Secure Palmprint Verification Using Random Measure and Permutations

1,2, LianHai Wang, 1, QiuLiang Xu, 2, Hengjian Li

1,2,*First and Corresponding Author School of Computer Science and Technology, Shandong University, Jinan 250101, Email: wanglh@keylab.net
2, Shandong Provincial Key Laboratory of computer Network, Shandong Computer Science Center, Jinan, 250014, Email: hengjianli2000@126.com

Abstract

Compared with the traditional verification schemes, the cancelability and re-issueability of biometric system is the inherent shortages. Therefore, problem of palmprint template security must be considered and solved in a real biometric system. To handle these problems, a hybrid palmprint template protection scheme using random measure and permutations is proposed in this paper. Firstly, the Gabor is employed to convolute with preprocessed palmprint image. Then, the obtained Gabor representation is compared with a chaotic random matrix to generate cancelable palmprint template. The random measure can improve the template's discriminabiliy. At last, the cancelable palmprint template is scrambled to strengthen the security of the template. The publicly available HongKong PolyU Palmprint Database is employed for evaluation. The experimental results show that our proposed scheme can separate the imposter and genuine population very well, that is also to say that, the EER is zero. And the re-usability of the proposed template protection scheme is very large to brute force attack.

Keywords: Biometric Recognition, Palmprint Template Protection, Chaotic Random Matrix, Permutations.

1. Introduction

With the increase in use of Internet, the problem of personal identification and related security become an urge problem. Traditional authentication cannot well deal with the new security questions. Biometric recognition give us to provide new approaches in a variety of security applications because of its reliable, robust and convenient way[1,2]. Palmprint identification has been researched for more than ten years. It has the several advantages, such as easy to capture the image, stable line features and high user acceptance and attracted lot of researchers’ interest[3]. There are mainly employed two categories in the palmprint recognition system. One is high resolution, in which the structure of a high resolution palmprint is similar to the fingerprint[4]. For example, Fig.1(a) is a Latent Palmprint and Fig.1(b) is captured with a non-contact manner with low-resolution.

Figure 1. Some orignal palmprint samples.(a) high-resolution palmprint image (b) a sample image from PolyU database.
Early work on palmprint recognition focused on extracting features from palmprint patterns. Extraction of line features and palmprint points as well as feature extraction using principal component analysis (PCA) and linear discriminant analysis (LDA) has been used to extract the feature of palmprint [5-8]. Since the CompCode[9], which uses a fusion rule to extract a more robust orientation code from the filter outputs, achieving a considerable improvement above the previous approach, the line and its orientation can always be the important and main characters of the palmprint images. And a lot of researchers developed different algorithms from different views.

With the growing of using biometrics in different applications, there is a rising concern about the security and privacy of the biometric data itself, especially for the cross-matching. As an example, a palmprint template stolen from a bank’s database may be used to search a criminal palmprint database or cross link to a person’s health records. And they may reveal sensitive information about personality and health, such as simian crease, which can be processed and distributed without the users’ permission [10].

Therefore, security and privacy problems of the users have been attracted more and more researchers’ interest in palmprint recognition system. In essence, the employed security schemes should be able to enhance biometric system resilience against attacks while allowing the matching to be performed efficiently. The straightforward solution to protect palmprint template is to encrypt the biometric template in a traditional way (such as DES or AES) on. However, due to the intra-class variations in biometric data (such as different poses and illustration influence), a small change in the raw biometric template will result in a completely different for the encryption form, as the data encryption algorithm required. Therefore, performing the matching process cannot be directly implemented in the encrypted domain. Before the matching process, they need to decrypted, and the privacy leak of the original template is possible[11].

To overcome this matching problem, a commonly proposed approach is not to store the original biometric template. Instead, a transformed version of the original template is stored, named cancelable biometric template[12]. For palmprint based authentication system, the idea of cancelable palmprint biometric has been introduced in, which can protect the original palmprint template as well as reissue novel template when the old ones are lost or stolen[13-15]. In order to solve the intra-class template variation problem while maintaining the template, a hybrid palmprint template protection scheme is proposed in this paper. Firstly, a novel cancelable is generated by measuring the Gabor based palmprint image with a chaotic random matrix. The basic idea is to transform a real value palmprint feature vector into a binary feature vector using a chaotic random matrix (The chaotic cipher has application in biometric security[13,16]). Then, the obtained Gabor representation is compared with a chaotic random matrix to generate cancelable palmprint template. The random measure can improve the template’s discriminability. At last, the cancelable palmprint template is scrambled to strengthen the security of the template.

The rest of paper is organized as follows. In Section 2, the different biometric templates protection solutions which have been investigated in the recent years are analyzed. The proposed approach for the protecting palmprint templates is illustrated in Section 3, and its verification performance and security analysis is outlined in Section 4. Finally, some conclusions are drawn in Section 5.

2. Biometric Template Security for palmprint template

Biometric template of an individual have a limited number of useful biometric traits and cannot be modified (Supposed the biometric invariance of life time in biometric authentication system ). Once this biometric data is compromised, it is impossible to have a replacement since everyone has a unique biometric. In addition, biometric traits may contain health information, for example, iris may be associated with diabetes mellitus.

To deal with biometric security and privacy issues, there are currently many research efforts toward protecting biometric systems against possible attacks which has been established at their vulnerable eight points in [12], as illustrated in Fig. 2. The eight possible vulnerable points have been identified and addressed systematically in a biometric system. Among the eight attacks, the biometric templates generated by the feature extractor module, which are stored in the database or matched against previously stored templates are the promising threat attacks point. The main reason is that there is a strong linkage between a user’s irrevocable biometric templates and his identity.
It has been suggested that a biometric template protection algorithm should satisfy the following requirements:

1. **Diversity**: templates from the same biometric traits should be different in different applications (such as different banks) to prevent cross matching.

2. **Security**: it should be computationally hard to reconstruct the original biometric template from the obtained biometric template. That is non-invertible.

3. **Discriminability**: The discriminability of the original biometric template should not be degraded after the cancelable biometric template is used.

To protect private information in palmprints, databases should not store the original template but store cancelable templates because the line orientation features can be reconstructed from raw palmprint templates, in which may contain personal health information. Different from the cryptosystem, cancelable biometrics matches in the transform domain while traditional encryption techniques require decryption before matching.

Consequently, a number of biometric template protection algorithms have been reported to overcome the security and privacy problems. There are many template protection schemes in the literature, and they are broadly classified into two categories [17]: biometric cryptosystems and feature transformation approaches. In [18], Boihaish were used to minimize the intra-class variations and protect the private biometric data of the users. The cryptographic techniques were applied to increase the security of palmprint system [19]. In [20], the error correcting codes were used to generate cancelable iris biometrics. A fuzzy commitment method was introduced in [21]. Another common method to get cancelable biometric template is using random projection algorithm [22, 23]. However, these methods would degrade the original biometric performance.

### 3. Biometric Cancelable palmprint verification using random measure

The ultimate purpose of the proposed hybrid cancelable palmprint recognition system can be mainly divided into the following steps, as illustrated in Fig. 3.

**Step 1:** For reliable feature measurements, the gaps between the fingers as reference points to determine a coordinate system is used to extract the region of interest from a palmprint image. The detail information can be found in [3].

**Step 2:** The preprocessed palmprint image is convoluted by a Gabor filter.

$$O(\theta) = G(\theta_p) * I(x,y)$$  \hspace{1cm} (1)

Where $\ast$ is an operator of convolution and $I(x,y)$ is a preprocessed palmprint image. The Gabor $G(\theta_p)$ is an effective tool for palmprint texture analysis [3], and can be represented as:

$$G(x, y, u, \sigma, \theta_p) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{x^2+y^2}{2\sigma^2}\right) \times \exp(2\pi i u(x \cos \theta_p + y \sin \theta_p))$$  \hspace{1cm} (2)
To make it more robust against brightness, a discrete Gabor filter is turned to zero DC (direct current) with the application of the following formula:

$$\overline{G}(x,y,u,\sigma, \theta_p) = G(x,y,u,\sigma, \theta_p) - \frac{\sum_{n=0}^{(2n+1)} \sum_{l=0}^{(2n+1)} G(x,y,u,\sigma, \theta_p)}{(2n+1)^2}$$

(3)

where \((2n+1)\) is the size of the filter. \((u, \sigma, \theta_p)\) are the Gabor filter parameters.

Step 3: Given an initial seed \(S_0\), using the following piecewise linear chaotic map to generate the random number, the distribution of the random follows uniform distribution[24]. It has the following characters: 1) the system is chaotic, and output signals in determined segment meet with ergodicity, mixing property and determinacy. 2) The distribution is unique uniform invariant distribution.

$$s_{n+1} = F(s_n, p) = \begin{cases} \frac{s_n}{p}, & 0 \leq s_n < p \\ 0, & s_n = 0.5 \\ \frac{(s_n - p)/(0.5 - p)}{p}, & p \leq s_n < 0.5 \\ 0, & s_n = 0.5 \\ F(1-s_n, p), & 0.5 < s_n < 1.0 \end{cases}$$

(4)

Where \(s_0\) is the initial state, and \(s_n \in (0,1)\), \(p\) is the control parameter, and \(p \in (0,0.5)\).

Step 4: Template Coding scheme: the sample point in the filtered image is coded to two bits, one fit for real part and the other bit for the imagery part by the following inequalities,

$$\begin{align*}
\tau_r &= 1 \quad \text{if } \Re\{O\} \geq s_n \\
\tau_r &= 0 \quad \text{if } \Re\{O\} < s_n \\
\tau_i &= 1 \quad \text{if } \Im\{O\} \geq s_{n+1} \\
\tau_i &= 0 \quad \text{if } \Im\{O\} < s_{n+1}
\end{align*}$$

(5)

Using this coding method, only the phase information in palmprint images is stored in the feature vector.

Step 5: The cancelable palmprint is scrambled with an address order algorithm.

Given a logistic map as the following form

$$x(n+1) = 3.999 \times x(n) \times (1- x(n))$$

(6)

For a initial value \(x(1)\), the chaotic map can be generated a serial values via iteration. The length of the serial sequence is the same with the palmprint template. Then the chaotic serial sequence \(X=[x(1),x(2),...,x(M \times N)]\) is sorted by a descending order, that is \(Y=[x(A(1)),x(A(2)),...,x(A(M \times N))]\).

We obtain the address of every number of serial sequence, for example, \(A(1), A(2), ..., A(M \times N)\). We can finally get the scrambled template using in the following manner \(T(A(i)), i = 1,2, ..., M \times N\).

Step 6: The matching scores are then calculated by the hamming distance to measure the most similarity to the test cancelable palmprint template set.
To describe the matching process clearly, we use a feature vector to represent the palmprint feature. A normalized Hamming distance is adopted to determine the similarity measurement for palmprint matching. Let $T_1$ and $T_2$ be two palmprint feature vectors. The normalized hamming distance can be described as

$$
    d = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} T_1(i, j) \oplus T_2(i, j)}{M \times N}
$$

Where $M \times N$ is the size of palmprint template. It is noted that $d$ is between 1 and 0. For the best matching, the hamming distance should be zero. Because of imperfect preprocessing, we need to vertically and horizontally translate one of the features and match again. The minimum $d$ value obtained from the translated matchings is considered to be the final matching score.
Fig. 4 shows the features generation cancelable palmprint template to improve the randomness of the biometric template. Fig. 4 (a) original palmprint image (b) ROI parts of the palmprint image, (c) Real part of palmcode, (d) imagery part of palmcode, (e) real part of random code, (f) imagery part of random code, (g) real part of cancelable code with the random matrix and permutations (h) imagery part of cancelable code with the random matrix and permutation. After the permutations, the randomness of the biometric template is improved, and the security is strengthened.

Firstly, in our proposed scheme, the main objective of the protection palmprint biometrics scheme is to provide the system cancelable ability and privacy security, therefore, a novel different chaotic random matrix would generate different a different cancelable palmprint template. And the permutation strategy can improve the security of cancelable template. Second, during the measuring with a random matrix, the matching distances of intra-class are reduced while the distances of interclass are increased. Also, this provides additional protection.

At the same time, the cancelable palmprint template can improve the discriminability in different class because of the randomness enhancement. In different applications require different sets of parameters in the random matrix. In our proposed scheme, we can generate a novel cancelable palmprint template just with a different initial parameter or control parameter and therefore, the secure palmprint templates of an individual in different applications will be different. In turn, the cross-matching across databases will not be feasible. Moreover, the secure palmprint template can be canceled and reissued by changing the chaotic parameters.

Another important aspect in palmprint biometrics is security and privacy of the users. When the template is obtained by the random comparison with the chaotic matrix, it can leak the user’s information for it is not randomness, especially in the three main lines in the palms. After the scrambled operation, the template is complete randomness, and the user’s privacy is protected.

4. Experimental results

4.1 Palmprint Database

In PolyU Palmprint Database, there are 600 gray scale images captured from 100 different palms by a CCD-based device(http://www.comp.polyu.edu.hk/ biometrics). Six samples from each palm are collected in two sessions: the first three samples were captured in the first session and the other three were captured in the second session. The average time interval between these two sessions was two months. The size of all the images in the database was $384 \times 284$ with a resolution of 75dpi. In our experiments, a central part ($128 \times 128$) of each image is extracted for further processing.

To evaluate the separation between the genuine and the impostor distributions, the discriminating index d’ (d-prime) is computed to measure how well the non-match score probability density and the match score probability density are separated. The discriminating index d’ is defined as[25]

$$d' = \frac{|\mu_g - \mu_i|}{\sqrt{(\sigma_g^2 + \sigma_i^2)/2}}$$

(8)
where $\mu_1$ and $\sigma_1$ are the mean and variance of the match scores of the genuine populations respectively; $\mu_2$ and $\sigma_2$ are the mean and variance of the match scores of the impostor populations respectively.

### 4.2 Cancelability Results using Random Measure

Verification is a one-to-one comparison against a stored training sample, which answers the question of “whether the person is whom he claims to be”. To obtain the verification performance of our cancelable palmprint system, each of the palmprint images was matched with all of the palmprint images in the database.

**Figure 5.** Comparison of the ROC curves of the different verification algorithm, including the PalmCode[3] and the proposed cancelable algorithm

A matching is noted as a genuine matching if two palmprint images are from the same hand. None of the hamming distances is zero. The failure to enroll rate is zero. The number of comparisons that have genuine matching is 1500. The rest are impostor matchings, and the number of this is 178200. The probability distributions for genuine and impostor are estimated by the correct and incorrect matchings, respectively. Fig. 5 gives the ROC curves using the Sum rule under different number of filters. The mean and variance of the intra-class and inter-class matching scores are also included in Table 1. From Fig. 5 and Tab.1, we can see that the verification performance using the random matrix is better than that of the PalmCode.

**Table 1.** Performance of different palmprint verification

<table>
<thead>
<tr>
<th></th>
<th>Intra-class</th>
<th>Inter-class</th>
<th>EER(%)</th>
<th>d-prime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mean</td>
<td>variance</td>
<td>mean</td>
<td>variance</td>
</tr>
<tr>
<td>Palmcode</td>
<td>0.2323</td>
<td>3.483×10^{-3}</td>
<td>0.4503</td>
<td>2.6065×10^{-4}</td>
</tr>
<tr>
<td>Proposed algorithm</td>
<td>0.0663</td>
<td>7.4181×10^{-4}</td>
<td>0.5001</td>
<td>1.2097×10^{-4}</td>
</tr>
</tbody>
</table>

From Tab.1, as can be seen, the mean of the normalized Hamming distance is very close to 0.5 with a very low standard deviation. Compared with the original genuine/impostor distributions, the distributions using the random matrix have smaller intra-matching scores while the distributions using matching all together strategy have larger inter-matching scores. Both of them can improve the authentication accuracy. As illustrated in Tab.1, the improvement of d-prime also demonstrates this point.

From Fig.6(a), the proposed cancelable palmprint authentication algorithm can obtain zero equal error rate (EER) and yields clean separation of the genuine and impostor populations as illustrated in Fig.6(b). Hence, the False accept rate (FAR) can be eliminated without suffering from the increased occurrence of the False reject rate FRR. From the Fig.6(b), the mean value of intra-class has dramatically reduced from 0.2323 to 0.0663. The mean value of interclass has increased from 0.4503 to 0.5001. All these properties show that the proposed scheme has more discriminative power. The
Different Matrix case has an impostor distribution that is more peaked and farther from the genuine distribution, indicating superior performance.

![Figure 6](image)

**Figure 6.** Experimental results of different algorithms (b) Comparison of the distribution of the Genuine and Impostor normalized Hamming distances for the original and cancelable templates

The Fig.6 shows that the histogram of hamming distance peaks at 0.5, empirically verifying that the random matrix pamprint template are significantly different from the original ones. Hence it is not possible to extract the original palmprint templates from the transformed version, thereby proving the non-invertible property of our transformation. The above analysis show that the random comparison strategy not only improves the recognition performance but also enhances the user’s privacy.

### 4.3 Cancelability of the proposed authentication system

To generate cancelable palmprint templates based on matrix random, we use a chaotic cipher to generate the random number. Thus, the capability of reissuing a palmprint template is characterized by the key space of the employed chaotic system. The key space is the total number of different keys that can be used in the cancelable template procedure. Numerical experiments show that the PWCL has uniform distribution. The key space size is the total number of different keys. A good cancelable template scheme is one in which the cancelable templates are completely sensitive to all the secret keys, and the ability to reissue templates is sufficiently large to make brute-force attacks infeasible. According to the IEEE floating-point standard, the computational precision of the 64-bit double-precision number is about $10^{-15}$. There is one initial parameter $s_0$ and a control parameter p in (4), therefore, the key space in the PWCL is $10^{30}$, which is enough to resist brute-force attacks.
Figure 7. (a) ROI parts of an original palmprint image, (b) real part of palmcode, (c) imagery part of palmcode, (d) real part of cancelable code with the random matrix and permutation, (e) imagery part of cancelable code with the random matrix and permutation, (f) and (g) are the cancelable palmprint template with a different initial parameters.

To evaluate the key sensitivity of cancelable palmprint template, we make some experimental in the following. The experimental results are shown in Fig.7. The differences between different template is approximately 0.5. That is, the XOR of Fig.7(d) and Fig.7(f) is 0.4996 while the XOR of Fig.7(e) and Fig.7(g) is 0.5001. Even an almost perfect guess of the key does not reveal any information about the original template. It also can be found that after the permutations, the randomness of the biometric template is improved, and the security is strengthened.

4.4 Security Analysis

This section analyzes the biometric template security strength of the proposed palmprint recognition system. Recovery of the cancelable template from the binary cancelable template might still be feasible because the transformed binary contains discrimination of the cancelable templates. Due to the information loss in the binarization, it would not be as easy as the first step.

As mentioned in the section 3, a new cancelable palmprint template can be generated by changing the random matrix parameters. In this section, we would like to see whether an attacker could successfully access the system using a compromised cancelable template as well as all the user-specific information. In this case, we assume that the attacker has accessed to the original palmprint template and the compromised random matrix.

To evaluate the cancelability of the proposed algorithm, Fig.8 gives the ROC curve at the user have the same random matrix (this is the worst case). The genuine accept rate (GAR) is as low as the false accept rate (FAR), implying that the query applying different projection matrix to the reference will mostly be rejected. This shows that the proposed hybrid algorithm has good diversity. At the same time, the accuracy of matching between templates generated by the same matrix is high, as illustrated in Fig.6(a). This shows that the proposed algorithm has a good revocability. Based on this, we conclude that the proposed algorithm has good cancelability.

Figure 8. ROC curve under the key-stolen case
5. Discussion and Conclusions

Based on the random measure and permutation, a hybrid palmprint template protection scheme is presented in this paper. The random measure, which is generated from chaotic cipher, can be employed to provide cancelability. Therefore, this scheme protects the template. On the other hand, the randomness is also able to increase the template discriminability. And the performance can be guaranteed. In the next, the permutation is to improve the cancelability and security of the biometric authentication system. Also, the chaotic map is used to generate the random matrix, which improve the scope of the chaos. The keyspace of the employed chaotic system is the cancelability of biometric system. Experimental results show that the proposed hybrid scheme not only protects the template but is also able to increase the template discriminability.

Acknowledgments

The authors are very grateful to the anonymous referees for their helpful comments. This work was supported by grants by National Natural Science Foundation of China (No. 61070163), by the Shandong Province Outstanding Research Award Fund for Young Scientists of China (No. BS2011DX034), and by the Shandong Natural Science Foundation (No. ZR2011FQ030).

References


Secure Palmprint Verification Using Random Measure and Permutations
LianHai Wang, QiuLiang Xu, Hengjian Li


