2021 IEEE 6th International Conference on Smart Cloud (SmartCloud) | 978-1-6654-4374-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/SMARTCLOUD52277.2021.00027

Deep Learning in Automatic Fingerprint Identification

Chunsheng Wu
Cyber Space Defense Department
Beijing Police College
Beijing, China
wuchunsheng@bjpc.edu.cn

Honghao Wu
Cyber Space Defense Department
Beijing Police College
Beijing, China
wuhonghao@bjpc.edu.cn

Song Lei
Cyber Space Defense Department
Beijing Police College
Beijing, China
songlei@bjpc.edu.cn

Xiaojun Li
Institute of Forensic Science, MPS
Beijing, China
com.cn.li@163.com

Hui Tong*
Cyber Space Defense Department
Beijing Police College
Beijing, China
tonghui@bjpc.edu.cn

***Abstract*—The development of fingerprint identification as a computer application technology is closely related to the new technology of computer science. The artificial intelligence technology, especially the image technology based on deep learning, has opened a new mode of fingerprint identification algorithm. In this paper, we divide the development of artificial intelligence in fingerprint field into three stages, and analyze the development trend of the second stage. The fingerprint identification technology based on deep learning uses image features instead of traditional minutiae feature, which changes the cognition of fingerprint recognition in the field of forensic science. This study investigate the application mode and typical methods of deep learning technology in fingerprint identification, give the technical schemes based on deep learning, and put forward several key technologies such as image processing and dimensionality reduction. The existing DNN models that can be used for fingerprint identification are introduced, such as convolutional neural network and auto-encoder network. The results show that the performance of artificial intelligence fingerprint identification algorithm is better than the traditional algorithm in many indicators.**

Keywords*—*deep learning, artificial intelligence, fingerprint identification, non-minutiae matching, AFIS

I. Introduction

Fingerprint is one of the biological characteristics of human body and widely used because of its uniqueness, easy access [1]. *Automatic Fingerprint Identification System* (AFIS) has been widely used in forensic science. The idea of automatic fingerprint identification algorithm based on minutiae feature points comes from the artificial fingerprint identification method [2]. This method relies on the extraction of fingerprint minutiae feature points, which is well solved by the research of pattern recognition technology and a series of derivative methods, and then the similarity of two fingerprints is calculated according to the maximum matching degree between the two minutiae point sets [3].

In recent years, with the significant advance in computer facility [4-5], software [6-7], big data [8-9], and cloud techniques [10-11], the fingerprint database capacity grows rapidly. The traditional fingerprint identification technology has encountered a bottleneck. At the same time, artificial intelligence technology represented by deep learning technology began to emerge in the field of fingerprint identification.

II. Artificial intelligence technology

Artificial Intelligence (AI) and big data technologies are widely used in many fields such as image recognition [12], health care [13-14], transportation [15], and finance [16-17] areas. AI and big data enhanced cybersecurity is an emerging new area. M. Qiu et al. had done significant works in this area [18-20]. His group had proposed a novel dynamic scalable blockchain based communication architecture for *Internet of Things* (IoT) [21] and privacy-aware adaptive data encryption strategy of big data in cloud computing [22].

Fingerprint identification technology is a specific application of artificial intelligence in the field of image recognition. In recent years, many institutions have carried out research on the application of artificial intelligence in automatic fingerprint recognition [23-24]. According to the general rules of the emergence and development of various technologies in the computer field, we divide the development of fingerprint identification technology based on artificial intelligence into three stages.

A. Initial stage

With the emergence of new artificial intelligence technology and the improvement of computer performance, the best way is to directly apply the existing mature technologies in the field of fingerprint identification. For example, the mature classification network and even portrait recognition technology are used for fingerprint classification and recognition [25-27]. The initial performance of new algorithm is poor because of lack of specific measures to improve. Only experiments can determine the effectiveness of a method.

978-1-6654-4374-6/21/$31.00 ©2021 IEEE
DOI 10.1109/SmartCloud52277.2021.00027

At this stage, artificial intelligence technology only carry out image quality processing, feature extraction and simple classification, which can be used as a supplement to traditional algorithms.

B. *Development stage*

On the basis of simple application, the technical method is improved according to the characteristics of fingerprint. Both the selection of training data and the construction of network structure reflect the characteristics of fingerprint. For example, the size of convolution window is set up according to the average width of fingerprint ridge, which can greatly improve the effectiveness of sampling [28]. The new algorithm can meet the demand of general applications and is complementary to the traditional algorithm based on minutiae points. The traditional and new algorithms can be applied in parallel in an AFIS to realize the complementarity and achieve the optimal performance of comprehensive application [29-30].

C. *Surpassing stage*

At this stage, the new algorithm greatly exceeds the traditional algorithm in the accuracy and speed of recognition, and the new system can completely replace the original system. The fingerprint experts are still required to participate in the final identification, but the workload is remarkably reduced. The new algorithms based on the combination of fingerprint image characteristics, basic theory of artificial intelligence and existing technical methods, will explain various performance problems of the algorithms. At present, we are in the transition period from the first stage to the second stage. The most commonly used technology of artificial intelligence in the field of image recognition is deep learning. Compared with the past neural networks, the main feature of the current depth neural network is that it has greater depth and dimension, that is, the number of network layers and the number of nodes per layer, which can realize the feature extraction of high-resolution images.

III. Application of deep learning technology in fingerprint identification

In the field of fingerprint, with the advantages of deep neural network in feature learning and extraction of high-resolution image, we can apply deep learning technology to feature recognition, feature compression and feature matching of fingerprint image. The design rule of fingerprint identification algorithm has been changed by the application of deep learning technology. Deep learning for fingerprint identification is based on image features rather than traditional minutiae points. These features constitute feature vectors, through which we can compute the similarity between fingerprint images.

A. *Construction of feature vector for fingerprint image*

The extraction and matching of fingerprint minutiae points is the key objective and standard of performance evaluation in the traditional fingerprint identification algorithm. Now, multi-scale and multi-morphological image features can be obtained from the whole fingerprint image after multiple transformations and dimensionality reduction of the image through depth learning method. The feature vector is constructed according to the image features. In order to ensure sufficient information, the fingerprint feature vector should usually be more than 100. Different from the minutiae points, the features extracted by DNN are compressed image features, and each feature cannot directly see the content it expresses. DNN has inherent technical advantages for image regions without feature points or image regions where minutiae points are difficult to locate. Taking the training fingerprint pattern classification network as an example, the construction steps of feature vector are:

- Create fingerprint training samples, verification samples and test samples.
- The structure of classification depth neural network is designed, and the network is constructed and initialized.
- The training samples are used to train the classification network, the network automatically adjusts its parameters through the loss function, and the verification samples are used to verify the accuracy.
- When the network training converges to meet the accuracy requirements, the test samples are used to test the classification performance of the network.

B. *Basic scheme of fingerprint identification based on deep learning*

The basic scheme of deep learning for fingerprint identification is to reduce the dimension of high-resolution fingerprint images for many times and map and transform them with neural network to obtain the feature vector of the image. The similarity of the two fingerprints is obtained by computing the spatial distance of the feature vectors of the two fingerprints. The application process is shown in Fig. 1. The main steps are as follows:

1) Design of neural network model. The structure of deep neural network is defined according to the needs of application. It mainly includes the design of input and output data dimensions at the beginning and end of the network, the number of network layers, the structure adopted by each layer, the type of network optimizer and so on. The basic network structure for fingerprint image is usually composed of several convolution layers, pooling layers and multiple full connection layers.

2) *Preparation of training data.* According to the input and output design of the network model, the data are divided into training data and verification data, and then selected to train and verify the network. The principle of data selection should be typicality and representativeness, and data are sufficient and well-distribution. For supervised learning mode, all data should be labeled. For example, the existing pattern category should be marked on the trained

fingerprint image during recognization of fingerprint pattern, and the images containing minutiae points should be marked when minutiae points are extracted. For unsupervised learning, the data are often grouped or classified. For example, when training fingerprint matching, the different data belonging to the same finger should be placed in the same group firstly.

3) Model training and Optimization. the training of neural network model is to input enough sample data to the network and adjust the structure of the network through optimization algorithm (mainly adjusting the weight of each node in the network) to make the output of the network consistent with the expected value. Training often requires a large number of cyclic iterations and lasts for a long time. The verification data shall be used to check whether it meets the expectation for a certain number of cycles. For the network that does not converge and fails to meet the expectations, the network parameters should be adjusted in time.

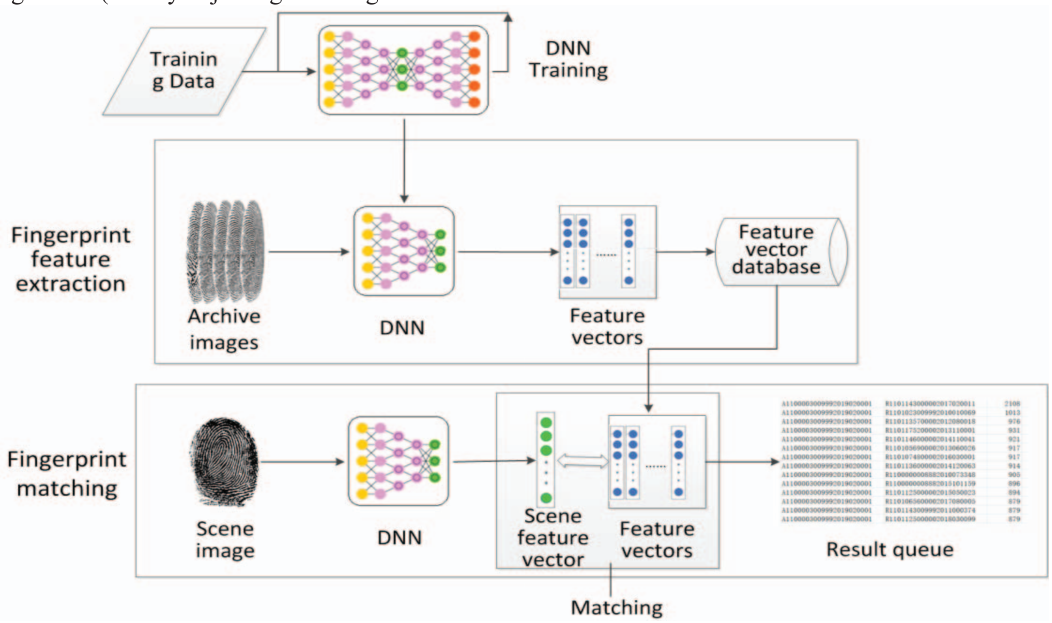

Fig. 1. Scheme of fingerprint identification based on deep learning

4) Extraction and storage of feature vectors. The main computation of deep learning focuses on the spatial mapping and transformation of images, while the computation of similarity between feature vectors is very small. When the network training meets the expectation, we save the node vector value of the last full connection layer in the network as the feature vector obtained by fingerprint conversion. As the abstract characteristics expression of the fingerprint, the feature vector can be directly used for similarity computation between fingerprints.

C. Key Technologies

Different model design or combination methods should be used for different requirements and application modes in the development process. For example, Training data and network model will be different in scene-archive mode and archive-archive mode. However, no matter which application mode, the following key technical links will be involved.

1) Image preprocessing. Deep neural network can directly reduce the dimension and extract the feature of fingerprint image. The experimental results are often good. As in the traditional way, it becomes an optional step to preprocess the fingerprint image. The advantage of preprocessing is that it can greatly reduce the image noise, equalize the image gray and obtain the effective area of fingerprint. The disadvantage is that some inherent features will disappear in the image. These features do not need attention in minutiae point extraction, but they are very important in deep learning.

2) Depth of network model. The more layers of the deep neural network, the more essential features of the image can be extracted. The visual features of the image can be easily extracted by the shallow network. Both have their own emphasis on the ability of image recognition. The local detail morphology often be expressed in the shallow network and the overall characteristics of the image are easier to learn when the number of layers is large. For example, it is not suitable to use deep network for the recognition of minutiae point, and it is recommended to use a network with more layers for fingerprint-pattern recognition.

3) Image dimensionality reduction. The police fingerprint image is collected with high resolution, usually 500 DPI [31]. There is multi-scale information in high-resolution images. For example, the spacing of fingerprint lines is generally 5-9 pixels. The convolution window should be designed according to the spacing of lines to judge the direction field. Most of minutiae points can be identified in a region of 3×3 to 7×7 pixels. The dimension of high-resolution image is far beyond the acceptable dimension of storage and matching, so it is necessary to reduce the dimension of image effectively. Usually, we use several convolution computations to reduce the dimension in order to achieve the required dimension.

4) The dimension of the feature vector. The content of feature vector is related to the network structure. The output of each layer of the deep neural network is the input to the next layer as a new feature. In practice, parameters of one-dimensional nodes of the last full connection layer in the network are often extracted as the final feature vector. Too long vectors will degrade the performance of the system, while too short feature vector will affect the accuracy. It can be set to about 1024 according to the empirical value at the initial stage. However, with the progress of research, we find that lower order feature vectors can also better express fingerprints.

D. Examples of common basic network models

1) Convolutional neural network

Convolutional neural network is the most popular deep neural network in image recognition in recent years. It can realize a series of functions such as dimension reduction, noise reduction and classification for the fingerprint image. Convolution operation is essentially a compression technology. Through convolution calculation, the dimension of fingerprint image can be effectively reduced and the large image can be gradually reduced to a small image [32-33].

2) Auto-encoder

For unsupervised deep learning, the same fingerprint image can be used as input and output data at the same time. We let the image make its own label. Such a network model is called auto-encoder. The goal of training the auto-encoder is to compress and encode the fingerprint image through the coding network, obtain the compressed feature expression, and then reverse compute and restore the original image through the decoding network. This shows that the node parameters of the middle layer can express the fingerprint image well. That is, it can be used as the feature vector of fingerprint [34-35].

3) Convolutional auto-encoder

The combination of convolutional neural network and auto-encoder is called convolutional auto-encoder, which is a specific implementation method of auto-encoder. If the output fingerprint is transformed, the network can also learn the potential law of transformation [36]. For example, we take the thinning image of fingerprint as the reconstructed image, and the deep neural network can be trained to realize the thinning image of fingerprint, as shown in Fig. 2.

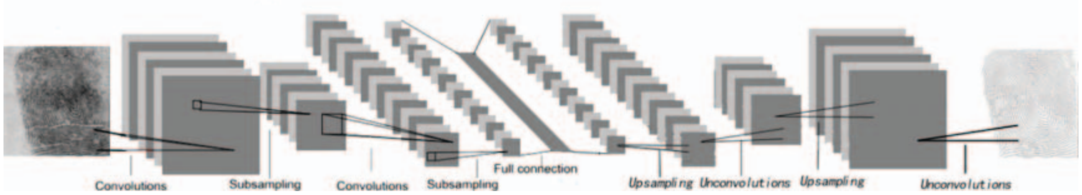

Fig. 2. Schematic for convolutional auto-encoder

IV. PERFORMANCE TEST AND COMPARISON OF AFIS

Since 2016, many research institutions around the world have carried out research on automatic fingerprint identification technology based on artificial intelligence. Of course, there are more enterprises involved. At present, few products have been formed. We give the performance test of a core algorithm of AFIS (recorded as system A) based on artificial intelligence technology in this chapter. Then, we compare it with the test results of several traditional AFIS products (recorded as system B, system C, system D and system E).

A. Performance test of system A

1) scene-archive test

We select the test data from the police fingerprint database, because the amount of data in the standard fingerprint database is small. After the fingerprint experts checked and confirmed one by one, we sorted out 6227 pairs of scene-archive fingerprints.

The selected archive fingerprints are randomly mixed with the archive fingerprint database of 5 million people. We use the algorithm of system A to match the selected scene fingerprints in the archive fingerprint database one by one. There are 4231 correct matching results in the top 200 of each candidate queue, accounting for 67.9%. If the correct result does not appear in the top 200 of a candidate queue, it is regarded as missing matching, accounting for 32.1%. See Table I for the test result.

2) *archive-archive test*

We extracted archival fingerprint data for testing from the fingerprint database of a police department, including 10000 group archive fingerprints with matched results and 10000 archival fingerprints without matched results. After further check, 20 archive fingerprints were found invalid, 10640 people had matched data (called positive data) in this database, 9340 people had no matched data (called negative data). A total of 19980 people's fingerprints were used as test data. The data is mixed into the former fingerprint database of 5 million people and do archive-archive test in system A. A total of 9281 archive fingerprints were declared to match other archives. The result is shown in Table II.

TABLE I. TEST DATA OF SCENE-ARCHIVE FINGERPRINT BY AI ALGORITHM (SYSTEM A)

Ranking of matching	**amount**	**proportion**	**Correct rate**
1	1490	35.22%	23.93%
2-3	1055	24.94%	16.94%
4-5	370	8.75%	5.94%
6-10	340	8.04%	5.46%
11-20	252	5.96%	4.05%
21-30	128	3.03%	2.06%
31-200	596	14.09%	9.57%

TABLE II. TEST DATA OF ARCHIVE-ARCHIVE FINGERPRINT BY AI ALGORITHM (SYSTEM A)

Statistical items	**Amount of positive data 10640**	**Amount of negative data 9340**	**Total 19980**
Amount of matched	9159	122	9281
Rate of matched quantity	86.1%(Detection rate)	1.3%(Error recognition rate)	Correct rate 92.34%
Amount of unmatched	1481	—	—
Rate of unmatched amount	13.9%(Missing recognition rate)	—	—

TABLE III. COMPARISON FOR TEST DATA OF SCENE-ARCHIVED FINGERPRINT AMONG MULTIPLE ALGORITHMS

Name	**Amount of tasks**	**Amount of tasks completed**	**Correct amount**	**Rate of correct**	**Rate of return**	**Ranking 1st**	**Rate of ranking 1st**	**Top 10**	**Rate of top 10**
System A	6227	6227	4231	67.9%	100%	1490	23.93%	3255	52.27%
System B	6496	6130	4052	66.10%	94.37%	668	10.90%	3275	53.43%
System C	6496	6314	3006	47.61%	97.20%	515	8.16%	2134	33.80%
System D	6496	5790	1761	30.41%	89.13%	395	6.82%	1367	23.61%
System E	6496	6478	4147	64.02%	99.72%	687	10.61%	3209	49.54%

TABLE IV. COMPARISON FOR TEST DATA OF ARCHIVE-ARCHIVED FINGERPRINT AMONG MULTIPLE ALGORITHMS

Name	**Missing recognition rate**	**Error recognition rate**
System A	7.41%	0.61%
System B	3.34%	0.00%
System C	5.86%	0.00%
System D	27.58%	0.46%
System E	4.07%	0.02%

System A declared that 9281 archive had repeat archive data among the 19980 archive fingerprint data. After manual verification by experts, correct results were 9159 and another 1481 were missing. Of 9340 people who had no matched data, 122 were wrong matched. Thus, the rates of detection, error recognition and missing recognition can be calculated. The correct ratio is the comprehensive ratio of the detection rate and error recognition rate. The correct ratio = ((detection rate) + (100% - error recognition rate)) / 2 = (86.1 + (100-1.3)) / 2 = 92.34%. The error ratio is the probability of error number in the total fingerprints. The error ratio = the number of error declaration / total = 122 / 19980 = 0.61%; The miss ratio is the probability that missing number in the total fingerprints. The miss ratio is the number of miss declaration / total = 1481 / 19980 = 7.41%.

B. *Performance comparison*

For several mainstream AFIS products in China, we used the same data for scene-archive test and archive-archive test. Since system B, C, D and E are based on manual marking of scene minutiae points, there are two or more marking methods for some scene fingerprints. Each marking method is submitted as a separate task. Therefore, the total number of tasks will exceed 6227 to 6496. The results are shown in Table III and table IV.

V. CONCLUSION

With the increase of fingerprint database capacity and the development of automatic identification technology, it is an inevitable trend for new technology to replace the old technology. In the field of pattern recognition and image processing, the artificial intelligence technology represented by deep learning has made a lot of remarkable achievements, which greatly promotes the technical progress and application development. Recently, the artificial intelligence algorithm has appeared and its performance is better than the traditional algorithm in many indicators. Along with the increasing demands of fingerprint application and the progress of artificial intelligence technology, the technology of fingerprint automatic identification will continue to develop and improve.

REFERENCES

[1] A. K. Jain, A. A. Ross, K. Nandakumer. Introduction to biometrics [M]. Springer, 2011.

[2] C. Christophe. Fingerprints and other ridge skin impressions [M]. Yaping Luo, Trans. Beijing: Chinese people's Public Security University Press, 2016.

[3] X. Wang. Research and implementation of fingerprint identification algorithm [D]. Nanjing: Nanjing University of Science and Technology, 2004.

[4] Y. Guo, Q. Zhuge, et al., Optimal data allocation for scratch-pad memory on embedded multi-core systems, International Conference on Parallel Processing, 464-471, 2011

[5] M. Qiu, Z. Chen, M. Liu, Low-power low-latency data allocation for hybrid scratch-pad memory, IEEE Embedded Systems Letters 6 (4), 69-72, 2014

[6] L. Tao, S. Golikov, et al., "A reusable software component for integrated syntax and semantic validation for services computing," IEEE Symposium on Service-Oriented System Engineering, 127-132, 2015

[7] K. Zhang, J. Kong, M. Qiu, G. Song, "Multimedia layout adaptation through grammatical specifications," Multimedia Systems 10 (3), 245-260, 2005

[8] X. Tang, K. Li, et al., "A hierarchical reliability-driven scheduling algorithm in grid systems," Journal of Parallel and Distributed Computing 72 (4), 525-535, 2012

[9] R. Lu, X. Jin, S. Zhang, M. Qiu, X. Wu, A study on big knowledge and its engineering issues, IEEE Transactions on Knowledge and Data Engineering 31 (9), 1630-1644, 2018

[10] J. Li, M. Qiu, J. Niu, et al., "Feedback dynamic algorithms for preemptable job scheduling in cloud systems," IEEE/WIC/ACM conf. on Web Intelligence, 2010

[11] Z. Lu, N. Wang, et al., IoTDeM: An IoT Big Data-oriented MapReduce performance prediction extended model in multiple edge clouds, Journal of Parallel and Dist. Computing, Vol. 118, 316-327, 2018

[12] A. K. Jain, R. Bolle, S. Pankanti. Biometrics personal identification in networked society [M]. Springer, 2009.

[13] L. Qiu, K. Gai, M. Qiu, Optimal big data sharing approach for tele-health in cloud computing, IEEE SmartCloud conf., 184-189, 2016

[14] K. Gai, M. Qiu, L. Chen, M. Liu, "Electronic health record error prevention approach using ontology in big data," IEEE 17th HPCC conf., 2015

[15] H. Su, M. Qiu, H. Wang, "Secure wireless communication system for smart grid with rechargeable electric vehicles," IEEE Communications Magazine 50 (8), 62-68, 2012

[16] K. Gai, M. Qiu, B. Thuraisingham, L. Tao, "Proactive attribute-based secure data schema for mobile cloud in financial industry," IEEE 17th HPCC, 2015

[17] M. Qiu, D. Cao, H. Su, K. Gai, Data transfer minimization for financial derivative pricing using Monte Carlo simulation with GPU in 5G, Intl Journal of Communication Systems 29 (16), 2364-2374, 2016

[18] K. Gai, M. Qiu, S. Elnagdy, A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance, IEEE 2nd International Conference on Big Data Security on Cloud, 2016

[19] Z. Zhang, J. Wu, et al., "Jamming ACK attack to wireless networks and a mitigation approach," IEEE GLOBECOM conf., 1-5, 2008

[20] M. Qiu, Z. Ming, J. Li, J. Liu, G. Quan, Y. Zhu, "Informer homed routing fault tolerance mechanism for wireless sensor networks," J. of Systems Archi. 59 (4-5), 260-270, 2013

[21] H. Qiu, M. Qiu, G. Memmi, Z. Ming, M. Liu, "A dynamic scalable blockchain based communication architecture for IoT," Int'l Conference on Smart Blockchain, 159-166, 2018

[22] K. Gai, M. Qiu, H. Zhao, J. Xiong, "Privacy-aware adaptive data encryption strategy of big data in cloud computing," IEEE 3rd CSCloud conf., 2016

[23] D. Song, Y. Tang, J. Feng. Aggregating minutia-centered deep convolutional features for fingerprint indexing [J]. Pattern Recognition, 2019, 88: 397-408.

[24] L. Jiang. Fingerprint feature extraction algorithms based on deep convolutional neural networks [D]. Beijing: University of Chinese Academy of Sciences, 2016.

[25] D. Peralta, I. Triguero, S. Garcia On the use of convolutional neural networks for robust classification of multiple fingerprint captures [J]. International Journal of Intelligent System, 2018, 33(1): 213-230.

[26] Y. Zhang, T. Cao, S. Li. Parallel processing systems for big data: a survey[J]. Proceedings of the IEEE, 2016,104(11): 211-2136.

[27] J. J. Engelsma, K. Cao, A. K. Jain. Learning a fixed length fingerprint representation [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2019, 43(6): 1981-1997.

[28] D. L. Nguyen, K. Cao, A. K. Jain. Robust minutiae extractor: integrating deep networks and fingerprint domain knowledge [C]//International Conference on Biometrics (ICB), 2018.

[29] H. Chen, X. Li, Y. Zheng. Research on fingerprint recognition based on depth learning [J]. Intelligent Computer and Applications, 2018, 8(3): 64-69.

[30] S. Li, T. Ben, G. Nadiradze. Breaking (global) barriers in parallel stochastic optimization with wait-avoiding group averaging. IEEE Transactions on Parallel and Distributed Systems, 2020, 32(7): 1725-1739.

[31] Criminal Investigation Department of Ministry of Public Security of P.R.C. Technical Specification of Living Fingerprint Image Acquisition: GA/T 625-2010 [S]. Beijing, 2006.

[32] F. Zhou, L. Jin, J. Dong. Review of convolutional neural network [J]. Chinese Journal of Computers, 2017, 40(6): 1229-1251.

[33] C. Nebauer. Evaluation of convolutional neural networks for visual recognition [J]. IEEE Transactions on Neural Networks, 1998, 9(4): 685-696.

[34] Y. Wang, H. Yao, S. Zhao. Auto-encoder based dimensionality reduction [J]. Neuro-computing, 2016, 184: 232-242.

[35] L. Theis, W. Shi, A. Cunningham. Lossy image compression with compressive autoencoders [EB/OL]. (2017-03-01)[2021-03-14]. https://arxiv.org/abs/1703.00395.

[36] W. Luo, J. Li, J. Yang. Convolutional sparse autoencoders for image classification [J]. IEEE Transactions on Neural Networks and Learning Systems, 2017, 29(7): 3289-3294.