Face Database Security Information Verification Based on Recognition Technology

Shumin Xue

(Corresponding author: Shumin Xue)

School of Computer Science and technology, Baoji University of Arts and Sciences

No.42 mailbox, Baoji University of Arts and Sciences, Baoji, Shaanxi 721016, China

(Email: shuminx84@126.com)

(Received Aug. 21, 2018; revised and accepted Mar. 12, 2019; First Online June 1, 2019)

Abstract

In recent years, with the rapid development of the Internet, information can be transmitted more and more rapidly, and the issue of confidentiality and security has become increasingly important. Compared with traditional information verification methods, biometric identification is more secure and convenient. This study used the MATLAB software to carry out the simulation of information verification performance of face recognition algorithm based on Local Directional Pattern Algorithm (LDP) and Principal Component Analysis (PCA). The face image data were from ORL database. The results showed that the increase of the training set samples could raise the accuracy of security information verification of the two algorithms and took less time, and under the same number of training samples, the algorithm of face recognition based on PCA, compared with face recognition algorithm based on LDP, had higher accuracy and less time consuming. In conclusion, PCA-based face recognition algorithm is more suitable for security information verification.

Keywords: Face Recognition; Local Directional Pattern; ORL Face Database; Principal Component Analysis

1 Introduction

After entering the 21st century, the Internet has been widely used, and the speed of data transmission is getting faster and faster. At the same time, the security of information data [10] is becoming more and more serious. How to ensure the identification and authentication in the process of network communication has become an important problem in the development of the Internet communication [27]. The essential principle of the identity authentication system [3, 12, 18] is to associate an identifier with the identity of the user, which is identification feature identity, in order to achieve the recognition of the identity of the holder [13]. However, in traditional identification systems, identifiers and holders are independent from each other [4,6,14,25,27]. The system will recognize the holder of the identifier as the correct person once confirming the identifier and will not judge whether the person who holds the identifier is the real owner [5, 24, 26, 28]. Therefore, the new biometric recognition technologies [8, 15, 16] are applied to the identity authentication system.

Biometric features mainly refer to voiceprint, fingerprint, face and so on. These features are unique to individuals. Using biometric features as identifiers in identity authentication systems can solve the disadvantages of physical isolation between identifiers and holders in traditional systems, which is because that biometric and its holder is impossible to separate under normal circumstances. No additional account password is required for biometric applications and the certification system will be more convenient. Gilani [11] proposed a model-based 3D face recognition algorithm, and tested the performance of the algorithm with two large common 3D face data sets. The results showed that the method could effectively recognize face with posture and expression change, and the comparison of single data set and composite data set showed that the recognition accuracy decreased as the size of the image library increased.

In order to achieve robust to illumination, posture and facial expression change of unconstrained face recognition, Ding *et al.* [7] proposed a new methods that extracted “multiple layers of double direction patterns” from face image, and the experimental results on Face Recognition Technology (FERET), CAS - pose, expression, accessories, and lighting (PEAL) - R1, Face Recognition Grand Challenge 2.0 (FRGC 2.0) and Labeled Faces in Wild (LFW) database showed that the method in face recognition and face verification tasks were superior to the most advanced local descriptor. In order to establish the connection between Kinect and face recognition research, Rui *et al.* [21] proposed the first publicly available face database based on Kinect sensor, and used the standards of the proposed face recognition methods to benchmark the proposed database, and proved the performance gain by fractional fusion when depth data was integrated with Red, Green, Blue (RGB) data. In this study, MATLAB software was used to simulate the security information verification performance of two face recognition algorithms based on Local Directional Pattern Algorithm (LDP) and Principal Component Analysis (PCA).

2 Face Detection, Recognition and Matching

As shown in Figure 1, in the security information verification based on face recognition, first of all, the face image of the registrant is collected through the camera, and then face detection is carried out on the image to ensure that there is only face area in the image. Then, the eigenvectors of the image are extracted by the recognition algorithm. After that, information verification is carried out. The camera is used to collect and verify images, and then face detection is carried out on the verified images. Meanwhile, the non-face area is removed. Then, the same recognition algorithm is used to extract the eigenvectors of the verified images and the classifier is applied to compare the registered image and verify whether the eigenvectors of the image can be classified into one category. If they can, the people in the two images will be judged to be the same person, and pass the verification of information, and if not, they will be determined as different persons, and information validation will fail.

3 Face Recognition Algorithm Based on LDP

LDP [23] can extract image features, the principle of which is statistics of directional edge. X is a pixel in the image and will be centered on the pixel gray value in the field of 3×3 to have convolution with Kirsch template N [1] to get the corresponding edge response $|n_i|$, and then edge response will be sorted according to the gradient. The first K is denoted as code 1, and the rest of the record is denoted as code 0. There are 8 types of template N, including

$$N_0 = \begin{bmatrix} -3 & -3 & 5 \\ -3 & 0 & 5 \\ -3 & -3 & 5 \end{bmatrix}$$

$$N_1 = \begin{bmatrix} -3 & 5 & 5 \\ -3 & 0 & 5 \\ -3 & -3 & -3 \end{bmatrix}$$

$$N_2 = \begin{bmatrix} 5 & 5 & 5 \\ -3 & 0 & -3 \\ -3 & -3 & -3 \end{bmatrix}$$

$$N_3 = \begin{bmatrix} 5 & 5 & -3 \\ 5 & 0 & -3 \\ -3 & -3 & -3 \end{bmatrix}$$

$$N_4 = \begin{bmatrix} 5 & -3 & -3 \\ 5 & 0 & -3 \\ 5 & -3 & -3 \end{bmatrix}$$

$$N_5 = \begin{bmatrix} -3 & -3 & -3 \\ 5 & 0 & -3 \\ 5 & 5 & -3 \end{bmatrix}$$

$$N_6 = \begin{bmatrix} -3 & -3 & -3 \\ -3 & 0 & -3 \\ 5 & 5 & 5 \end{bmatrix}$$

$$N_7 = \begin{bmatrix} -3 & -3 & -3 \\ -3 & 0 & 5 \\ -3 & 5 & 5 \end{bmatrix}$$

The formula of LDP coding [2] is:

$$\left\{ \begin{array}{l} n_k = k_{th}(N) \\ N = |n_0, n_1, \cdots, n_7| \\ LDP_k(r,c) = \sum_{i=0}^{7} b_i(n_i - n_k) \times 2^i \\ b_i(n_i - n_k) = \left\{ \begin{array}{ll} 1 & n_i - n_k \geq 0 \\ 0 & n_i - n_k < 0 \end{array} \right\} \end{array} \right\} \tag{1}$$

where n_k is the edge response of K^{th}, N is Kirsch template, $LDP_R(r,c)$ is the LDP code corresponding to center point c, and r is the radius of the field which was set as 3 in this study.

As shown in Figure 2, each pixel in the original face image was converted into LDP code by combining 8 Kirsch templates and Equation (1), and then the LDP coded image of the face was constructed according to the LDP code. After that, the LDP coded image was divided into blocks of number $a \times b$ to extract histogram in each of them. Finally, the histogram of the extracted block was connected end to end to obtain the final eigenvector.

After obtaining the final eigenvector, the classifier was required to classify the collected eigenvector to determine whether the face image was the same face classification. Moreover, different face recognition algorithms had different vector classifiers, and the selection of classifier would directly impact on the recognition effect.

In this study, LDP recognition algorithm adopted nearest neighbor classifier [20] to classify eigenvectors, and distance function was applied to calculate the contiguous degree between samples. The formula of LDP recognition algorithm is as follows:

$$d_{\chi^2}(a,b) = \sum_n \frac{a_n^2 - 2a_n b_n + b_n^2}{a_n + b_n} \tag{2}$$

where a, b are LDP eigenvectors which are corresponding to two face images respectively, and $d_{\chi^2}(a,b)$ is the chi-square distance between the eigenvectors of two images.

4 Face Recognition Algorithm Based on PCA

The basic principle of PCA [19] is to transform the original random vector related to components into random

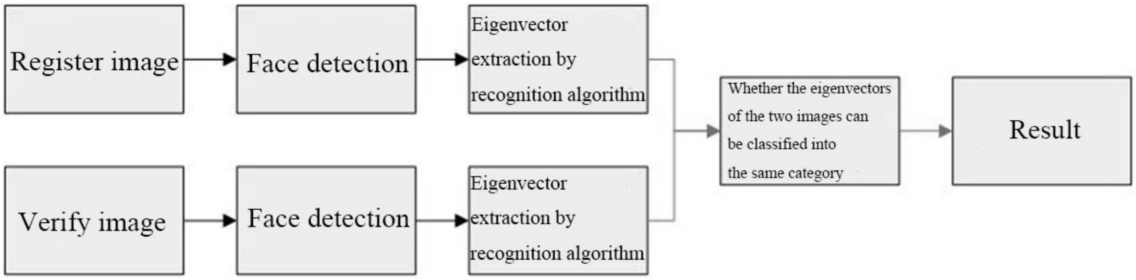
Register image
Face detection
Eigenvector extraction by recognition algorithm
Verify image
Face detection
Eigenvector extraction by recognition algorithm
Whether the eigenvectors of the two images can be classified into the same category
Result

Figure 1: Face detection, recognition and matching

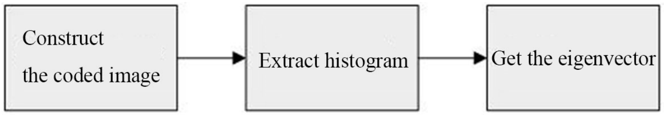

Figure 2: The extraction process of facial features of LDP

vector unrelated to components by means of orthogonal transformation, reduce the dimensionality of the transformed multidimensional variable system, and then transform the low-dimensional variable system into a one-dimensional system through value function. PCA is a statistical method of dimensionality reduction in mathematics, which can greatly reduce the amount of calculation and improve the efficiency of calculation.

The extraction process of eigenvectors based on PCA is as follows. First, it is necessary to calculate the mean vector of all images in the training sample. The calculation formula of the mean vector of all images [29] is as follows:

$$n = \frac{\sum_{i=1}^{Q} A_i}{Q} \tag{3}$$

where n is the mean vector of all training sample images, Q is the sum of training sample images, and A_i is the original eigenvector of the i^{th} training sample image.

Then, the original eigenvector mean value of the single face image in the training sample is calculated, and the calculation formula of the original eigenvector mean value of the single face image is as follows:

$$n_i = \frac{\sum_{j=1}^{L} A_{ij}}{L} \tag{4}$$

where n_i is the average value of the original eigenvector of the i^{th} person's face image, L is the number of training samples of the i^{th} person's face image, and A_{ij} is the original eigenvector of the j^{th} individual face image training sample of the i^{th} individual. Then the population dispersion matrix is calculated:

$$\left\{ \begin{array}{l} S_b = \frac{BB^T}{P} \\ B = [(n_0 - n), (n_1 - n), \cdots, (n_{P-1} - n)] \end{array} \right\} \tag{5}$$

where S_b is the total population scatter matrix, P is the sum of people trained, and B is the matrix of the difference between the vector mean of single face image and the vector mean of all training samples. Then the construction matrix is calculated:

$$\left\{ \begin{array}{l} R = B^T B \\ \sum_{i=1}^{t} \delta_i / \sum_{i=1}^{P} \delta_i \geq \theta \\ U_i = \frac{BN_i}{\sqrt{\delta_i}} \end{array} \right\} \tag{6}$$

where R is the construction matrix, δ_i is the eigenvalue of the i^{th} training sample, V_i is the orthonormalized eigenvector of the i^{th} training sample, and U_i is the orthonormalized eigenvectors of S_b.

To sum up, the projection of the average eigenvector of each person's training sample in the eigensubspace is $C_i = W^T m$, where C_i is the feature subspace for each person and W^T is the dimension reduction matrix.

After the dimensionality reduction of high-dimensional facial image eigenvectors by PCA, it is necessary to select an appropriate classifier to classify the collected eigenvectors. In this study, linear kernel function (SVM) classifier was selected to recognize the eigenvectors.

Firstly, the training data set of some feature space was selected, and then the optimization problem was constructed for the data set: the objective function was:

$$\left\{ \begin{array}{l} \min[\frac{\sum_{i=1}^{M} \sum_{j=1}^{M} \alpha_i \alpha_j y_i y_j (K(x,z) + \frac{\lambda_{ij}}{C})}{2} - \sum_{j=1}^{M} \alpha_j] \\ \lambda_{ij} = \left\{ \begin{array}{ll} 1 & i = j \\ 0 & i \neq j \end{array} \right\} \end{array} \right\} \tag{7}$$

The condition was:

$$\left\{ \begin{array}{l} \sum_{i=1}^{M} \alpha_i y_i = 0 \\ \alpha_i \geq 0 \end{array} \right\} \tag{8}$$

where $K(x, z)$ is kernel function, α is a parameter suitable for C and λ_{ij} is the parameter that determines whether or not $\frac{1}{C}$ exists.

Finally, the decision function was constructed:

$$\left\{ \begin{array}{l} b = y_j(1 - \frac{\alpha_j}{C}) - \sum_{i=1}^{M} \alpha_i y_i K(x, z) \\ 0 < \alpha_j < C \\ f(x) = sign(\sum_{i=1}^{N} \alpha_i y_i K(x, z + b)) \end{array} \right\} \tag{9}$$

where α_j is a positive component of α and b is a parameter involved in the decision.

5 Simulation Experiment

5.1 Experimental Environment

The experiments in this study were carried out on a laboratory server. The server configuration was Windows7 system, I7 processor and 16G memory. MATLAB software [9] was used for algorithm programming.

5.2 Experimental Data

This study adopted the data set of ORL face database [22] that contained 400 positive face images of people distributed in 40 folders which were corresponding to 40 people respectively. Each folder contained 10 positive face images of the same person with different expressions, and the image size was 112 × 92 pixels.

5.3 Experimental Settings

The experimental procedure of this study is shown in Figure 3. Firstly, the data set was divided into training set and test set. n face images were randomly selected from the folder corresponding to each person as the training set, and the rest as the test set. The selection of n was one, three and five. Then, the training set was used to train LDP recognition algorithm and PCA recognition algorithm respectively for face recognition where block parameters of 7×7 were selected when LDP image histogram was extracted from the LDP recognition algorithm. After extracting LDP eigenvectors, the nearest neighbor classifier was applied to classify features, so as to train LDP recognition algorithm; in the PCA recognition algorithm, the image was dimensionalized by PCA, the principal components of the 20-dimensional vector were obtained, and the SVM classifier classified them. The kernel function in the SVM was the linear kernel function. was set as 1, so as to train the PCA recognition algorithm. At last, the face images in the test set were detected and classified by two recognition algorithms respectively.

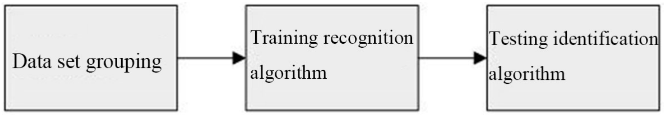
Data set grouping
Training recognition algorithm
Testing identification algorithm

Figure 3: Experimental flow

When the face image in the test set was classified to the corresponding person, it meant that it passed the security information verification. The correct number of test set of each person should be counted, and the accuracy of the two recognition algorithms through the security information verification should be calculated.

5.4 Experiment Results

As shown in Figure 4, when the number of training sets was one face image per person, the accuracy of security information verification of the LDP-based recognition algorithm was 68.45%, and that of the PCA-based recognition algorithm was 70.12%. When the number of training sets was three face images per person, the accuracy of the LDP based recognition algorithm was 78.15%, and that of the PCA-based recognition algorithm was 86.45%. When the number of training sets was five face images per person, the accuracy of the LDP based recognition algorithm was 88.54%, and that of the PCA-based recognition algorithm was 98.41%.

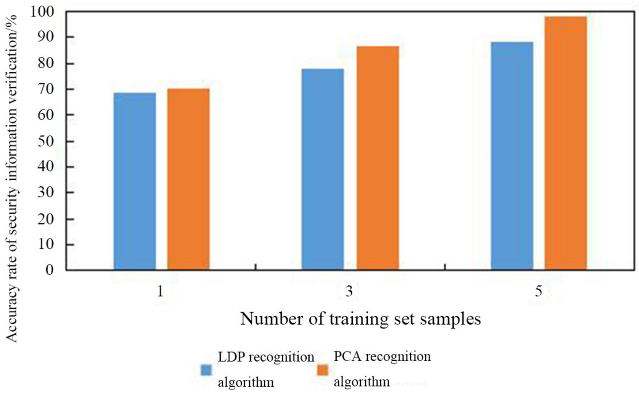

Figure 4: The accuracy rate of security information verification of the two algorithms

It could be seen from Figure 4 that with the increase of the sample number of the training set, the accuracy of the two recognition algorithms also increased. At the same time, with the same number of training samples, the accuracy of the PCA based recognition algorithm was higher than that of the LDP-based recognition algorithm.

As shown in Table 1, when the number of training samples was one face image per person, the security information verification of LDP algorithm took 366 ms, while that of PCA algorithm took 354 ms. When the number of training samples was three face images per person, the security information verification of LDP algorithm took 329 ms, while that of PCA algorithm took 321 ms. When the number of training samples was five face images per person, the security information verification of LDP algorithm took 315 ms, while that of PCA algorithm took 301ms. It could be seen that with the increase of training samples, the time required by the two recognition algorithms to verify the security information of the test set also decreased. At the same time, under the same number of training samples, the PCA recognition algorithm took less time.

6 Conclusion

This paper simply introduced face recognition algorithms based on LDP and PCA, and the MATLAB software information was used to simulate the security information verification performance of two face recognition al-

Table 1: Security information verification time of the two recognition algorithms

Training sample size	The time consumed by LDP algorithm/ms	The time consumed by PCA algorithm/ms
1	366	354
3	329	321
5	315	301

gorithms, the two algorithms were trained by training samples containing one face image per person, three face images per person and five images per person, and then the rest of the image was as a test set. When the training samples were 1, 3 and 5 per person, the accuracy rate of security information verification of LDP recognition algorithm was 68.45%, 78.15% and 88.54%, respectively. The accuracy rate of security information verification of PCA recognition algorithm was 70.12%, 86.45% and 98.41%, respectively. The accuracy of both algorithms increased with the increase of training samples, and the accuracy of PCA algorithm was higher. When the number of training samples was one, three and five per person, the security information verification of LDP recognition algorithm took 366 ms, 329 00 ms and 315 ms, while the security information verification of PCA recognition algorithm took 354 ms, 321 ms and 301 ms. The time of the two algorithms decreased with the increase of training samples, and the time of PCA algorithm was less.

References

[1] S. Chakraborty, S. K. Singh, P. Chakraborty, "Local directional gradient pattern: A local descriptor for face recognition," *Multimedia Tools & Applications*, vol. 76, no. 1, pp. 1201–1216, 2017.

[2] S. Chakraborty, S. K. Singh, P. Chakraborty, "Correction to: Local directional gradient pattern: A local descriptor for face recognition," *Multimedia Tools & Applications*, vol. 77, no. 15, pp. 20269, 2018.

[3] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol", *Computers & Mathematics with Applications*, vol. 49, pp. 703–714, 2005.

[4] T. Y. Chen, C. C. Lee, M. S. Hwang, J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, Nov. 2013.

[5] Y. C. Chen, W. L. Wang, M. S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection", in *The 9th International Conference on Advanced Communication Technology*, pp. 255–259, 2007.

[6] M. A. A. Dewan, E. Granger, G. L. Marcialis, *et al.*, "Adaptive appearance model tracking for still-to-video face recognition," *Pattern Recognition*, vol. 49(C), pp. 129–151, 2016.

[7] C. Ding, J. Choi, D. Tao, *et al.*, "Multi-directional multi-level dual-cross patterns for robust face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 38, no. 3, pp. 518–531, 2016.

[8] C. Ding, D. Tao, "A comprehensive survey on pose-invariant face recognition," *ACM Transactions on Intelligent Systems & Technology*, vol. 7, no. 3, 2016.

[9] A. Fathi, P. Alirezazadeh, F. Abdali-Mohammadi, "A new global-Gabor-Zernike feature descriptor and its application to face recognition," *Journal of Visual Communication & Image Representation*, vol. 38, pp. 65–72, 2016.

[10] J. Galbally, S. Marcel, J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2017.

[11] S. Z. Gilani, A. Mian, "Towards large-scale 3D face recognition," in em International Conference on Digital Image Computing: Techniques & Applications, 2016.

[12] M. S. Hwang, Li-Hua Li, "A New Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, Feb. 2000.

[13] M. S. Hwang, J. W. Lo, S. C. Lin, "An efficient user identification scheme based on ID-based cryptosystem", *Computer Standards & Interfaces*, vol. 26, no. 6, pp. 565–569, 2004.

[14] M. S. Hwang, C. H. Wei, C. Y. Lee, "Privacy and security requirements for RFID applications", *Journal of Computers*, vol. 20, no. 3, pp. 55–60, Oct. 2009.

[15] C. T. Li, M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 5, pp. 2181-2188, May 2010.

[16] C. T. Li, M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards", *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010.

[17] C. T. Li, M. S. Hwang, C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile Ad hoc networks," *Computer Communications*, vol. 31, no. 10, pp. 2534–2540, June 2008.

[18] H. Li, L. Zhang, H. Bing, *et al.*, "Sequential three-way decision and granulation for cost-sensitive face

recognition," *Knowledge-Based Systems*vol. 91(C), pp. 241–251, 2016.

[19] Y. Qiang, W. Rong, X. Yang, *et al.*, "Diagonal principal component analysis with non-greedy ℓ_1-norm maximization for face recognition," *Neurocomputing*, vol. 171, pp. 57–62, 2016.

[20] S. P. Ramalingam, "Dimensionality reduced local directional number pattern for face recognition," *Journal of Ambient Intelligence & Humanized Computing*, vol. 9, no. 1, pp. 1–9, 2016.

[21] M. Rui, N. Kose, J. L. Dugelay, "KinectFaceDB: A kinect database for face recognition," *IEEE Transactions on Systems Man & Cybernetics Systems*, vol. 44, no. 11, pp. 1534–1548, 2017.

[22] A. Soula, S. B. Said, R. Ksantini, *et al.* , "A novel kernelized face recognition system," in *4th International Conference on Control Engineering & Information Technology*, pp. 1–5, Hammamet, 2016.

[23] Srinivasa PerumalR.aChandra MouliP.V.S.S.R., "Dimensionality reduced local directional pattern (DR-LDP) for face recognition," *Expert Systems with Applications*, vol. 63, pp. 66–73, 2016.

[24] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.

[25] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "An authentication protocol for low-cost RFID tags", *International Journal of Mobile Communications*, vol. 9, no. 2, pp. 208–223, 2011.

[26] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "An improved authentication protocol for mobile agent device in RFID," *International Journal of Mobile Communications*, vol. 10, no. 5, pp. 508–520, 2012.

[27] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "Security analysis of an enhanced mobile agent device for RFID privacy protection," *IETE Technical Review*, vol. 32, no. 3, pp. 183–187, 2015.

[28] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.

[29] Z. Zhong, L. Shuang, "Coupled principal component analysis based face recognition in heterogeneous sensor networks," *Signal Processing*, vol. 126, pp. 134–140, 2016.

Biography

Xue Shumin, February 1984, master, lecturer, mainly engaged in computer applications, face recognition and database research. Presided over and completed two university-level key projects, presided over one university-level educational reform project, participated in two industrial key projects of baoji science and technology bureau, participated in one project of shaanxi provincial department of education, and participated in a number of university-level key and general projects. Guided the undergraduate innovation and entrepreneurship project "classroom attendance system based on face recognition", which was rated as a national innovation project; guided the student "Internet +" project "ZhenShiTong – campus intelligent management platform based on face recognition", published many papers, two patents and three software Copyrights.