# Palmprint Template Protection Scheme with Matrix Transformation

Hengjian Li*
Shandong Provincial Key Laboratory of Network based Intelligent Computing, University of Jinan
ise_lihj@ujn.edu.cn

Jian Qiu
Shandong Provincial Key Laboratory of Network based Intelligent Computing, University of Jinan
806091457@qq.com

Changzhi Yu
Shandong Provincial Key Laboratory of Network based Intelligent Computing, University of Jinan
420886387@qq.com

## ABSTRACT
In this paper, we proposed a palmprint template protection scheme based on matrix transformation. Firstly, the competition code features of original palmprint is extracted through the Gabor filters. Then, a general permutation matrix is generated randomly and two elementary permutation matrices are obtained by changing any two rows of it. Nextly, irreversible matrix is generated by XORing operation. Finally, cancelable palmprint templates are produced by multiplying the irreversible matrix and the original palmprint feature. Our experiments were carried out in a public database of Hong Kong Polytechnic University. The experimental results show that our cancelable palmprint scheme can not only ensure high safety but also meet the recognition accuracy requirements.

## CCS Concepts
**• Security and privacy→Security services→Authentication→ Biometrics.**

## Keywords
Biometrics; Cancelable palmprint; matrix transformation.

## 1. INTRODUCTION
With the development of computer technology and communication technology, people's lifestyle has undergone tremendous changes, and gradually enter the information age. In this era, information security has become a major challenge to the global information technology. Traditional identification methods cannot meet the requirement of information security. The most convenient and safe solution is biometrics technology [1].

Palmprints have several advantages, such as the rich information for feature extraction, the simplicity of data collection and a high level of user acceptability [2] Once the user's palmprint template in a database is stolen, the privacy covered in the palmprint features is likely to be leaked and hard to reuse in other recognition systems. Therefore, it is very important to research a safe biometric authentication method. In the protection of biometric template, the most classic algorithm is Biohash [3]. By generating random projection by user's password and product with feature data. Then, the results are binarized to generate a cancelable template. Then Biohash algorithm is then used in the palmprint template protection known as Palmhash [4]. However, the Palmhash method is not very accurate for large database. Lee generated the cancelable fingerprint template by changing the detail points with parameters [5]. However, the details of the point features are disorderly and it is difficult to establish matching point pairs. In [6] a new Cancelable fingerprint templates generation scheme based on minutiae-based bit-strings is proposed. This method has low computational complexity and does not require prealignment. In the aspect of iris template protection, Umer proposed a method based on feature learning. The iris template is generated by employing multi-level quantization [7]. In addition, Lai proposed a cancellable iris scheme, known as IFO hashing which is inspired from the Min-hashing. One advantage of the scheme is that it does not need to keep their permutation token in secret [8]. In the palmprint feature template protection, Li proposed a CNDF chaotic stream-ciphers encrypt the multi-direction PalmCodes to generate cancelable palmprint [9]. The recognition rate is still high when the keys are stolen. Furthermore, Leng proposed a method for generating a cancelable palmprint feature which is robust against several specific security attacks simultaneously.

In this paper, a palmprint templates protection scheme based on matrix transformation are proposed. Firstly, competition code features are extracted by Gabor filters. Then irreversible matrix is generated by general permutation matrix. Finally, cancelable palmprint templates are produced by multiplying the irreversible matrix and the original palmprint feature. The rest of this paper is organized as follows. Section 2 introduces the method of extracting competition code features. Section 3 introduces our basic scheme. Section 4 provides the experimental results and security analysis. Finally, the conclusions are drawn in Section 5.


*ICCCV '18*, June 15–18, 2018, Singapore, Singapore.

ACM ISBN 978-1-4503-6470-6/18/06…$15.00.
https://doi.org/10.1145/3232651.3232662

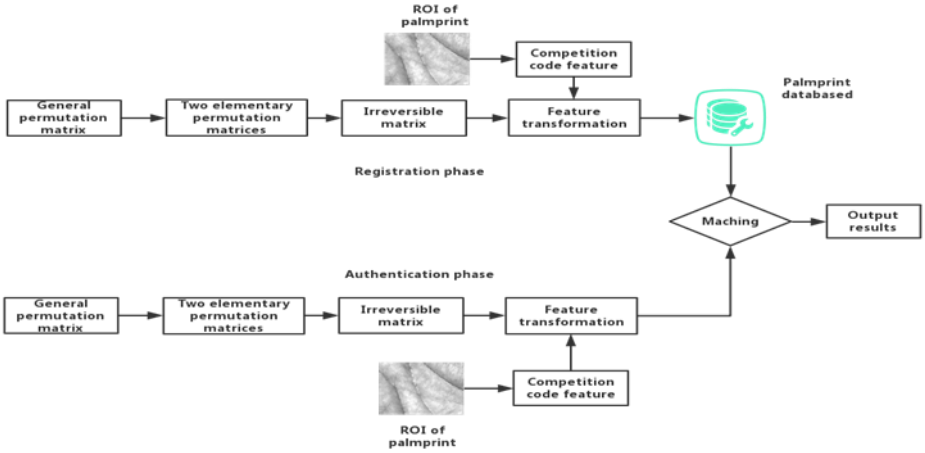


**Figure 1. The proposed system**

## 2. COMPETITION CODE FEATURES

Gabor filters are widely used in palmprint recognition. The Gabor wavelet is sensitive to the edge of the palmprint image and canprovide good direction selection and scale selection. In addition, it is not sensitive to light changes, and can provide good adaptability to light changes [10-11]. Gabor filter can be expressed as follows:

$$\psi(x,y,\omega,\theta)=\frac{\omega}{\sqrt{2\pi}K}e^{-\frac{\omega^2}{8K^2}(4x'^2+y'^2)}(e^{i\omega x'}-e^{-\frac{K^2}{2}}) \quad (1)$$

In addition, it can also be expressed as follows:

$$\psi(x,y,x_0,y_0,\omega,\theta,K)=\frac{\omega}{\sqrt{2\pi}K}e^{-\frac{\omega^2}{8K^2}(4x'^2+y'^2)}(\cos(\omega x')-e^{-\frac{K^2}{2}}) \quad (2)$$

In this formula, $x'$ and $y'$ is the center of the function. can be represented as follows:

$$x'=(x-x_0)\cos\theta+(y-y_0)\sin\theta \quad (3)$$

$$y'=-(x-x_0)\sin\theta+(y-y_0)\cos\theta \quad (4)$$

Where $\omega$ is the radial frequency and $\theta$ is the orientation of the Gabor filters. The expression of k is:

$$K=\sqrt{2\ln 2}(\frac{2^{\delta}+1}{2^{\delta}-1}) \quad (5)$$

Where $\delta$ is the half-amplitude bandwidth of the frequency response. The Competition code features of palmprint can be extracted by the following formula:

$$\arg \quad \min_j(I(x,y)*\psi_R(x,y,\omega,\theta_j)) \quad (6)$$

where $I$ is a ROI of palmprint image, $\psi_R$ is the real part of Gabor filter. $\theta_j$ represents the orientation of the Gabor filters.

## 3. BASIC SCHEME

In this section, we present the proposed method for protecting palmprint template. Furthermore, in order to achieve the privacy protection of palmprint and ensure the accuracy of recognition, a cancelable palmprint generation scheme based on matrix transformation is proposed. It is overall flowchart is demonstrated in Figure1.

Step1: For the preprocessed palmprint ROI region, its competitive code feature is extracted by using a set of Gabor filters [11]. It is transformed into a binary matrix. For example, 3 is converted to 0,1,1. 6 is converted to 1,1,0. Specific method as shown in Session 2. The competitive code feature is the expression of the direction, which can map the palmprint ROI image from the grayscale space to the direction information space. The extracted features of the competing code occupy a small space, and the extraction accuracy is high.

Step2: A general permutation matrix is generated randomly. It is a generalization of the permutation matrix, which is a special (0,1) matrix. There is only one non zero element in each row of the general permutation matrix. In addition, two elementary permutation matrices $p_1$ and $p_2$ are obtained by two independent transformations of the general permutation matrix. The method of transformation is a row exchange. The formula is as follows:

$$p=P(i\leftrightarrow j) \quad 1\le i\le m,1\le j\le m \quad (7)$$

Where $i$ and $j$ denote the $i$th row and $j$th row of the general permutation matrix, and m denotes the dimension of the general permutation matrix.

Step3: The irreversible matrix is generated by XORing the two elementary permutation matrices $p_1$ and $p_2$ which are obtained by the above Step2. The formula is shown below:

$$P=p_1\oplus p_2 \quad (8)$$

where P represents an irreversible matrix.

Step4: Cancelable palmprint templates are produced by multiplying the irreversible matrix and the original palmprint feature. They are then stored in the palmprint database. The formula for generating the final cancelable palmprint features is shown below:

$$F'=P\times F \quad (9)$$

**Figure 2. ROIs of palmprints**

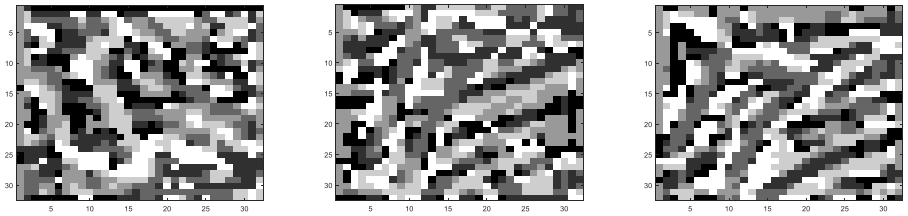

**Figure 3. Competition code features**

$F^{'}$ represents the final generated security palmprint features.

Step5: For any palmprint image to be identified, the cancelable palmprint features are extracted by the above Step1 to Step4.

Step6: In the classification, we first use Hamming distance for identification, the formula is as follows:

$$H = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} F_{i,j}^{'1} \oplus F_{i,j}^{'2}}{m \times n} \qquad (10)$$

Where $H$ denotes the final Hamming distance, m, n denotes the number of rows and columns of the cancelable palmprint features. Second, we use the SVM classifier for classification. SVM classifier can achieve better results than other algorithms even if the original palmprint image is less, thus improving the recognition rate. Both of these classification methods are to prove the validity of our methods.

## 4. EXPERIMENTAL RESULTS AND ANALYSIS

Our experiments were carried out in a public database of Hong Kong Polytechnic University [12]. The database consists of 600 palmprint images of a size of $384 \times 284$ , taken from 100 individuals and each of collecting 6 palmprints. Each of the six palmprint images taken from two different periods, the time interval is about two months. In our work, the size of the ROI obtained from the palmprint image is $128 \times 128$ [13]. In the experiment, the size of the competition code features extracted by the formula shown in Section 2 is $32 \times 32$ . Figure 2 is the palmprint ROIs area. The competition code features are shown in Figure 3.

When the hamming distance was used for matching identification, 179,700 experiments were conducted, of which 1500 were intra-class matches and 178,200 were inter-class matches. The ROC curve of the experiments is shown in Figure 4.

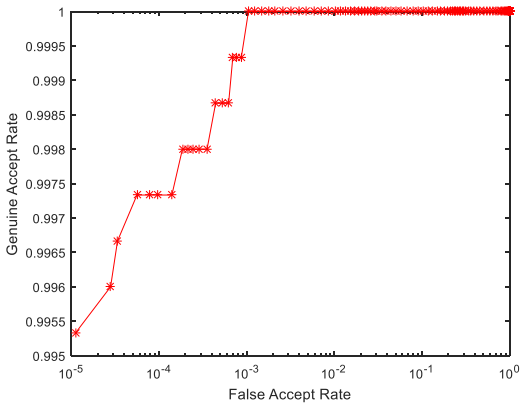


**Figure 4. ROC curve of the experiments**

It can be seen from the Figure4 that when the false accept rate is $10^{-4}$ , the genuine accept rate is 99.73%. When the false accept rate is $10^{-3}$ , the genuine accept rate is 100% and a better recognition result is achieved. In our experiment, the EER of our scheme is near zero at 0.07%. The FAR and FRR curves are shown in Figure 5 below:

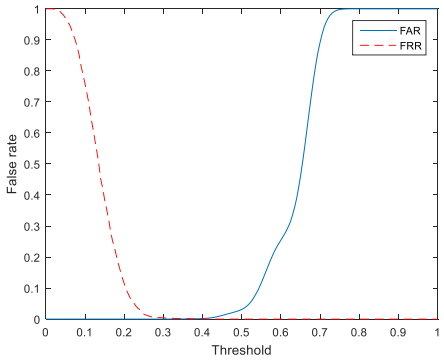


**Figure 5. FAR and FRR curves**

**Table 1. Classification accuracy rates of different methods**

| | BOCV[14] | SUM[9] | Half-orientation[15] | VO-WRHOG-LSP[16] | Our Methods |
|---|---|---|---|---|---|
| EER(%) | 0.10 | 0.08 | 0.0204 | 0.10 | 0.007 |

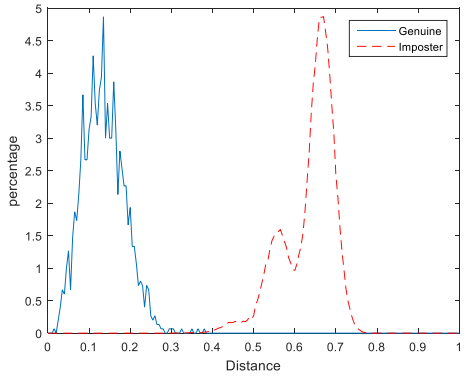


**Figure 6. The distance distribution of authenticator and impostor**

The EER of our method is compared with other methods as shown in Table 1. we can see their distance distribution of authenticator and impostor from Figure 6. The distance of the authenticator is in the vicinity of 0.135 and impostor is in the vicinity of 0.66. We can completely identify whether the authenticator or impostor. In addition, in the authentication phase, 3 images of per palmprint are selected to train SVM classifier, a total of 300. The remaining 300 palmprint images are used for classification identification. The proposed cancelable scheme based on matrix transformation has a recognition rate of 100%. This also shows the effectiveness of our method.

## 4.1 Security Analysis

Let's analyze if the size of the key space (irreversible matrix) is large enough to produce sufficient cancelable palmprint features. The irreversible matrix is generated by XORing the two elementary permutation matrices $p_1$ and $p_2$ .Because the size of the competition code feature we extract is 32*32, a general permutation matrix of the same size is generated. So, a total of 32! elementary permutation matrices can be obtained from a general permutation matrix. Therefore, we can calculate the number of irreversible matrices by the following formula:

$$C_n^r = \frac{n!}{r!(n-r)!} \tag{11}$$

So, a total of $C_{32!}^2 = \frac{(32!)!}{2!(32-2)!}$ irreversible matrices are generated. Therefore, the secret key space is large enough to produce enough cancelable palmprint features.

We analyze its security, in the case of our secret key (irreversible matrix) and the protected palmprint feature being stolen at the same time. The final cancelable palmprint features can be obtained by $F' = P \times F$ .The original palmprint features can be calculated by the following formula:

$$F = F' / P \tag{12}$$

Because $F'$ is an irreversible matrix, so we can't get our original template by this method, so our scheme is safe.

# 5. CONCLUSION

In this paper, a palmprint templates protection scheme based on matrix transformation are proposed. competition code features of palmprint are extracted by Gabor filters. The extracted features of the competing code occupy a small space, and the extraction accuracy is high. Irreversible matrix is generated by general permutation matrix. The key space is large enough. The cancelable palmprint templates are produced by multiplying the irreversible matrix and the original palmprint feature. In this paper, the method based on matrix transformation can not only protect the original palmprint template, but also satisfies the recognition accuracy.

# 6. REFERENCES

[1] Leng, L., Teoh, A., Alignment-free row-co-occurrence cancelable palmprint Fuzzy Vault. 2015, 48, 2290-2303.

[2] Saedi, S., Charkari, N., Palmprint authentication based on discrete orthonormal S-Transform. Applied Soft Computing.2014,21,341-351.

[3] Teoh, A., Ngo, D., cancellable biometrics featuring with tokenized random number. Pattern Recognition Letters, 2005,26(10),1454-1460.

[4] Connie, T., Teoh, A., Goh, M. PalmHashing: A novel approach for cancelable biometrics. Information Processing Letters,2005,93(1),1-5.

[5] Lee, C., Choi, C., Toh, K. Alignment-free cancelable fingerprint templates based on local minutia information. IEEE Transactions on Systems, Man and Cybernrtics, Part B: Cybernrtics,2007,37(4),980-992.

[6] Lee, C., Kim, J. Cancelable fingerprint templates using minutiae-based bit-strings. Journal of Network and Computer Applications.2010,33(3),236-246.

[7] Umer, S.,Dhara, B., Chanda, B. A novel cancelable iris recognition system based on feature learning techniques. Information Sciences.2017,406-407, 102-118.

[8] Lai, Y., Jin, Z., Teoh, A., Goi, B., et al. Cancellable iris template generation based on Indexing-First-One hashing. Pattern Recognition.2017,64,105-117.

[9] Hengjian, L., Jiashu, Z., Zuotao, Z. Generating cancelable palmprint templates via coupled nonlinear dynamic filters and multiple orientation palmcodes. Information sciences, 2010, 180,3876-3893.

[10] Kaur, H., Khanna, P. cancelable features using log-Gabor filters for biometric authentication. Multimedia Tools and Applications.2017, 76(4),4673-4694.

[11] Hong, D. Liu, W. Wu, X. et al : Robust palmprint recognition based on the fast variation vese–osher model Neurocomputing, 2016,174, 999–1012, 2016.

[12] Kong, A., David, Z. Competitive Coding Scheme for Palmprint Verification. Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04) 520-523 (2004).

[13] PolyU Palmprint Database. <http://www4.comp.polyu.edu.hk/~biometrics/>.

[14] Li, H., Zhang, J., Wang, L. Robust palmprint identification based on directional representations and compressed sensing. Multimed Tools Appl., 2014, 70, 2331–2345.

[17] Danfeng, H., Wanquan, L., Xin, W., et al. Robust palmprint recognition based on the fast variation Vese–Osher model. Neurocomputing,2016, 174, Part B, 999-1012.

[15] Guo, Z., Zhang, D., Zhang, L., Zuo, W.: Palmprint verification using binary orientation co-occurrence vector. Pattern Recognition Letters, 2009, 30, 1219-1227.

[16] Fei, L., Xu, Y., Zhang, D. Half-orientation extraction of palmprint features. Pattern Recognition Letters. 2016, 69,35-41.