Journal of Network Intelligence ©2019 ISSN 2414-8105 (Online)
Taiwan Ubiquitous Information Volume **4**, Number **4**, November **2019**

The Research of Identity Authentication Based on Multiple Biometrics Fusion in Complex Interactive Environment

Yingli Wang[1], Yan Liu[1],Hongbin Ma[1], Qitao Ma[2], Qun Ding[1]

[1]Electronic Engineering College of Heilongjiang University
Harbin, China
No.74 XueFu Road, NanGang, Harbin
mahongbin@hlju.edu.cn
[2]The Hong Kong Polytechnnic University
Hong Kong,China
No.11 Yucai Road, Hong Kong

Received July 2019; revised September 2019

Abstract. *To prevent internal employees to steal confidential data by counterfeiting the fingerprint and other biological information of the employees with high authority, to resist the replay attacks from the authentication systems outside, and to reduce the impact of environmental factors such as illumination and noise on the performance of the system in practical applications, an authentication method for complex interactive environments is proposed. The images feature of palmprint and palm veins can be extracted by an improved LBP algorithm; The images classification of palmprint and palm veins can be classified by the method of SVM multiple classification; and the final authentication result can be given by the D-S fusion strategy. After repeated experiments, the recognition rate of decision-level D-S fusion is 100%, which verifies that this method can solve the above problems and has obvious effects.*
Keywords: Complex interactive environment, Internal threat, Multiple biometrics D-S fusion, Multi-Block Multi-Filter LBP algorithm

1. **Introduction.** The vigorous development and improvement of social engineering provides criminals from the company s inside with a lot of methods to obtain the biometric (such as fingerprint, face, retina, palmprint, etc.) of employees who have access to high-level confidential data, and these criminals use forged biometrics to steal high-level confidential data which their permissions cannot be accessed, so that the existing authentication systems become unreliable. On the other hand, the feature acquisition and transmission equipment of the common biometric-based identity authentication system is in an environment where the electromagnetic signal is open, and it is easy for the monitoring equipment to steal the collected biometric data, making the identity authentication system suffer the replay attacks. Therefore, the identity authentication system based on a single biometric becomes no longer safe and reliable [1]. In addition, biometric capture devices are susceptible to environmental factors such as light, noise, etc., resulting in a reduction in the Correct Recognition Rate (CRR) of the identity authentication system in such complex acquisition environments.

In the complex network environment and social environment, the existing authentication scheme based on a single biometric identity is not very accurate and reliable. But,

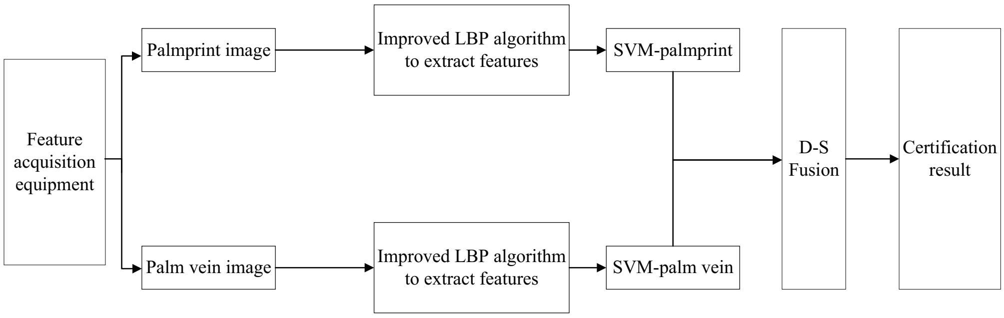

FIGURE 1. The Model of Multi-biometrics Fusion Authentication in Complex Interactive Environment

it is difficult for criminals to obtain a variety of biometric original data at the same time, so a new idea for solving the problem of reliability and accuracy of the biometric-based identity authentication system can be provided, which is use the information fusion solutions to solve the problems of reliability and accuracy caused by forged signature attacks, replay attacks, and environmental factors. In the existing feature fusion scheme, fusion is mainly performed at the following four levels: original data layer fusion, feature layer fusion, matching layer fusion, and decision layer fusion. It is very important to choose the reasonable biometrics and fusion strategies. It is the key to improve the identity authentication systems ability based on biometric of resist counterfeit feature attacks and replay attacks in a complex interactive environment, and to reduce the adverse effect from the environmental factors in practical applications such as illumination, noise, etc.

Based on the above issues, this paper researches the identity authentication method based on multi-biological feature fusion strategies for the complex interactive environment, and proposes an identity authentication method which can effectively prevent internal employees from posing as employees with high authority to access confidential data. This method is mainly aimed to reduce from the complex interactive environment of internal threats and external environment influences, based on SVM and DS evidence theory. Palmprint and palm veins is the authentication features in this method. The same acquisition equipment can collect palmprint and palm vein images with different wavelength light sources; the improved LBP algorithm can extract the features of the two images; the one-to-one SVM multi-classification method can classify different individuals; the DS fusion strategy at the decision-making level can improve the reliability and accuracy of the identity authentication system and resist the counterfeit feature attacks and replay attacks. The model of the method which we proposed can be described like the figure 1.

2. Improved LBP Algorithm for Complex Interactive Environments.

2.1. Reliable Biometric in Complex Interactive Environments. From the point of the features physiological characteristics, the palm s area is large, so that the palmprint has lost of main lines, papillae, creases, etc. and it is not easy to be imitated and damaged. The palm vein features can only be detected when person is live, and generally cannot be changed for physiological reasons. More important, the palm vein located in the deep skin. It is difficult to be replicated inside the vein. These properties make it capable of robustly resisting the attack of counterfeit feature, and because it is not required for the user to touch the device in the acquisition, it is easy for the user to accept. In addition, veins are extremely robust to light. In the literature[2], Wang Yiding compared the average information entropy of image samples in the hand vein and other large biometric libraries, the average mutual information entropy of similar type images, and the average mutual information entropy between various types, indirectly proved the feasibility of vein identification. The literature[3]also indirectly proves that no two people have the same vein characteristics, and the vein characteristics will not change for a long time. Many researches show us that the vein features such as the number of the blood vessels intersections, the curvature and relative positions of blood vessels have a great degree of differentiation.

From the point of the feature acquisition, in a complex collection environment, such as lack of illumination and low resolution of the camera, the biological features which use the image as a carrier are less likely to be disturbed by environmental factors such as noise. Palmprint and palm vein features are located on the hand, compared with the iris and other biological features, which can be easily accepted by users. On the other hand, palmprint and palm vein s images collected in a black box and will not be disturbed by the external background. In the actual, palmprint and palm vein s characteristics cannot be affected by accessories and expressions.

Therefore, the combination of palmprint features and palm vein features not only contains a wealth of information, but also has the ability to resist the attack of counterfeit feature, so that can significantly improve the identification efficiency and reliability of the authentication system under complex interactive environments.

2.2. **Multi-Block Multi-Filter LBP Algorithm (MBMFLBP).** Due to the influence of factors such as light intensity, hand posture, and signal noise, a large amount of noise is contained in the collected images. Palmprint image and palm vein image contain a large amount of veins information, however, the presence of noise will destroy the veins in the image[4]. At the same time, for the palm vein, the acquired image will inevitably contain part of the palmprint s trace. This palmprint trace is a kind of noise for the palm vein. How to remove the palmprint noise in the palm vein image and effectively extract the palm vein s feature is the difficulty of this article.

Local Binary Patterns (LBP) is a classical algorithm for feature extraction of textures. It has strong texture description capability and can effectively describe line features and cross-point features of palmprint or palm vein. But in a complex environment, the collected images are disturbed by the noise from the camera and the background light source, the collected images contain a lot of noise, mainly salt and pepper noise and Gaussian noise, which leads to false recognition caused by the degradation of image quality. In order to remove the noise as much as possible, especially the palmprint noise in the palm vein image, and to accurately extract the LBP eigenvalues of palmprint or palm vein, it is necessary to improve the traditional LBP feature extraction algorithm. The improved LBP algorithm is called Multi-Block Multi-Filtering LBP (MBMFLBP). The improved LBP algorithm s steps can be shown as follows.

Suppose there is an $N \times N$ captured image, denoted by $f(x, y)$:

First, the pre-processed standard-size image is divided into $k \times k$ blocks, and one of them is traversed using a 3×3 matrix. The gray value of the central pixel of the matrix is replaces the median number of the eight neighborhoods values in the matrix. It was shown in the figure 2.

Then, the following changes should be made in each block :

$$g(x, y) = \frac{1}{9} \sum_{(i,j) \in S_k} f(i, j) \tag{1}$$

It was shown in the figure 3.Where $x, y \in 0, 1, 2, \cdots, N-1$; S_k is the set of 8 neighborhoods whose kth block is centered on (x, y).

90	89	99	105	18
11	102	35	53	2
95	102	44	58	102
66	20	15	90	45
88	19	66	250	128

to $\longrightarrow$

90	89	99	105	18
11	90	35	53	2
95	102	44	58	102
66	20	15	90	45
88	19	66	250	128

FIGURE 2. The Results of Blocked Median Filter

90	89	99	105	18
11	90	35	53	2
95	102	44	58	102
66	20	15	90	45
88	19	66	250	128

to $\longrightarrow$

90	89	99	105	18
11	73	35	53	2
95	102	44	58	102
66	20	15	90	45
88	19	66	250	128

FIGURE 3. The Results of Blocked Average Filter

Next, the value of LBP feature for each block should be defined as:

$$LBP(x_k, y_k) = \sum_{i=0}^{n-1} u(g_i, g_k) \cdot 2^i \tag{2}$$

$$u(x) = \left\{ \begin{array}{l} 0, x < 0 \\ 1, x \geq 0 \end{array} \right. \tag{3}$$

Where (x_k, y_k) is the coordinate of the center pixel k; $u(x)$ is the threshold function; i is the ith pixel; g_i is the gray value of the ith pixel; k is the center pixel, and g_k is the gray value of the center pixel.

Finally, the LBP vectors of each region should be concatenated together and become the LBP feature vector of the entire image.

3. Multi-feature Fusion Strategy Based on D-S Evidence Theory for Complex Interactive Environments.

3.1. The Status Quo of Biometric Fusion Technology Based on D-S Evidence Theory. Multi-feature fusion is the application of information fusion technology in the field of pattern recognition. In terms of image-based biometrics, it is mainly divided into four levels of fusion: image data layer fusion, feature layer fusion, matching layer fusion, decision layer fusion. Image data layer fusion is a kind of underlying fusion, which can preserve to the utmost extent the original image data information, and the fused image can intuitionally uniquely represent an organism. Feature layer fusion is to combine the feature vectors obtained after feature extraction of a variety of biological features in accordance with certain rules to form a high-dimensional joint feature vector before recognition. In matching layer fusion, a single biometric vector is firstly matched, then the matching scores are output, and finally multiple matching scores are merged to achieve identity authentication. The fusion of decision-making layer belongs to the top-level fusion method. According to the result of a single feature recognition, the fusion decision is made according to a certain distribution principle, and finally the identity authentication will be output[5].

According to Dempster-Shafer (D-S) evidence theory, we define an identification framework : $\Theta = \{\theta_1, \theta_2, \cdots, \theta_N\}$, where θ_1,θ_2,$\cdots$,θ_N represent a set of mutually exclusive and complete hypotheses. In this recognition framework, there is a mapping called Basic Probability Assignment (BPA): $2^\Theta \to [0, 1]$, $m(\emptyset) = 0$ and $\sum_{\theta\subseteq\Theta} m(\theta) = 1$,$m(\theta)$represents the degree of trust in θ. Among them,θ with $m(\theta) > 0$ is called a focal element. Define the Belief function B_el: $\theta \to [0, 1]$, and satisfy $B_el(\theta) = \sum_{B\subseteq\theta} m(B)$, $B_el(\theta)$ can represent the BPA s sum of all the determinations given to θ and its smaller subset. Define the Plausibility function P_l:$\theta \to [0, 1]$, and satisfy $P_l(\theta) = \sum_{B\cup\theta\neq\emptyset} m(B)$, so $P_l(\theta) = 1 - B_el(\theta^-)$, where θ^- is the complement of θ. $[B_el(\theta), P_l(\theta)]$ constitutes a confidence interval, indicating the degree of confirmation of θ. Assume that there are two completely independent and safe and reliable evidences of BPA m_1 and m_2 respectively. For any $\theta \subseteq \Theta$, the Dempster synthesis rule is:

$$m(\theta) = [m_1 + m_2](\theta) = \{ \begin{array}{ll} 0, & \theta = \emptyset \\ \frac{\sum_{B\cup C=\theta} m_1(B)m_2(C)}{1-\sum_{B\cup C\neq\emptyset} m_1(B)m_2(C)}, & \theta \neq \emptyset \end{array} \tag{4}$$

In the process of multi-feature fusion, there are some uncertain factors. The D-S evidence theory has good fuzzy inference performance for the uncertainty evidence. Xu et al.[6] pointed out that the D-S method provides strong theoretical basis for the expression and synthesis of uncertain information. Chang et al. [7] used the D-S evidence theory to fuse the features of the image such as color and texture. Experiments have shown that it has a good recognition effect. In the field of identity authentication, researches of using D-S evidence theory for multi-feature fusion are rare.

In order to ensure the identification efficiency of the identity authentication system in the actual complex environment, this paper applies the D-S evidence theory fusion algorithm to the decision-making layer. Firstly, the MBMFLBP algorithm be used to extract the eigenvalues of a single biological image on the training data set. Then the recognition subsystem be used to train. Next the parameter correction set be used to test the recognition accuracy rate of the feature, which will be consider as the BPA of D-S evidence theory and the different BPA is used for decision-level fusion recognition. Finally the recognition result and rate of the system after feature fusion will be obtained.

3.2. **SVM-based Probability Estimation Theory and BPA Function Construction.** Support vector machine (SVM) model has the advantages of small sample size and strong generalization ability. In practical applications, it is difficult to establish large sample libraries for the same organism due to various factors such as device storage capacity and acquisition conditions, however the SVM model is very suit for this research to build the identification subsystem. When using a single biometric to perform two-class authentication (users are in or out of the system database, a total of l training data samples), for each test data sample x, the SVM model s output is:

$$f(x) = sgn(\sum_{x_i\in S_V} a_i y_i K(x_i, x) + b), (i = 1, 2, 3, \cdots, l) \tag{5}$$

Where a_i is the Lagrange multiplier, b is the threshold determined from the sample and $K(x_i, x)$ is the kernel function.

However, the decision output $f(x)$ of the standard SVM is a hard output, which means that only x is or does not belong to a certain class, and does not provide the probability of belonging to this class. The Dempster synthesis rule first needs to determine the basic probability setting of each piece of evidence. The recognition accuracy rate of each biometric in this paper is a piece of evidence s BPA. Therefore, when determining the BPA of each piece of evidence, the method has be proposed by Platt [8]. We have made improvements to this. On this basis, the above Dempster synthesis rules are used to synthesize the relevant evidence into a new evidence, and the final credibility and judgment results are obtained. Because the evidence here comes from a number of different subsystems, they have ensured the independence of the evidence. The core idea of the method proposed by Platt is that the divided correct possibility when the points be divided closer to the interface are smaller and the divided correct possibility when the points be divided farther away from the interface are more big. Therefore, if a sigmoid function is used to map the output value of the SVM to $[0, 1]$, the output of the final recognition subsystem of a single feature is the probability estimate of the sample judges as a positive class $p(y = 1|f)$ form as follows:

$$p(y = 1|f) \approx P_{A_s}B_s(f(x)) = \frac{1}{1 + exp(A_s f(x) + B_s)} \tag{6}$$

The A_s, B_s is used to control the sigmoid function form in order to obtain more accurate classification results, and respectively referred to as scale parameters and position parameters. In order to solve the problem of overflow of the lg and exp function in computer applications, we use the following formula provided by Lin Chih-Jen [9] the author of libsvm:

$$\min_{Z=A_s,B_s} F(Z) = \{ \begin{array}{ll} -[\sum_{i=1}^{l}(t_i - 1)(C) + lg(1 + exp(C))], & C < 0 \\ -[\sum_{i=1}^{l} t_i(C) + lg(1 + exp(-C))], & C \geq 0 \end{array} \tag{7}$$

$$C = A_s \cdot f_i + B_s \tag{8}$$

$$t_i = \{ \begin{array}{ll} \frac{N_+ + 1}{N_+ + 2}, & (y_i = 1; i = 1, 2, 3, \cdots, l) \\ \frac{1}{N_- + 2}, & (y_i = -1; i = 1, 2, 3, \cdots, l) \end{array} \tag{9}$$

Where N_+, N_- represent respectively the number of positive and negative samples.

The above method is effective for the two-classification problem, but it cannot directly deal with the multi-classification problem in identity authentication. Sima Liping et al. [10] used the pair-by-pair coupling method and the one-to-one SVM classification method to solve problem for transformation multiple classifications result to the posterior probability. This paper uses the method of [10] to calculate the multiclasses classification posterior probability $p_i = p(y = i|x)$ in identity authentication, where $i = 1, 2, 3, \cdots, k$; k is the number of categories.

$$\{ \begin{array}{ll} min_p \frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{k} (r_{ji} \cdot p_i - r_{ji} \cdot p_j)^2 & \\ \sum_{i=1}^{k}(p_i = 1), & p_i \geq 0, \forall i \end{array} \tag{10}$$

Where $i, j = 1, 2, 3, 4, \cdots, k$, and $j \neq i$; r_{ij} is the posterior probability of x belonging to the ith class when the ith class and the jth class is pairing. After the iterative algorithm is calculated, the probability that a sample belongs to each category can be obtained. The category with the highest probability is the discrimination result given by the classifier.

After learning the training data set of a single feature, in order to ensure the objectivity of the BPA assignment, a parameter-corrected data set will be used to obtain more reliable position parameters, scale parameters, and recognition accuracy α of the feature-corresponding classifier.Then the identification framework of the method in this paper is

$$\Theta = \{C_1, C_2, \cdots, C_i, \cdots, C_N\} \tag{11}$$

Where C_i refers to the user's category number, and i is the number of categories. The definition of the palmprint feature recognition result is the first proof body, the vein feature recognition result is the second proof body, and the BPA function corresponding to the jth proof body can be described in the following form:

$$m_j(C_1, C_2, \cdots, C_i, \cdots, C_N) = \begin{pmatrix} p_1 1a_1, p_1 2a_1, \cdots, p_1 N a_1 \\ \cdots \\ p_j 1a_j, p_j 2a_j, \cdots, p_j N a_j \end{pmatrix}, j = \{1, 2, \cdots\} \tag{12}$$

The degree of uncertainty of the jth evidence body is described in the following form:

$$m_j(\Theta) = 1 - \alpha_j \tag{13}$$

We define that the confidence of an SVM classification is equal to its recognition accuracy rate α_j, then the probability of classification error $1 - \alpha_j$ can be regarded as the uncertainty information of the SVM classifier in the D-S fusion. Therefore, the BPA function for each picture is shown in equation (11).

According to the Dempster synthesis rules and calculating the belief function and the Plausibility function of the two evidence bodies, the reliability of the evidence to identify all the propositions of the framework and the uncertainty of the evidence are obtained. Finally, we must make judgments based on the decision rules and draw conclusions. The decision rules adopted in this paper are as follows:
(1)The category that the user passes the authentication is the class corresponding to the maximum value among all degrees of trust, that is, $B_el(\theta_1) = max\{B_el(\theta_i), \theta_i \subset \Theta\}$;
(2)The difference between the user's category and other categories must be greater than a certain threshold ε_1, that is, $B_el(\theta_1) - B_el(\theta_2) > \varepsilon_1(\varepsilon_1 > 0)$, where $B_el(\theta_2) = max\{B_el(\theta_i), \theta_i \subseteq \Theta, \theta_i \neq \theta_1\}$;
(3)The trust degree of the target class must be greater than the uncertainty trust assignment value,that is, $B_el(\theta_1) - m(\Theta) > \varepsilon_2(\varepsilon_2 > 0)$;
(4)The degree of uncertainty of uncertainty should be less than a certain threshold λ, $m(\Theta) < \lambda(\lambda > 0)$. If they cannot meet the above rules at the same time, a conclusion cannot be obtained.

4. **Experiments and Analysis.**

4.1. **The Source of Image Database.**

In order to verify the effectiveness of the proposed method, it is necessary to do the simulation experiment. This paper uses the database of palmprint and palm vein images provided by the Hong Kong Polytechnic University as experimental data. The University of Hong Kong Polytechnic University's open palmprint database (v2) is a widely used benchmark database in the field of palmprint recognition. It collected about 20 samples from each of 384 volunteers in two sessions. About 10 samples were captured at the first meeting and the second meeting. The average time between the first and second collections is two months. Its image size is 384×284. The Palm Vein Library is a palmprint image database under the near-infrared illumination conditions of a multispectral palmprint description database. The database contains a total of 500 palms from different individuals, and each individual acquires 6 images at two sessions at intervals of 9 days. A total of 12 images under near-infrared light were collected.

In this paper, 40 people were randomly selected from the above image library as the internal staff of a small company. The palmprint image and the palm vein image were combined one by one. One person has 8 palmprint images and 8 palm vein images. 4 palms were randomly selected from one feature. The 4 of palmprint images and the 4 of palm vein images are used as training data set to train the model proposed in this paper.

The next 2 of them are selected as parameter correction data set to correct the probability of the single feature SVM classifier output and obtain the classification accuracy rate. The last two of them are used as test data set to obtain the accuracy of the fusion method proposed in this paper. Then the training data set of this paper contains 40 individuals and 4 palmprint images and 4 palm vein images per person are divided into 40 categories and a total of 320 images. The parameter correction data set contains 40 people and 2 palmprint images and 2 palm vein images per person are divided into 40 categories and a total of 160 images The test data set contains 40 people and each has 2 palmprint images and 2 vein images, and a total of 160 images. The evaluation index of the proposed method is Correct Recognition Rate (CRR).

4.2. **Multi-Block Multi-Filter LBP Algorithm s Effect and Analysis.** In the first experiment, the improved MBMFLBP algorithm is used to extract the texture features of palmprint and palm vein images on the training data set, and using the parameter correction set and the SVM algorithm to obtain the recognition results, which be compared with the traditional LBP algorithm. The results are shown in the figure 4. It can be seen from the figure 4 that the proposed MBMFLBP algorithm has little effect on palmprint features, and it even affects the recognition of palmprint to a certain extent. This is due to the slender characteristics of palmprint features. Expect for three main lines, the rest of the palmprint lines are relatively shallow and short in length. Under the action of blocking and filtering, the original features become blurred, which leads to a decrease in the distinguishability of the features, resulting in a decrease in recognition performance. The palm vein itself is coarser than the palmprint. After action of this algorithm, the palmprint noise in the palm vein image is eliminated in a certain extent, making the palm vein texture feature more obvious. Therefore, the MBMFLBP algorithm proposed in this paper is very effective for the recognition of palm vein characteristics. In addition, with the increase in the number of blocks, the recognition rate has decreased. This is due to too many blocks, ignoring the global features caused the decline in the recognition performance, so the appropriate block helps improve the recognition rate of the algorithm.

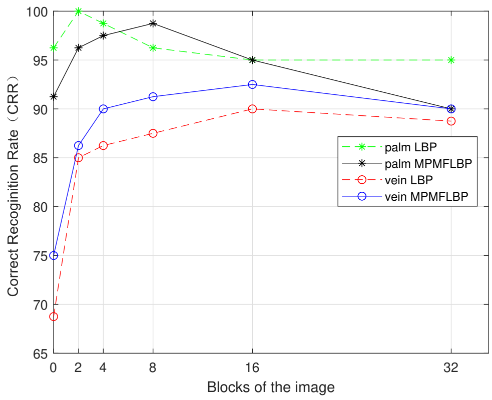

FIGURE 4. MBMFLBP and LBP algorithm performance comparison

we also can see from the figure 4, for palmprint, when divided into 8×8 blocks, the MBMFLBP algorithm proposed in this paper is superior to the traditional LBP algorithm in the recognition rate, so the author after repeated cross-data validation and the recognition time of the two is tested. The recognition time of the traditional LBP algorithm is 1.27s. The identification time of the MBMFLBP algorithm proposed in this paper is 1.10s. It is believed that this algorithm is better under the 8×8 block. The noise effect of each block is removed and the local features are efficiently extracted, however, the traditional LBP algorithm cannot do this.

4.3. **Posterior Probability of SVM Estimation Experiment and Analysis.** Based on the first experimental results in Section 4.2, the second experiment uses the palmprint eigenvalues extracted by the ordinary LBP algorithm in 2×2 blocks, and the palm vein eigenvalues extracted by the MBMFLBP algorithm in 16×16 blocks as the template. To randomly selecting one sample form test data set, the palmprint and palm vein image of an individual were collected for analysis, and the individual was recorded as P1. Its SVM posterior probability estimation output is respectively shown in the figure 5 and figure 6.

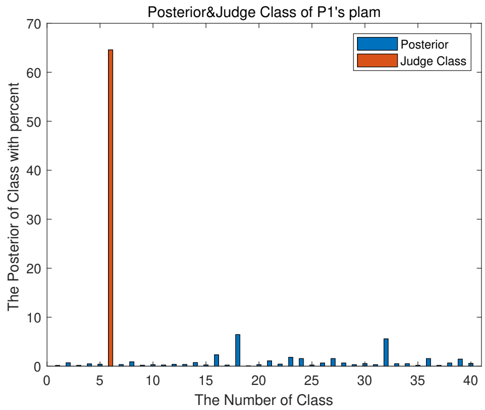

FIGURE 5. The posterior probability of P1's palmprint sample

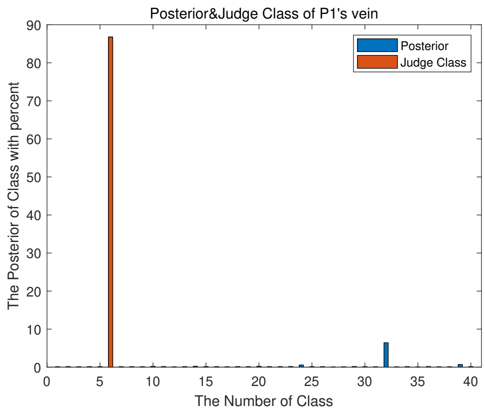

FIGURE 6. The posterior probability of P1's vein sample

Figure 5 is the probability that the palmprint image of P1 is classified into each class after LBP algorithm extraction and SVM algorithm classification, and the largest probability is the final classification result. It can be seen from the above that the palmprint of P1 has the highest similarity with the 6th class, followed by the similarity of about 7% with the 18th class, and the similarity with other classes decreases in turn. Therefore, the class of P1 is judged as 6th class. Figure 6 is the classification result of the palm vein picture of P1. It can be clearly seen from the figure that it has a similarity degree of more than 85% with the 6th class, and has similarity of about 8% with the 32nd class, and then with other classes the similarity decreases in turn.

For another test individual P2, its palmprint and palm vein classification results are different. Figure 7 and figure 8 are the posterior probability distributions of P2 s palmprint samples and the posterior probability of palm vein sample classification. From the posterior probability distribution map of the palmprint classification, palmprint features are as high as 95% similarity to the 18th class, and less than 5% of the sum of the similarities to the rest of the classes. Therefore, it is interpreted as 18th class. In the posterior probability distribution map of palm vein classification, its palm vein feature has a similarity with the 32nd class of pictures as 28.11%, and with the 18th class, that is, its real category, only nearly 15% similarity.

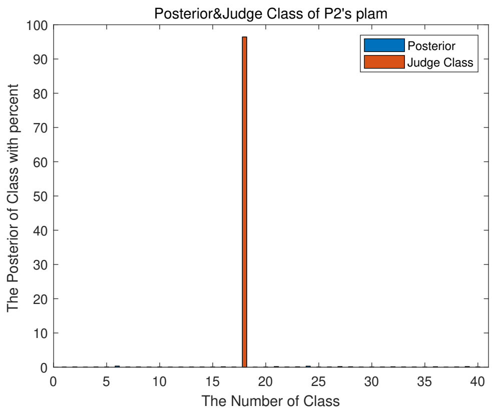

FIGURE 7. The posterior probability of P2's palmprint sample

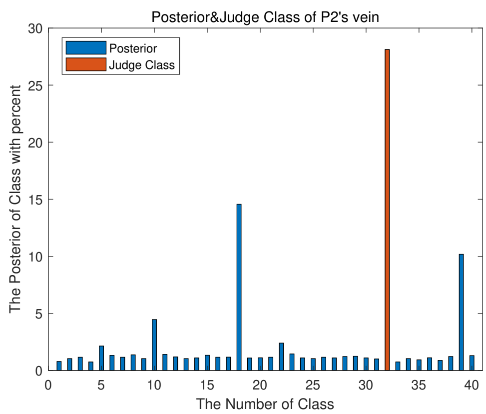

FIGURE 8. The posterior probability of P2's vein sample

Figure 9 and figure 10 are palm vein images of P2 and a picture in class 32. From the images, we can see that there is a similarity between the two sides of the great fish near the upper right corner of the picture, and there is also a certain degree of similarity between the middle and lower palms near the hypothenar. In addition, the reason for the palm vein classification error caused by this test example also includes the individual's own palm vein deep in the skin so that the image acquisition effect is not obvious, which affects the palm vein recognition performance.

4.4. **D-S Fusion Experiment and Analysis.** The construction of BPA function of palmprint and palm vein evidence body depends on the classification accuracy rate. In the second experiment, the recognition rate of palmprint is 100.00%, the palm vein recognition

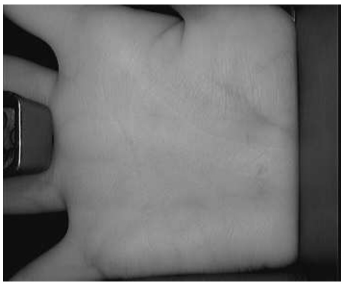

Figure 9. The image of P2's palm vein sample

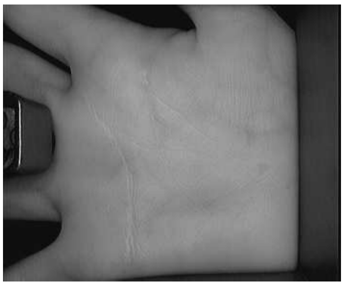

Figure 10. The image of the 32th sample

rate is 92.5%. In the third experiment, it was be brought into the D-S fusion rule. The BPA function of the proof body was fused, and the method proposed in this paper was tested using the test data set. Table 1 shows the recognition results of the D-S fusion palmprint and palm vein method proposed in this paper.

Table 1. The Comparison of the D-S Fusion Performance

The name of experiment	The numbers of test images	The right numbers of the results	CRR in (%)	The max time of one sample in(s)
palmprint	80	80	100	1.091947
palm vein	80	74	92.5	1.533456
D-S Fusion	80	80	100	5.365985

As can be seen from Table 1, the D-S evidence theory proposed in this paper can effectively improve the palm vein and palmprint recognition rate, and the recognition time is acceptable. Figure 11 shows the probability distribution of individual P1 for each class in third experiment. Figure 11 shows the original probability distribution. Figure 12 shows the local enlarged image of the figure 11. From the two images, the probability of 6th class is far than other classes, so the final judgment result is class 6.

In the second experiment, the palm vein images of the P2 were misclassified. After D-S fusion, the P2's final probability is shown in the figure 13. Figure 14 shows the local enlarged image of the figure 13. It can be seen that the highest probability of P2 fusion

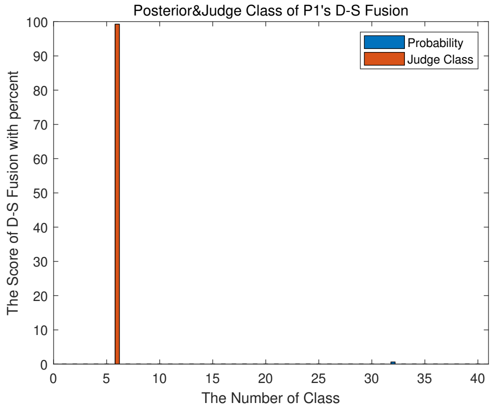

FIGURE 11. The result of P1 after D-S fusion

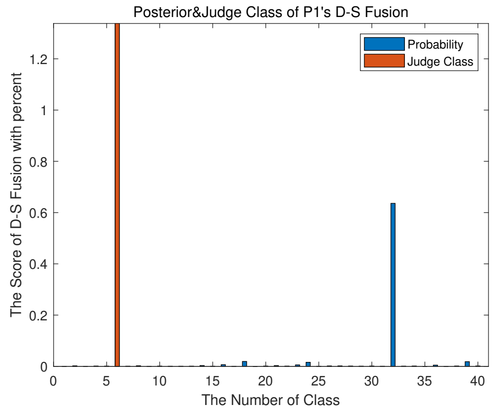

FIGURE 12. The local enlarged result of P1 after D-S fusion

is in the 18th class, followed by the 32nd class, and the real class of the P2 is the 18th class. Therefore, the success of the P2 classification proves the feasibility of the method.

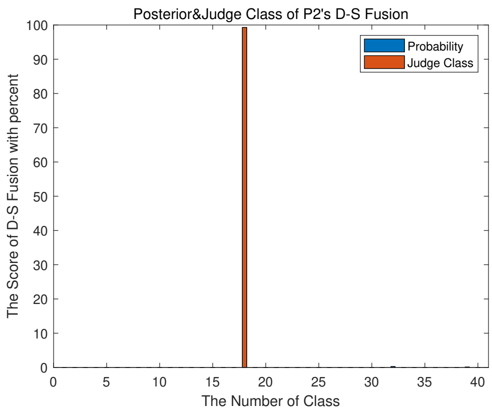

FIGURE 13. The result of P2 after D-S fusion

4.5. **To Prevent the Counterfeit Biometric Attacks Experiment and Analysis.** To verify that the method proposed in this paper can prevent the internal personnel of the company from Counterfeiting fingerprints and other biological information impersonating

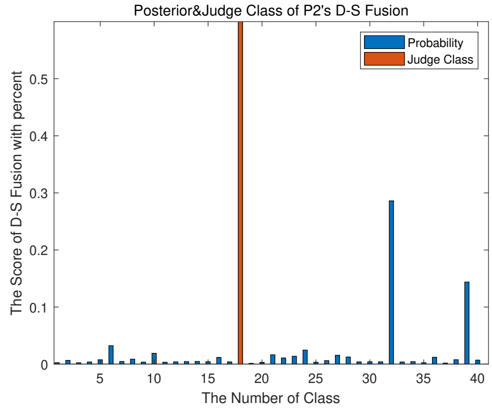

Figure 14. The local enlarged result of P2 after D-S fusion

employees with high authority to steal confidential data and to resist the ability of replay attacks from outside the authentication system, the forth experiment was conducted based on the third experiment. First, all palmprint and palm vein features are time-stamped. If the time from acquisition to authentication ends more than the maximum time that the fusion algorithm takes in the previous section, it is considered that a replay attack has been received, and thus this Certification is refused. Then on the test data set to test the palmprint and palm vein characteristics, and measure the average posterior probability of the corresponding category when the test image should be correctly classified. Through experiments, the average posterior probability of all classes palmprint features is shown in the figure 15, and the average posterior probability of all classes vein features is shown in the figure 16. In the figure 15, we can see that when all palmprint are classified correctly, the lowest average posterior probability is the 6th class, which is 29%. If the posterior probability of palmprint is less than 29%, it should be considered that the system was subjected to the counterfeit palmprint attack and refused to pass the certification. In the figure 16, we can see that when all the palm veins are classified correctly, the lowest average posterior probability is the 30th class, which is 18.47%. In other words, if the posterior probability of the palm vein is lower than 18.47%, it is considered that the system may be counterfeit palm vein attack and refuse to pass the authentication.

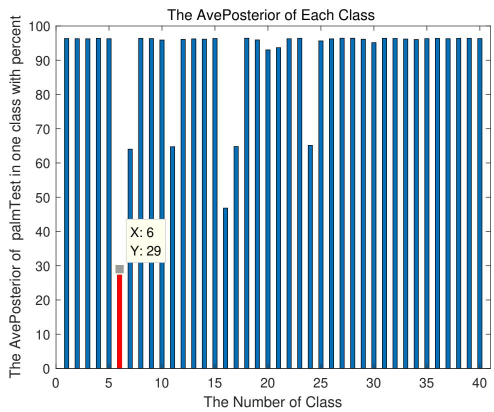

Figure 15. The average posterior probability of all classes' palmprint sample

Finally, we assume that A intends to steal the palmprint feature of B and impersonate B to steal confidential data. Then A can only use B's palmprint and its own palm veins

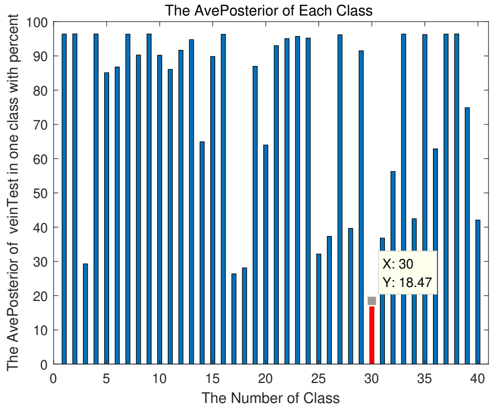

Figure 16. The average posterior probability of all classes' palm vein sample

to pass the authentication. After several experiments, we randomly selected a set of data for analysis. The palmprint feature authentication of B is shown in the figure 17, and the palm vein feature authentication of A is shown in the figure 18.

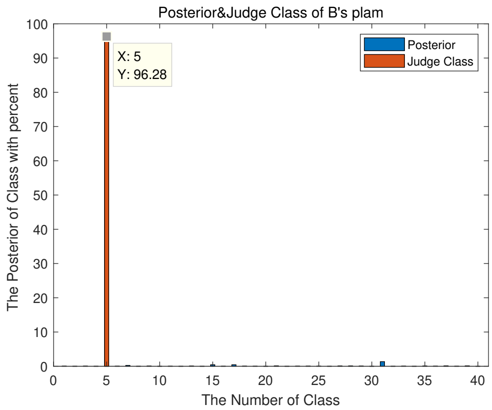

Figure 17. The posterior probability of B's palmprint

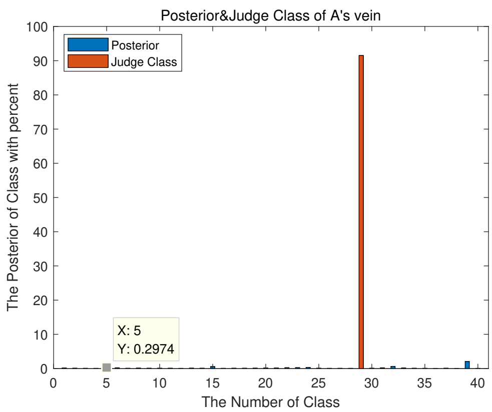

Figure 18. The posterior probability of A's palm vein

From the figure 17, it can be seen that A uses B's palmprint for authentication and the probability of being considered as B is 96.28%. From the figure 18, it can be seen that A uses its own vein for authentication and the probability of being considered as B is only 0.2974%. Because the threshold for vein authentication cannot be reached, the system considers it to be subject to counterfeit feature attacks and thus refuses the A's authentication request. However, if the recognition rate of the palm vein is not checked by the posterior probability check, fusion recognition is performed. As shown in the figure 19, the system will regard A as B, and the system security cannot be guaranteed at this time.

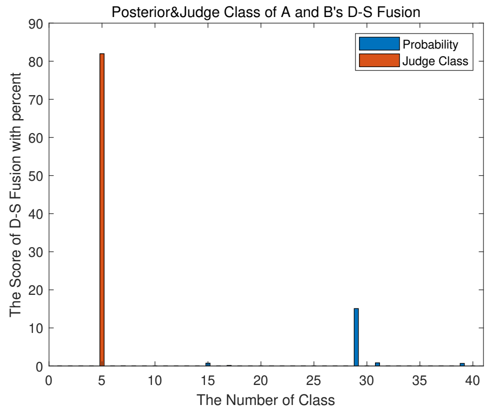

FIGURE 19. The posterior probability of A's palm vein and B's palmprint after D-S fusion

By analyzing the above multiple experiments, we can draw the following conclusions:
(1)Although the traditional LBP algorithm can extract palmprint features with a recognition rate of 100%, it can be easily forged because it is easily forged. Therefore, using only the palmprint feature does not guarantee that the feature is not obtained through forgery.
(2)Although the palm vein recognition rate is not high, even after the optimization of the MBMFLBP algorithm in this paper, the recognition rate is less than 95%. This is because the presence of palmprint affects the recognition performance of the palm vein, but the palm vein only exists in the living body. Each individual's palm veins are very different. Therefore, the palm vein is a biological feature that can effectively resist counterfeit feature attacks. Its existence will help improve the security of the system.
(3)This paper proposes to use the D-S fusion strategy to improve the recognition performance of the palm vein. Because the recognition rate of palmprint is 100% in this paper. If it is confirmed that it has not been subjected to counterfeit feature attacks and replay attacks, and the posterior probability of vein recognition is relatively small, this fusion method can effectively improve the recognition rate of the system.

5. **Conclusion.** This paper proposes a secure and reliable authentication method for complex acquisition environment and network environment. This method uses palmprint and palm vein feature as recognition features, firstly uses an improved LBP algorithm (MBMFLBP algorithm) to extract the palmprint and palm veins feature, secondly respectively uses SVM algorithm classification, thirdly determines whether the probability of palmprint and palm vein characteristics reaching the threshold requirement and the output of two SVMs is used as independent evidence body in D-S fusion theory for data fusion, finally, the result of the classification is obtained. This method has the following advantages:
(1)These two features can be acquired using the same device. Only the wavelength of

the light source needs to be adjusted. The palm vein has a living body and cannot be forged. Using the palm vein feature as a recognition feature can improve the security of the system.

(2)The palm vein images inevitably include palmprint lines. The MBMFLBP algorithm proposed in this paper can significantly improve the recognition performance of palm veins compared with the traditional LBP algorithm, and it increases by an average of 2.5% under different number of blocks, which proves the algorithm has a certain effect.

(3)In this paper, the D-S evidence theory is applied to the authentication method based on palmprint and palm vein. The experimental results show that the method is simple and effective, it can not only resist the counterfeit feature attack and playback, but also to achieve high recognition rate authentication system, provided an effective program with a certain engineering significance.

However, there are some deficiencies in this paper. For example, the number of test samples is not enough, and the performance of the method under the large-scale sample set is not verified. The recognition performance of palm veins needs to be further improved. The next step is to use the deep learning methods to extract the deep features of palm veins in order to improve the recognition rate of palm veins.

Acknowledgments. This project is supported by the National Natural Science Foundation of China (No. 61471158).

REFERENCES

[1] Zhang Yu, Pan Xiaoming, Liu Qingzhong, Cao Junkuo, Luo Ziqiang, APT attack and defense, *Journal of Tsinghua University Science and Technology*, 2017, vol.57, no. 11, pp. 1127-1133.

[2] Wang Yiding, Cao Xi. Research on the identification of the dorsal veins of hand[J]. *Chinese High Technology Letters*, 2014, vol. 24, no. 6, pp. 632-642.

[3] Ma X, Jing X, Huang H, et al. Palm vein recognition scheme based on an adaptive Gabor filter[J]. *Iet Biometrics,* 2017, vol. 6, no. 5, pp. 325-333.

[4] Chate Harold, Niquice Nelta. Blind Images Quality Assessment of Distorted Screen Content Images[J]. *Journal of Network Intelligence*, vol. 3, No. 2, pp. 91-101, May 2018.

[5] Zhang Lu, Tao Liang. Adaptive multi-modality biometric fusion based on classification distance scores [J]. *Journal of Computer Research and Development*, vol. 2018, no.1, pp. 151-162.

[6] Xu Congfu, Geng Weidong. A Review of Theory and Application of Dempster-Shafer's Evidence Reasoning Method[J]. *Pattern Recognition and Artificial Intelligence*, 1999, vol. 12, no. 4, pp. 424-430.

[7] Chang C, Xiaoyang Y, Guang Y. The Research of Image Retrieval based on Multi Feature DS Evidence Theory Fusion[J]. *International Journal of Signal Processing, Image Processing and Pattern Recognition,* 2016, vol. 9, no. 1, pp. 51- 62

[8] Platt J C. Probabilistic Outputs for Support Vector Machines and Comparisons to Regularized Likelihood Methods[J]. *Advances in Large Margin Classifiers,* 2000, vol. 10, no. 4, pp. 61–74.

[9] Chih-chung Chang , Chih-jen Lin. LIBSVM: A library for support vector machines[M]. *ACM*, 2011.

[10] Sima Liping, Shu Naiqiu, Li Zipin, et al. Identification of Internal Fault Location of Power Transformer Based on SVM and D-S Evidence Theory[J]. *Electric Power Automation Equipment,* 2012, vol. 32, no. 11, pp. 72-77.