A High Performance and Secure Palmprint Template Protection Scheme

Hengjian Li, Lianhai Wang, Ruichao Zhang, Lu Wu
Shandong Computer Science Center,
Shandong Provincial Key Laboratory of computer Network, Jinan,, P.R.China
Email:{lihengj, wanglh, zhangrch, wul}@keylab.net

***Abstract*—Security and protection of biometric template has been the bottleneck of its applications due to permanent appearance of biometric features. To tackle this problem, many algorithms, that do not store the template in its original form, have been reported in recent years. In this paper, we propose a high performance and secure cancelable palmprint authentication algorithm for palmprint template protection based on texture features. Firstly, the anisotropic filter is employed to obtain the original palmprint template. Then, the feedforward–feedback nonlinear dynamic filter (FFNDF) is used to generate Cancelable Palmprint templates. At last, the independent matching scores are fused at the score level. The cancelable system can provide large re-issuance ability and can be implemented very fast for real applications. The experimental results on PolyU palmprint database show that both the chaotic key and biometrics play equally significant roles in cancelable and it can be easily generalized to other palmprint texture codes.**

***Index Terms*— palmprint template protection; palmprint authentication; chaotic encryption; matching score level;**

I. INTRODUCTION

In recent years, palmprint biometrics has attracted an increasing amount of attention from researchers[1].However, Biometrics characteristics are immutable. When biometrics is compromised, user can not revoke and reissue their biometric templates. Besides, one biometric template of the same user may be stored and shared in various databases with more and more biometric systems. With the growing use of palmprint biometrics, there is a rising concern about the security and privacy of the biometric data itself[2-3].The vulnerabilities of biometrics systems and potential eight of attacks have been identified and addressed systematically in[2]. The straightforward solution to the template security is to apply password-like encryption algorithm (hashing) on biometric template and perform the matching process in the encrypted domain. However, due to the intraclass variations in biometric data, a small change in the raw biometric data input will result in a large change in the encrypted data, leading to degradation in system accuracy. Therefore, directly applying password-like encryption method is not feasible. On the other hand, if the encrypted secure template is decrypted for matching process, it is susceptible to interception by an impostor.

In order to solve the intra-class template variation problem while maintaining the template security, a number of biometric template protection schemes have been reported[3]. Most of these algorithms have been focused on biometric template due to strong linkage between a user's template and his identity and the irrevocable nature of biometric templates,which can be categorized into two main approaches: (1) biometric cryptosystem approach and (2) transform-based approach. The basic idea of both the approaches is that instead of storing the original template, transformed/encrypted template which is intended to be more secure, is stored. In case the transformed/encrypted template is stolen or lost, it is computationally hard to reconstruct the original template and to determine the original raw biometric data simply from the transformed/encrypted template. In the biometric cryptosystem approach, the error correcting coding techniques are employed to handle intra-class variations. Two popular techniques, namely fuzzy commitment scheme [4] and fuzzy vault scheme [5] have been proposed. The advantage of this approach is that, since the output is an encrypted template, its security level is high. However, the error correcting ability of these schemes may not be strong enough to handle large intra-class variations such as face images captured under different illumination and pose.. In transform-based approach, a transformed template is generated using a "one-way" transform and the matching is performed in the transformed domain. The transform-based approach has a good cancelability (revocability) property, but the drawback of this approach is the trade-off between performance and security of the transformed template. Based on the random projection, class distribution preserving transform and hash function, a three-step cancelable framework which is a hybrid approach for face template protection is proposed[6].

At present, researchers proposed some cancelable palmprint biometrics techniques such as Palmhashing[7] and cancelable CompCode[8] have been proposed. A dual-key-binding cancelable palmprint cryptosystem to enhance the security and privacy of palmprint biometric was developed in[9]. But as other biometrics, the claim of having achieved a zero equal error rate (EER) in palmhashing is based upon the impractical hidden assumption of no stealing of the hash key[10]. Therefore,

doi:10.4304/jsw.7.8.1827-1834

Kong suggested that using invertible transform to generate cancelable palmprint biometrics, which a random orientation filter bank (ROFB) is employed as a feature exactor to generate noise-like feature codes [8]. The cancelable Competitive Code can be thought a two-factor authentication algorithm. According to the modeling and analysis in [11], it is computationally infeasible to break into the competitive code based system using brute-force attacks. Based on the texture features of cancelable PalmCode, Leng etal proposed Cancelable PalmCode generated from randomized Gabor filters[12]. However, the performance is not very high especially in the stolen-token case.

To overcome the degraded recognition performance, we develop a novel cancelable template generated scheme, which can preserve the intra-class variations while reducing the inter-class variations when the genuine tokens are used. Also, the mean value of imposter distribution would be large for the random of the cancelable templates is enhanced.In this paper, firstly, we use a 2D anisotropic filter (AF) to exact and encode the texture information. Then, the FFNDF chaotic stream cipher, which has good cryptographic characters for the FFNDF has uniform distribution and large key space[13], is employed to generate cancelable plamprint templates. At last, the matching score is fused at the matching score level and the hamming distance is used to distinguish the different user. Experimental results on Hong Kong PolyU Palmprint Database[14]show that our proposed cancelable palmprint verification scheme can achieve nearly zero equal error rate (EER). The rest of this paper is organized as follows. Section 2 briefly describes the binary texture coding scheme based on the AF. The chaotic cancelable palmprint template is presented in section 3. Experimental results and analysis are given in Section 4, which compares the performances of our proposed algorithm with the state–of–art approaches. Finally, conclusions are made in Section 5.

II. BINARY MULTIPLE ORIENTATION BINARY TEMPLATE BASED ON ANISOTROPIC FILTER

The AF is firstly used in building over-complete dictionary to obtain sparse representation by the idea of efficiently approximating contour-like singularities in 2-D images [15]. The AF is a smooth low resolution function in the direction of the contour, and behaves like a wavelet in the orthogonal (singular) direction. That is, the AF is built on Gaussian functions along one direction, and on second derivative of Gaussian functions in the orthogonal direction. The structure of AF is very special for capturing the orientation of palmprint image. The AF has the following general form

$$G(u,v) = (4u^2 - 2)\exp(-(u^2 + v^2)) \qquad (1)$$

where (u,v) is, in this case, the plane coordinate and can be obtained in the following way.

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} 1/\alpha & 0 \\ 0 & 1/\beta \end{bmatrix} \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x - x_0 \\ y - y_0 \end{bmatrix} \qquad (2)$$

Where $[x_0, y_0]$ is the center of the filter, the rotation θ, to locally orient the filter along palm contours and α and β are to adapt to contour type. The choice of the Gaussian envelope is motivated by the optimal joint spatial and frequency localization of this kernel and by the presence of second derivative-like filtering in the early stages of the human visual system. It is also motivated by the presence of second derivative-like filtering in the early stages of the human visual system. Usually, $\beta > \alpha$ is set to better obtain the orientation of palmprints. A 3D visualization of an AF can be seen in Fig.1.

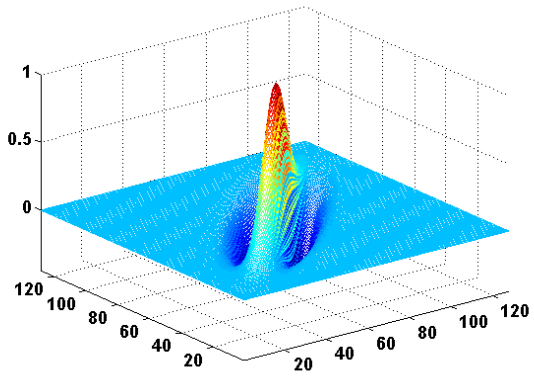
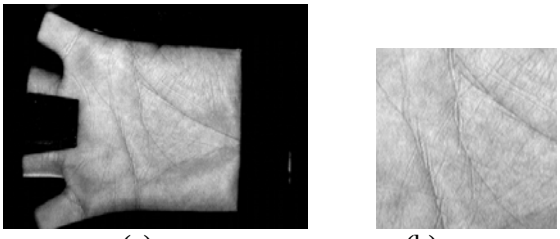


Figure1. Appearance of anisotropic filter

Multiple Binary Orientation Template aims to exact all the orientation information of palmprint [15]. More concretely, let $\boldsymbol{I}$ denote the preprocessed image, the orientation co-occurrence vector (OCV) can be obtained by the following formula

$$F = I * G(u,v) \qquad (3)$$

Where "*" is an operator of convolution According to the[15], six filters with orientations $\theta_p = p \times \pi / 6$, $p = \{0,1,\mathrm{L}\ ,5\}$ could be a better choice. For each local region in palmprint, the OCV can be obtained via by concatenating the normalized responses along six directions. After binarization, we get the palmprint template- Multiple Binary Orientation Template. Fig. 2 shows a palmprint image and its extracted Multiple Binary Orientation Template.



(a) (b)

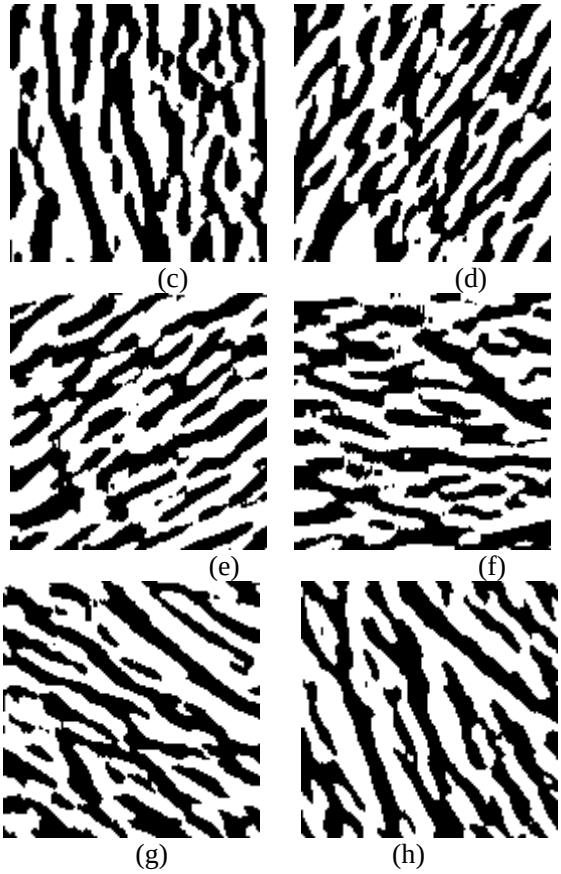


Figure 2. A palmprint image and its Multiple Binary Orientation Template features. (a) Original palmprint image; (b) its region of interest (ROI); (c–h) are the binarized feature maps by six AR filters with orientations are 0^0, 30^0, 60^0, 90^0, 120^0 and 150^0.

III. CANCELABLE MULTIPLE BINARY ORIENTATION TEMPLATES FOR PALMPRINT VERIFICATION

Chaos is a deterministic and random-like process, which is ubiquitously present in the world. Because of its random-like behavior, sensitivity to initial conditions and parameter values, ergodicity, and confusion and diffusion properties, chaotic cryptography has become an important branch of modern cryptography. Khan and Zhang proposed an efficient and practical chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices, which provide biometric template protection over insecure networks[16]. In this section, we present chaos-based cancelable palmprint recognition system, in which the rare palmprint templates can efficiently work in multiple applications. The Hamming distance is applied for match. The matching score(normalized Hamming distance) is used as a classification tool. If the score is smaller than a certain level, the two palmprints would be thought form the same user. To generate cancelable template, the real multiple orientation texture template is encrypted with chaotic stream cipher based on the FFNDF via exclusive OR operation. Fig.3 gives the block diagram of cancelable palmprint verification system.

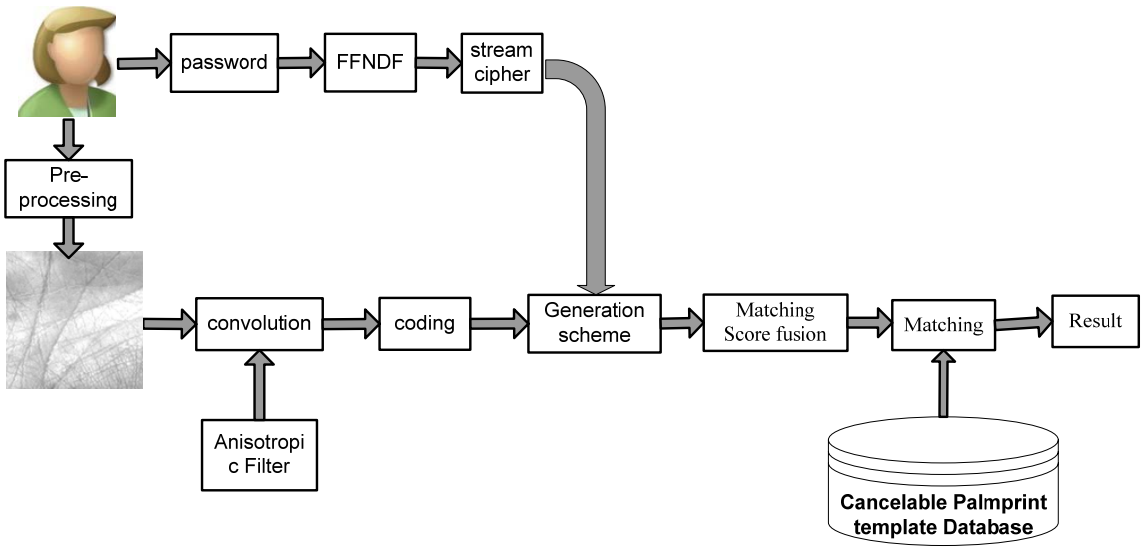


Figure 3. Block diagram of cancelable palmprint verification system

A. Cancelable Palmprint Templates Security and User's Privacy

The template can be protected by the chaotic stream cipher. Another advantage is that the randomness and independence of the obtained cancelable palmprint template are enhanced. The probability of "0" (p0) in the cancelable template approximates to p1, that is, $p_0=p_1=0.5$. From the theory of probability, the matching scores between the cancelable encrypted templates which are exacted from different palms are:

$$s = 1 - p_0^2 - p_1^2 = 1 - 0.5^2 - 0.5^2 = 0.5 \qquad (7)$$

While the hamming distances between the cancelable templates from the same palms are the same with that of the original templates. The XOR operations can maximally increase the inter-class divergence of different palms while maintaining intra-class distance of the same

palms. Therefore, the standard deviation of inter-class population would be decreased, that is, the discriminative ability is improved and the performance of the authentication system would be better.

B. The Fusion Rule and Cancelable Palmprint Authentication Frame

Of course, the database stores the cancelable palmprint templates. In the matching phase, the Hamming distance is employed to measure the similarity of different palmprint and can be performed in the encryption domain directly. To speed up the matching process, every orientation in the Multiple Binary Orientation Template is computed independently in parallel. During computation of each orientation(dimension) in the Multiple Binary Orientation Template, to account for alignment imperfections, we need to translate one of the templates vertically and horizontally and then perform the matching again. The ranges of the vertical and horizontal translations are defined from -2 and 2. The minimum of these matching scores is regarded as the final matching score. At last, the final match score can be obtained by fusing that of six different orientations at the matching score level. Usually, there are common five rule rules[17]:

(a)Maximum Rule $s = max(s_1, s_2, \mathrm{L}\ , s_6)$

(b) Minimum Rule $s = min(s_1, s_2, \mathrm{L}\ , s_6)$

(c) Median Rule $s = median(s_1, s_2, \mathrm{L}\ , s_6)$

(d) Sum Rule $s = \dfrac{s_1 + s_2 +, \mathrm{L}\ , + s_6}{6}$ (8)

(e)Product Rule $s = (s_1 \times s_2 \times, \mathrm{L}\ , \times s_6)^{\frac{1}{6}}$

Where s_i is the matching source of one texture orientation and it can be obtained by the normalized hamming distance. The S_{final} is between 0 and 1. The fused match score which contain contribution of multiple directional features can provide an exactly classification evidence. The Sum and Product fusion rules can provide both higher recognition performances for a given threshold. However, the computation of Sum fusion rule is more simply than the Product fusion rule. Therefore, the Sum rule is employed in this scheme.

The ultimate purpose of the proposed framework can be mainly divided into the following steps:

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 part of a palmprint image.

Step 2: The preprocessed palmprint image is passed to an anisotropic filter banks using six different orientations 0^0, 30^0, 60^0, 90^0, 120^0 and 150^0. The filtered image is coded to one bit for each orientation. And we obtain six bits for one image sample.

Step 3: The chaotic stream cipher generated from FFNDF, in which the user posses the initial values and control parameters, is employed to XOR-ed the coded palmprint texture templates.

Step 4: The matching score is calculated in each orientation using Hamming distance. Finally the six matching scores fused on the matching score level act as the final score.

Step 5: A distance measure is used to measure the similarity of two palmprints.

C. Security Analysis of the Cancelable Authentication System

Our basic design depends on two factors: a biometric and a physical token. If only one factor is compromised, the biometric authentication system can still run in a secure manner. If the biometric becomes known, this does not help the attacker because the key is randomly generated. The cancelable templates are stored either distributed on a smart-card or centrally database. In a central database of templates, the template is encrypted and the key is known to the user, therefore, our scheme can resist administrator attack.

The system can provide different tokens from one application to another, which also prevents cross-matching databases, thereby ensuring the user's privacy. If the palmprint template is compromised, it can easily revoke a compromised template and reissue a new one based on the same palmprint just with another token, thus providing revocability. It is impossible to obtain the original palmprint image from the cancelable template since the encoding of the palmprint orientation feature is non-invertible, which prevents an adversary from creating a physics spoof of the palmprint from a stolen template. Once all the token are shared or open, the palmprint system reverts to the original palmprint authentication system. What is important, this does not degrade the authentication performance of the biometric system. In a word, our cancelable palmprint template scheme has diversity, revocabil ity and performance is not affected in the stolen-token case. It could be seen as a good cancelable biometrics authentication scheme. Ability of template re-issuance will be disused in section 4.

IV. EXPERIMENTS AND DISCUSSIONS

A second-order FFNDF is selected to generate chaotic stream cipher and the simulation conditions are given in the following. The coefficients are 3.57 and 4.0 for the part of feedback, and the coefficients 5.70 and 7.0 for the forward part. The initial value is 0.6587. The state values are 0.3564 and -0.8021, respectively. The control parameter is 0.45 of the piecewise linear maps. The experiments are conducted on a personal computer with an AMD processor (2.6GHz) and 2GB RAM configured with Microsoft XP operating system, in which the test platform are Matlab 7.6 with image processing toolbox and Microsoft Visual C++6.0

All the experiments are performed on the Hong Kong PolyU palmprint database contains 7752 grayscale images captured from 193 individuals, 386 different palms. The performance of a verification method is often measured by false acceptance rate (FAR), false reject rate (FRR) and equal error rate (EER). With regard to the evaluation of the separation between the genuine and

imposter 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. d' prime is defined as following:

$$d' = \frac{\mu_1 - \mu_2}{\sqrt{\left(\sigma_1^2 + \sigma_2^2\right)/2}} \qquad (9)$$

Where μ_1 and σ_1 are the mean and variance of the match scores of genuine populations，respectively；μ_2 and σ_2 are the mean and variance of the match scores of imposter populations，respectively.

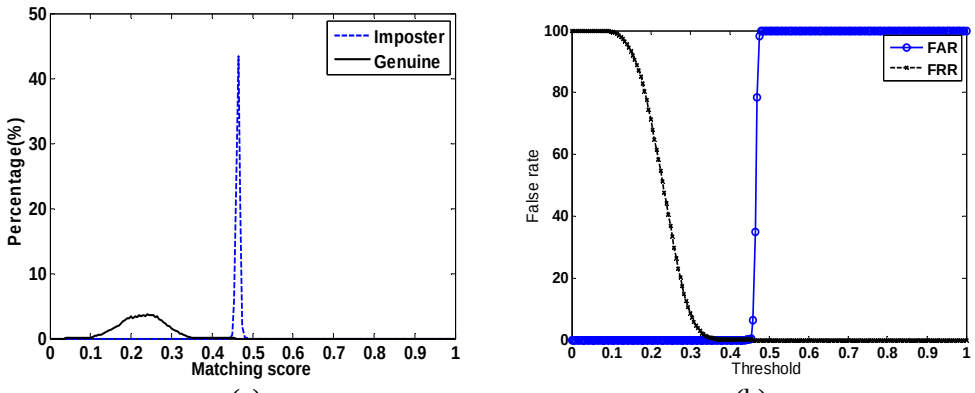
A. Verification Test

To obtain the verification accuracy of our palmprint system, each of the palmprint images is matched with all the others in the database. A matching is noted as a genuine matching if two palmprint images are from the same palm. The total number of matching is 30,042,876. None of the matching scores is zero. The failure to enroll rate is zero. The number of comparisons that have genuine matching is 74,086, and the rest are imposter matching. To demonstrate the effectiveness of the cancelable Multiple Binary Orientation Template, a series of comparison experiments are carried out in the following.

Compared with original Multiple BinaryOrientation Template, the peak/mean value of imposter matching (the peak value approximates the mean value for the imposter matching nearly satisfies symmetrical distribution) increases from 0.4462 to 0.4666 while the genuine matching scores distribution is maintained as shown in Tab.1. Corresponding, the variance of the imposter matching scores reduces by roughly an order of magnitude since the randomness and independent of encryption template is enhanced. That is, the variance decreases from 1.2806×10^{-4} to 1.8051×10^{-5}. d'-primes is also computed and is increased by 0.6689 via matching in the encryption domain. The peak value of the imposter matching scores is smaller than 0.5 since the translated templates are used to compute the distances to overcome imperfect preprocessing. The encrypted peak value of imposter matching scores is also bigger than that of unencrypted. To employ multi-orientation of palmprint, a SUM rule is a leading candidate fused scheme since the feature exacting and matching methods are the same. More information is used can reduce the variance by 3~5 times as illustrated in Tab.1.

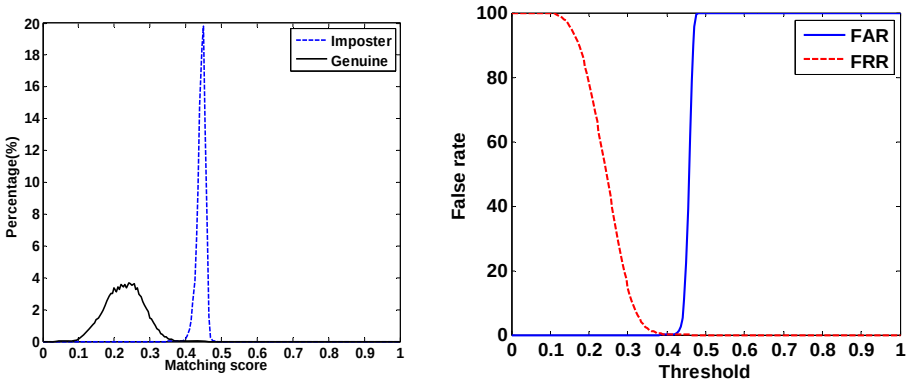
TABLE I
VARIETIES BETWEEN MATCHING IN ORIGINAL AND CANCELABLE TEMPLATE

orientation	original template					cancelable template				
	Intra-class(genuine)		Inter-class(imposter)		d' prime	Intra-class(genuine)		Inter-class(imposter)		d' prime
	mean	variance	mean	variance		mean	variance	mean	variance	
0^0	0.2241	0.0038	0.4426	4.2919×10^{-4}	4.7593	0.2241	0.0038	0.4670	9.7671×10^{-5}	5.5129
30^0	0.2208	0.0035	0.4456	4.3011×10^{-4}	5.0972	0.2208	0.0035	0.4664	9.4799×10^{-5}	5.8236
60^0	0.2325	0.0031	0.4476	3.0145×10^{-4}	5.2200	0.2325	0.0031	0.4665	9.6776×10^{-5}	5.8560
90^0	0.2477	0.0035	0.4480	3.2386×10^{-4}	4.5736	0.2477	0.0035	0.4671	9.9133×10^{-5}	5.1629
120^0	0.2348	0.0033	0.4479	2.9646×10^{-4}	5.0342	0.2348	0.0033	0.4663	9.3952×10^{-5}	5.6303
150^0	0.2234	0.0036	0.4456	3.8457×10^{-4}	5.0037	0.2234	0.0036	0.4662	9.3386×10^{-5}	5.6817
Fused	0.2305	0.0027	0.4462	1.2806×10^{-4}	5.7480	0.2305	0.0027	0.4666	1.8051×10^{-5}	6.4169



(a) (b)

Figure 4. Verification test results with different tokens. (a)Genuine and imposter distributions of matching score;(b)FAR and FRR curves.



(a) (b)

Figure 5. Verification test results in the token-stolen scenarios. (a)Genuine and imposter distributions of matching scores. (b) FAR and FRR curves.

From Fig.4, the genuine and imposter matching scores distributions can be separated well at the threshold between 0.37 and 0.45. However, the operation threshold in this range is not the best in the applications since the FAR is very high in the range of 0.40 ~ 0.45 in the token-stolen case as illustrated in Fig.5. Therefore, considering all the aspects, the optimized threshold in our system is between 0.37 and 0.39. More interesting, the FRR within the cancelable palmprint template is zero while GAR is very high (GAR is 99.88% when the threshold is set 0.39) if the operating range 0.37 ~ 0.39. The threshold in this range leads to the security level very high and a user may try many times to reduce the FAR in the real systems.

At last, Fig.6 depicts the corresponding Receiver Operation Characteristics (ROC) curves, which is a plot of false reject rate against false acceptance rate. The results of our approach and other approaches, such as Cancelable CompCode([8]), Orthogonal Line Ordinal Code(OLOC) [18]and RLOC [19] are compared in Fig.7 and Table 2. From Fig.6 and Tab.2, our proposed scheme is zero EER which achieves perfect separate genuine match and imposter match. The clear separation indicates that our approach results in dramatically reduced error rates in comparison to user versus imposter classification. Even in token–stolen scenario, the EER of our scheme is 0.07%, near zero. Especially, the genuine acceptance rate of the proposed approach is about 1.49 % higher than that of Ordinal Code, 1.19% higher than that of RLOC and 2.39% higher than that of Cancelable Competitive Code while the FAR is 1×10^{-4}%.

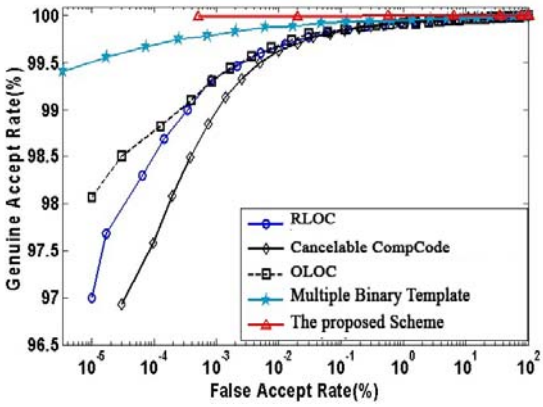


Figure 6. The receive operating characteristic (ROC) curves.

TABLE. II
COMPARISON OF DIFFERENT PALMPRINT VERIFICATION SCHEMES

	Ordinal Code[18]	Cancelable Competitive Code[8]	RLOC[19]	Multiple Binary Orientation Template	The proposed Scheme
FAR(%)	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}
FRR(%)	1.5	2.4	1.2	0.30	0.01
EER(%)	0.14	0.16	0.14	0.07	0.006

B. Template Re-issuance Ability of the Palmprint Authentication System

To generate cancelable palmprint templates based on AFs, we use a chaotic cipher to encrypt the palmprint templates. Thus, the capability of palmprint template re-issuance is characterized by the key space of the employed chaotic cipher. Numerical experiments show that the attractor of NDF expands evenly over phase and the system is sensitive to all components of key. Key space size is the total number of different keys that can be used in the encryption. A good cancelable biometric template scheme indicates that the cancelable templates are completely sensitive to all the secret keys and the ability of template re-issuance should be large enough to make brute-force attacks infeasible.

The FFNDF is very sensitive to initial values and control parameter in its chaotic phase, which ensures the key sensitivity of the encryption scheme. Take the orientation 30^0 for an example, Fig.8 illustrates the processed palmprint image and its cancelable template. The difference of key between the two cancelable templates in Fig.7(c) and Fig.7(d) is 10^{-15}. The cancelable palmprint template is the noise-like feature images in

Fig.7(c) and Fig.7(d) and therefore it is unreadable. The test which calculates the ratio of different bits between the two cancelable palmprint templatess shows that about 50.47%. The freely chosen key of the proposed scheme consists of the control parameters and the initial value and state values of the FFNDF. According to Fig. 8, the sensitivity to initial value key component is 10^{-15}. And the sensitivities to other key components are with 10^{-16}. Also consider the value ranges of components, i.e. the trajectory of FFNDF is between -1 and 1. Therefore, the key space is $2\times10^{15+16\times3}=2\times10^{63}=\approx 2^{210}$, which is large enough to resist the exclusive key search. That is, the re-issuance ability of the cancelable plmprint template is 2^{210}.

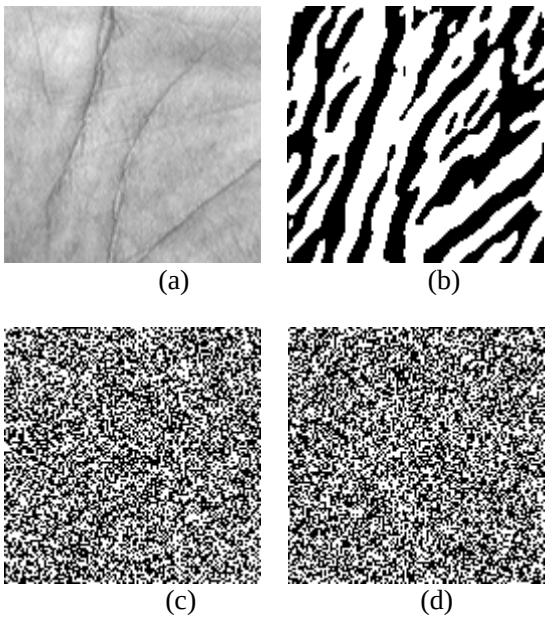


Figure 7. (a)Original palmprint and (b)its binary orientation template. (30^0);(c) cancelable binary orientation template. The key is (0.6587, 0.3564,-0.8021) (d) cancelable binary orientation template. The key is ($0.6587+10^{-15}$, 0.3564,-0.8021)

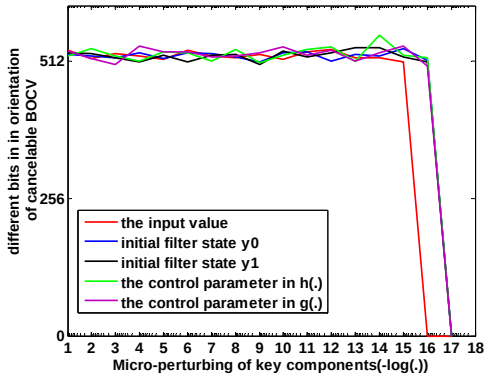


Figure 8. key sensitivity test

C Speed Analysis of the Palmprint Authentication System

Due to the symmetric structure of FFDNF, the chaotic stream cipher based on FFNDF very suitable for hardware implementation. It should be stressed that in hardware implementation, its computations are sharply declined. More importantly, the FFNDF with uniform distribution has good cryptographic properties. The chaotic stream cipher based on FFNDF has large key space. Therefore, the proposed scheme is more desirable in a comprehensive consideration or from strict cryptographic viewpoint.

The software implement of execution time for ROI extraction, feature extraction and matching is about 95 ms, 120 ms, and 1.9 ms respectively. The total execution time of verification is about 0.2 s, which is fast enough for real-time application. However, during the authentication stage, the implementation of feature exacting and matching stage, every orientation in the implementation can be computed in parallel. If the system is implemented in parallel, the executive time is faster than cancelable CompCode[8].

V. CONCLUSION

A high performance and secure palmprint template protection scheme and its authentication system are proposed in this paper. Firstly, a novel 2D anisotropic filter is used to obtain binary orientation texture，which can efficiently represent multiple orientations for a local region of palmprint. And then the binary palmprint features are XOR-ed by a chaotic stream cipher based on FFNDF to generate cancelable palmprint templates, which has large re-issuance ability. The cancelable templates preserve the intra-class variations while reducing the inter-class variations when the genuine tokens are used. Also, the mean value of imposter distribution would be large for the random of the cancelable templates is enhanced. And the matching implemented in the encrypted domain is very efficient and secure for protecting user's privacy. In one the worst case, for example, all the users share or lose their tokens, the result reverts to the original palmprint authentication performance since we use hamming distance is preserved. Even in the stolen-token case, the result just reverts to the original performance without loss in performance and it can still achieve state-of-the-art authentication accuracy, i.e., the EER is 0.07%.. Experiments on PolyU Palmprint Database confirm the effectiveness of the proposed approach.

ACKNOWLEDGEMENTS

This work is supported by grants by National Natural Science Foundation of China (Grant No. 61070163), by the Shandong Province Outstanding Research Award Fund for Young Scientists of China (Grant No. BS2011DX034) and by Shandong Natural Science Foundation (Grant No. ZR2011FQ030).

REFERENCES

[1] A.Kong, D.Zhang, M.Kamel，"A survey of palmprint recognition," Pattern Recognition,vol.42,No.7, pp.1408-1418, 2009

[2] N.Ratha, J. Connell and R.Bolle, "Enhancng security and privacy in biometric-based authentication systems," IBM

Systems Journal, vol.40,No.3, pp.614 – 634,2001.
[3] A.K.Jain, K.Nandakumar and A.Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, January 2008.
[4] A.Juels, M.Wattenberg, "A fuzzy commitment scheme", Proceedings of the Sixth ACM Conf. on Comp. and Comm. Security, pp. 28-36, 1999.
[5] A Juels and M Sudan. A Fuzzy Vault Scheme, IEEE International Symposium on Information Theory, 2002.
[6] Y.C.Feng, P. C.Yuen and A.K.Jain, "A Hybrid Approach for Generating Secure and Discriminating Face Template", IEEE Transactions on Information Forensics and Security, vol.5,No.1, pp. 103 – 117,2010.
[7] Connie T, Teoh A B. J, Goh M, Ngo D, PalmHashing: a novel approach for cancelable biometrics, Inf. Process. Lett. 2005: 93 (1): 1–5.
[8] A.Kong, D.Zhang, M.Kamel., "Three measure for secure palmprint identification", Pattern Recognition, vol.41,No.4, pp.1329–13372008.
[9] L.Leng, J.S.Zhang, "Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security", Journal of Network and Computer Applications, vol.34,No.6, pp.1979–1989,2011.
[10] A.Kong, K.H.Cheung, D.Zhang, M.Kamel, "An analysis of Biohashing and its variants", Pattern Recognition, vol.39,No.7, pp.1359–1368,2006.
[11] A.Kong, K.H.Cheung, D.Zhang, M.Kamel, "A study of brute-force break-ins of a palmprint verification system, "IEEE Transactions on Systems, Man and Cybernetics, Part B vol.36,No.5, pp. 1201–1205.,2006.
[12] L.Leng J.S.Zhang, M.K.Khan, "Cancelable PalmCode generated from randomized Gabor filters for palmprint template protection," Scientific Research and Essays, Vol. 6,No.4, pp. 784-792, 2011
[13] J.S.Zhang, X.M.Wang, W.F.Zhang. "Chaotic keyed hash function based on Feed forward-Feedback nonlinear digital filter". Phys Lett A. Vol.362,pp.439–448,2007.
[14] PolyU Palmprint database available: http://www4.comp.polyu.edu.hk/~biometrics/.
[15] P.Vandergheynst, P.Frossard. "Efficient image representation by anisotropic refinement in matching pursuit". In: Proceedings of IEEE on ICASSP. Salt Lake City, UT, USA, Vol(3):1757~1760, 2001.
[16] M.K.Khan, J.S.Zhang. X.M.Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices". Chaos, Solitons and Fractals, Vol.(35),No.3,pp. 519-524, 2008.
[17] J. Kittler, M. Hatef, R.P.W. Duin, J. Matas, "On combining classifiers", IEEE Trans. Pattern Anal. Mach. Intel.Vol. 20 No.3, pp.226–239,1998.
[18] Z.Sun, T.Tan, Y.Wang, S.Z.Li, "Ordinal palmprint representation for personal identification", in: IEEE Proceedings .CVPR,pp.279–284, 2005.
[19] W.Jia, D.S. Huang, D.Zhang, "Palmprint verification based on robust line orientation code", Pattern Recognition,Vol.41, pp. 1504–1513,2008.

Hengjian Li, received the B.S. and Ph.D. degrees from Southwest Jiaotong University, Chengdou, Sichuan Province, P.R.China in 2004 and 2010 respectively.
Currently, he is an assistant researcher in theShandong Provincial Key Laboratory of computer Network, Shandong Computer Science Center,Jinan, Shandong Province, P.R.China. His research interests involve biometric recognition, image forensics, information security and computer forensics.

Lianhai Wang, professor at Shandong computer Science center, Supervisor of master. He is an outstanding contributions expert of Shandong provience and was awarded with special allowance from the national government. He research interests involve pattern recognition, information security，live forensics and memory analysis.