difference of face is larger in different observation angle. In addition, face recognition is also susceptible to illumination conditions, human face cover and other factors.

Iris recognition is probably the most reliable biometric feature recognition technology, but the iris image acquisition equipment needs expensive camera equipment and the size of the equipment is very difficult to be miniaturized. In practical applications, the camera may produce image distortion. The iris images obtained in the darker environment are often of poor quality and cannot complete the recognition task.

Voice-print recognition does not involve user privacy issues, so the user acceptance is higher. On the one hand, the acquisition of voice print is the most convenient. A microphone or phone and mobile phone can collect user voice feature information and complete identity authentication. The complexity of the voice-print recognition algorithm is low. With some other measures, such as content identification through speech recognition, the accuracy rate can be improved. These advantages make the application of voice recognition more and more favored by system developers and users. The Voice-print recognition technology is based on the speaker’s invariance, but the same person’s sound is susceptible to age, mood, physical condition and so on, resulting in lower recognition performance. In addition, different microphones and channels have varying degrees of influence on recognition performance. The environment noise and the mixed speaker situation also have great influence.

The signature recognition technology also has the characteristic which is easy to be accepted by the populace. As people’s experiences and habits change, so does the way they sign up. The electronic signature board used for signature recognition is complex and expensive, and it is very different from the touchpad on the notebook, so it is difficult to be a remote identity authentication technology on the Internet. At the same time, the current physical and material technology is also difficult to the electronic signature board miniaturization.

The 2 key metrics for measuring biometric performance are False Rejection Rate (FRR) and false Accept Rate (FAR). FRR refers to mistaking a test sample from a real person for a rate of rejection by the impostor, while far refers to the ratio of mistaking a test sample from a pseudo person to a real man (Table 1).

Table 1. The comprehensive comparison and analysis of several biometric identification techniques

The methods of identity recognition	False Accept Rate (FAR)	False Rejection Rate (FRR)	Stability	The degree of counterfeiting
Fingerprint recognition	Very low	Very low	General	General
Palmprint recognition	Low	5%	General	General
Face recognition	0.5%	<0.2%	General	General
Iris recognition	Very low	10%	All the same for life	Extremely difficult
Retinal recognition	<0.0001%	<0.1%	All the same for life	Extremely difficult
Vein recognition	<0.0001%	<0.01%	All the same for life	Extremely difficult
Gait recognition	Unknown	Unknown	Unstable	General
Voice recognition	Low	Low	Unstable	Difficult
Signature recognition	Low	10%	Unstable	General

4 Summary and Prospect

This article reviews current research and applications of biometrics such as facial, voiceprint, fingerprint, palm print, iris, retina, gait, vein and signature. The characteristics and safety of biometrics are compared and discussed. The application of biometric technology in different fields is summarized.

Due to its unique advantages, biometric technology has shown great application prospects. At present, fingerprint recognition has been basically popularized. In the near future, biometrics will move toward high security, portability, non-contact and low cost. Face recognition and vein recognition have shown great advantages. With the development of science and technology, the cost of 3D face recognition and vein recognition will become smaller and smaller, gradually replacing other biometric methods.

Identity technology is an important technology in the government and business sectors. Biometric technology has the advantages of traditional certificate and key authentication technologies. However, a single biometric system is not reliable in the application field. A powerful biometric fusion recognition system is the research direction. The maturity of this technology will bring about great changes in the economy and society.

In the future, there is no doubt that the application of this technology will have a profound impact on our future economic and social life.

References

1. Glossary of Key Information Security Terms. Diane Publishing, Collingdale (2011)
2. Wang, Y., Hu, J.: Global ridge orientation modeling for partial fingerprint identification. IEEE Trans. Pattern Anal. Mach. Intell. **33**(1), 72–87 (2011)
3. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer, London (2009). https://doi.org/10.1007/978-1-84882-254-2
4. Pankanti, S., Prabhakar, S., Jain, A.K.: On the individuality of fingerprints. IEEE Trans. PAMl **24**(8), 1010–1025 (2002)
5. Kumar, A.: Contactless 3D Fingerprint Identification. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-319-67681-4
6. Zhang, L.: Extraction of direction features in fingerprint image. Appl. Mech. Mater. **518**, 316–319 (2014). Trans Tech Publications
7. Maio, D., Maltoni, D.: Direct gray-scale minutiae detection in fingerprints. IEEE Trans. Pattern Anal. Mach. Intell. **19**, 27–40 (1997)
8. Hrechak, A.K., McHugh, J.A.: Automated fingerprint recognition using structural matching. Pattern Recognit. **23**(8), 893–904 (1990). 27–40
9. Lin, C., Kumar, A.: Contactless and partial 3D fingerprint recognition using multi-view deep representation. Pattern Recognit. **83**, 314–327 (2018)
10. Wu, X., Wang, K., Zhang, D.: Palmprint texture analysis using derivative of Gaussian filters. In: 2006 International Conference on Computational Intelligence and Security, vol. 1, pp. 751–754. IEEE (2006)
11. Li, W., Zhang, D., Zhang, L.: Three dimensional palmprint recognition. In: Proceedings of IEEE International Conference on Systems, Man, and Cybernetics, October 2009, pp. 4847–4852 (2009)
12. Chan, H., Bledsoe, W.W.: A man-machine facial recognition system: some preliminary results. Panoramic Research Inc., Palo Alto, CA, USA1965 (1965)
13. Taigman, Y., Yang, M., Ranzato, M.A., et al.: DeepFace: closing the gap to human-level performance in face verification. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1701–1708 (2014)
14. Parkhi, O.M., Vedaldi, A., Zisserman, A.: Deep face recognition. In: BMVC, vol. 1, no. 3, p. 6 (2015)
15. Sun, Y., Wang, X., Tang, X.: Deep learning face representation from predicting 10,000 classes. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1891–1898 (2014)
16. Sun, Y., Chen, Y., Wang, X., et al.: Deep learning face representation by joint identification-verification. In: Advances in Neural Information Processing Systems, pp. 1988–1996 (2014)
17. Sun, Y., Liang, D., Wang, X., et al.: DeepID3: face recognition with very deep neural networks. arXiv preprint arXiv:1502.00873 (2015)
18. Sun, Y., Wang, X., Tang, X.: Deeply learned face representations are sparse, selective, and robust. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2892–2900 (2015)
19. Schroff, F., Kalenichenko, D., Philbin, J.: FaceNet: a unified embedding for face recognition and clustering. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 815–823 (2015)
20. Szegedy, C., Liu, W., Jia, Y., et al.: Going deeper with convolutions. In: CVPR (2015)
21. Liu, J., Deng, Y., Bai, T., et al.: Targeting ultimate accuracy: face recognition via deep embedding. arXiv preprint arXiv:1506.07310 (2015)

22. He, K., Zhang, X., Ren, S., et al.: Deep residual learning for image recognition. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 770–778 (2016)
23. Wu, X., He, R., Sun, Z.: A lightened cnn for deep face representation. In: 2015 IEEE Conference on IEEE Computer Vision and Pattern Recognition (CVPR), p. 4 (2015)
24. Wen, Y., Zhang, K., Li, Z., Qiao, Y.: A discriminative feature learning approach for deep face recognition. In: Leibe, B., Matas, J., Sebe, N., Welling, M. (eds.) ECCV 2016. LNCS, vol. 9911, pp. 499–515. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-46478-7_31
25. Wildes, R.: A system for automated iris recognition. In: Proceedings of the Second IEEE Workshop on Application of Computer Vision, pp. 121–128 (1994)
26. Boles, W.W., Boashash, B.: A human identification technique using images of the iris and wavelet transform. IEEE Trans. Signal Process. **46**(4), 1185–1188 (1998)
27. Daugman, J.: High confidence recognition of person by rapid video analysis of iris texture. In: Proceedings of European Convention on Security and Detection, pp. 244–251 (1995)
28. Rahman, N.A., Mohamed, A.S., Rasmy, M.E.: Retinal identification. In: Biomedical Engineering Conference. CIBEC 2008. Cairo International, pp. 1–4. IEEE (2008)
29. Borgen, H., Bours, P., Wolthusen, S.D.: Visible-spectrum biometric retina recognition. In: IIHMSP 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing 2008, pp. 1056–1062. IEEE (2008)
30. Mariño, C., Penedo, M.G., Penas, M., et al.: Personal authentication using digital retinal images. Pattern Anal. Appl. **9**(1), 21 (2006)
31. Lee, E.C., Jung, H., Kim, D.: New finger biometric method using near infrared imaging. Sensors **11**(3), 2319–2333 (2011)
32. Matsuda, Y., Miura, N., Nagasaka, A., et al.: Finger-vein authentication based on deformation-tolerant feature-point matching. Mach. Vis. Appl. **27**(2), 237–250 (2016)
33. Hu, H.: Enhanced gabor feature based classification using a regularized locally tensor discriminant model for multiview gait recognition. IEEE Trans. Circuits Syst. Video Technol. **23**(7), 1274–1286 (2013)
34. Lee, H., Baek, J., Kim, E.: A probabilistic image-weighting scheme for robust silhouette-based gait recognition. Multimed. Tools Appl. **70**(3), 1399–1419 (2014)
35. Ferrer, M.A., Vargas, J.F., Morales, A., et al.: Robustness of offline signature verification based on gray level features. IEEE Trans. Inf. Forensics Secur. **7**(3), 966–977 (2012)
36. Kaur, R., Choudhary, P.: Offline signature verification in Punjabi based on SURF features and critical point matching using HMM. Int. J. Comput. Appl. **111**(16), 4–11 (2015)
37. Abdoli, S., Hajati, F.: Offline signature verification using geodesic derivative pattern. In: 2014 22nd Iranian Conference on Electrical Engineering (ICEE) IEEE (2014)
38. Shekar, B.H., Bharathi, R.K.: DCT-SVM-based technique for off-line signature verification. In: Sridhar, V., Sheshadri, H., Padma, M. (eds.) Emerging Research in Electronics, Computer Science and Technology. LNEE, vol. 248, pp. 843–853. Springer, New Delhi (2014). https://doi.org/10.1007/978-81-322-1157-0_85
39. Vargas, J.F., et al.: Off-line signature verification based on grey level information using texture features. Pattern Recognit. **44**(2), 375–385 (2011)
40. Wen, J., Chen, M., Ren, J.: Off-line signature verification based on local structural pattern distribution features. In: Li, S., Liu, C., Wang, Y. (eds.) CCPR 2014. CCIS, vol. 484, pp. 499–507. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45643-9_53
41. Azmi, A.N., Nasien, D.: Freeman chain code (FCC) representation in signature fraud detection based on nearest neighbour and artificial neural network (ANN) classifiers. Int. J. Image Process. (IJIP) **8**(6), 434 (2014)

42. Das, S., Roy, A.: Signature verification using rough set theory based feature selection. In: Behera, H.S., Mohapatra, D.P. (eds.) Computational Intelligence in Data Mining—Volume 2. AISC, vol. 411, pp. 153–161. Springer, New Delhi (2016). https://doi.org/10.1007/978-81-322-2731-1_14
43. Hatkar, P.V., Salokhe, B.T., Malgave, A.A.: Off-line hand written signature verification using neural network. Methodology **2**(1), 1–5 (2015)