Bits Extraction for Palmprint Template Protection with Gabor Magnitude and Multi-bit Quantization

Meiru Mu, Xiaoying Shao,
Luuk Spreeuwers, Raymond Veldhuis
Signals and Systems group,
University of Twente
Enschede, The Netherlands
{M.Mu, R.N.J.Veldhuis}@utwente.nl

Qiuqi Ruan
Institute of Information Science,
Beijing Jiaotong University
Beijing, P.R. China
qqruan@bjtu.edu.cn

Abstract

In this paper, we propose a method of fixed-length binary string extraction (denoted by LogGM_DROBA) from low-resolution palmprint image for developing palmprint template protection technology. In order to extract reliable (stable and discriminative) bits, multi-bit equal-probability-interval quantization and detection rate optimized bit allocation (DROBA) are operated on the real-valued features, which are resulted from representing the palmprint image by simple statistics on logarithmic transform of Gabor magnitude (LogGM). Assuming the Helper Data Scheme with a BCH error correction coding is adopted for template protection, the performance is evaluated on the Hong Kong PolyU palmprint database. The experimental results show that our method can achieve low Bit Error Rate (BER) resulted from genuine binary strings so that a long secret key (around 100 bits) is allowed to be combined for security, and low False Rejection Rate and low False Acceptance Rate (FRR/FAR) when the key retrial process is considered as a Hamming distance classifier, which verify the high stability and strong distinctive ability of our extracted palmprint binary string.

1. Introduction

Biometric authentication technique, based on the natural linkage of biometric traits and individual identity, has received world-wide attention and gained significant development in the last decades. Varieties of biometric recognition systems are being used in the kinds of government and commercial applications around the world. Although most of them are successful, it raises concerns about system security and potential user privacy [1]. For higher levels of security, two main approaches have been developed to secure biometric template including biometric feature transformation by a one-way function, and binding the biometric template with a cryptographic key. As to the latter, the key-retrieval rate and allowed key length are the most important factors which can often be trade-off against each other to meet operational constrains. In this paper, our study is based on the Helper Data Scheme (HDS) for binding the palmprint template with a cryptographic key [2]. For its successful application of HDS, the biometrical traits are required to be presented as fixed-length binary strings, which are usually noisy due to the intra-class varieties. To bridge the gap between fuzziness of genuine biometric strings and exactitude of cryptographic key, Error Correction Code (ECC) is designed to overcome the biometric variance. So far, most of template protection attempts, based on sorts of biometric modalities including iris, fingerprint, face, voice, and handwriting signatures, suffer from an excessive False Rejection Rate (FRR) - usually over 20%, or a small allowed key length - smaller than 70, which is unacceptable for practical applications [3]. The well-known difficulty is how to represent the biometrical traits as fixed-length binary strings, which can be of low Bit Error Rate (BER) for genuine samples, and of strong distinctive ability. The main obstacle is that most of genuine biometric strings provide BER as high as 40%, which is far beyond the error-correcting capability of the currently existed ECC module (less than 25%).

In this paper, a framework of binary feature extraction for palmprint template protection is surveyed, which includes real-valued feature extraction, binary quantization on single feature component and reliable bit selection. Emphasis is put on extracting reliable (*i.e.* stable and discriminative) bits as a binary palmprint representation, which is expected to achieve low key-retrieval error rate (*i.e.* FRR and FAR), and provide low BER for genuine samples so that a secret key length of more than 70 is allowed to be bound, given the system works under the Helper Data Scheme with BCH codes for error correcting. The following issues are

978-1-4799-0310-8/13/$31.00 ©2013 IEEE

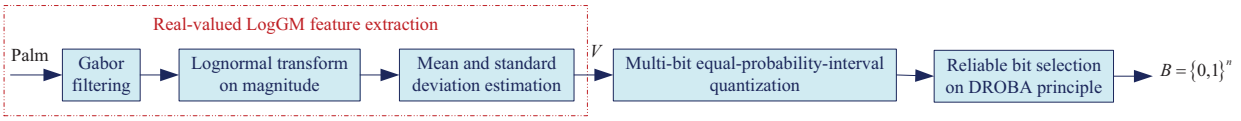

Figure 1: The flow chart of our proposed binary feature extraction method for palmprint template protection.

mainly considered:

(1) For the real-valued feature extraction from palmprint image, Gabor filtering is exploited in this study. For the typical palmprint recognition system (unprotected), the coding-based methods are considered to be most promising, which are generally based on the pixel-to-pixel quantization of wavelet filtered responses and can achieve high recognition accuracy [4]. However, for palmprint template protection system, those pixel-to-pixel encoded bits are too noisy to bind a secret key. Therefore, we resort to the sub-block partition based Gabor magnitude statistical features (denoted by LogGM) [5], which are expected to be more stable. In addition, for achieving bits of statistically independent and identically distributed bits so as to maximize the attacker's efforts in guessing the target template, we consider to perform PCA and LDA process respectively on LogGM before quantization [6]. Experimental results show that PCA/LDA transform causes that the discriminability of binary string improves while the bit stability heavily declines.

(2) For fixed-length binary string generating, we take the one-bit and multi-bit quantization into consideration which are both based on the fixed equal-probability intervals so as to ensure the bits are identically distributed. After quantizing all the feature components into bits, we select the steady ones by some principle and then concatenate them into a string. Given the same binary string length, multi-bit quantizer could achieve more stable bits of lower BER than one-bit quantizer. While for better FRR/FAR performance, the selected bit number needs to be investigated. Here we resort to the detection rate optimized bit allocation principle (DROBA) for reliable bit selection [6]. The performance comparison with one-bit quantization will be presented in experiments.

(3) With regards to the performance evaluation, the secret key retrieval rate and the allowed maximum key size are considered as the most important factors in this study. Because the secure key retrieval process with an error-correcting operation can be modeled as a threshold classifier based on matching scores by the Hamming distance, we indicate the key retrieval performance by FRR and FAR, which is depended on the distinctive ability of the extracted bits . Given the enrolled and the genuine query palmprint binary strings are denoted by B and B' respectively (B and $B' = \{0,1\}^n$, and generally $B \neq B'$ due to the inevitable noisiness), the system will retrieve the secret key successfully in case $\|B - B'\| \leqslant t$, under the assumption that the BCH (n, k, t) code is used for ECC, where n is binary template size, k is the allowed key length, and t indicates the error correction capacity. Otherwise, a failure message is returned. The stability of binary strings is indicated by BER, which can be formulated as $\frac{\sum(B \oplus B')}{n} \times 100\%$. In order to prevent the secret key from being guessed by exhaustive searching, k is expected to be more than 70 (Having a key of k bits on average will take 2^{k-1} guesses in order to obtain the correct one, hence adding a single bit to the key doubles the adversary's effort).

Taking all these factors into consideration, a novel binary palmprint feature extraction method based on Gabor statistical features and multi-bit fixed-interval quantization on DROBA (denoted by LogGM_DROBA) is proposed for template protection in this paper, whose flow chart is depicted in Fig. 1. Experimental results verify its high efficiency in terms of FAR, RRR, BER, and allowed secret key size given BCH codes are adopted, when compared with methods of the one-bit quantization on LogGM, LogGM and PCA/LDA based quantization, and the promising coding-based methods reported for unprotected palmprint recognition.

The remainder of this paper is organized as follows: in Section 2 the real-valued LogGM feature extraction algorithm is reviewed. Section 3 illustrates the proposed method (denoted by LogGM_DROBA) in detail. Section 4 presents experiments including the performance evaluation and contrast results on the HongKong PolyU palmprint database. Finally, conclusions and outlook are given in Section 5.

2. Brief review of LogGM feature

Gabor filter bank is a powerful tool for characterizing texture image features. Aiming to achieve the rotation and scale invariant image representation, the mean and standard deviation statistics resulted from Gabor responses are reported to be efficient. Inspired by those work, a method denoted by LogGM is presented for palmprint recognition based on the fact that the Gabor magnitude within each filtered subband uniformly approximates the Lognormal distribution [5]. The applied Gabor function is expressed as

following:

$$g_{r,s}(x,y) = \frac{1}{2\pi\sigma^2}\exp\left\{\frac{-(x^2+y^2)}{2\sigma^2}\right\} \times \exp\{2\pi i(u_r x\cos\theta_s + u_r y\sin\theta_s)\}. \quad (1)$$

u_r is the frequency of sinusoidal wave along directional θ_s from x-axis, and σ specifies the Gaussian envelope along x and y axes, which determines the bandwidth of the Gabor filter. Each Gabor function $g_{r,s}(x,y)$ with the parameters (u_r,θ_s,σ) is commonly transformed into a discrete Gabor filter and its direct current is turned to zero, which can be denoted by $\tilde{g}_{r,s}(x,y)$. Given an image $I(x,y)$, The Gabor magnitude (GM) can be expressed by $GM_{r,s}(x,y) = \parallel \tilde{g}_{r,s}(x,y) * I(x,y) \parallel$. It has been empirically found that the lognormal densities fit the GMs very well, and the sub-blocks of each GM are also close to lognormal distribution. Accordingly, a group of Gaussian densities (LogGMs) can be obtained by $LogGM_{r,s}(x,y) = \log(GM_{r,s}(x,y))$, the mean and standard deviation from which are exploited to construct the real-valued palmprint features $V = [v_1, v_2, ..., v_m]$. Following the experimental results in Ref. [5], five-scale and eight-frequency Gabor filters are carried out, and the mean and standard deviation are calculated from 21 sub-blocks. Therefore the number of feature components is $m = 5 \times 8 \times 21 \times 2 = 1680$.

3. Binary LogGM_DROBA feature extraction

With regard to reliable bits extraction from LogGM feature $V = [v_1, v_2, ..., v_m]$, we resort to multi-bit quantization with equal-probability intervals and reliable bit selection on detection rate optimized bit allocation (DROBA) principle [6].

For a single feature component v_i, due to its inter- and intra-class variation, it can be modeled by a background probability density function (PDF) p_b, and a genuine user PDF p_g to indicate the probability density of the whole population and the genuine user, respectively. Assuming p_b and p_g both approximate Gaussian distributions, we have $p_b \backsim G(v_i, \mu_b, \sigma_b)$ and $p_g \backsim G(v_i, \mu_w, \sigma_w)$ as the background PDF and the genuine user PDF respectively. As to the b_i-bit quantization for each v_i, 2^{b_i} intervals are symmetrically constructed around the mean of the background PDF (usually μ_b and σ_b are normalized into $\mu_b = 0, \sigma_b = 1$), with equally 2^{-b_i} background probability mass, which is independent of the genuine user PDF. Gray codes are allocated for each interval so that the Hamming distance between two adjacent quantization intervals is limited to one which results in a better performance of a Hamming distance classifier. The feature component v_i derived from genuine user is expected to fall into one interval which is referred to as the genuine interval. Figure 2 gives an illustration of b_i-bit equal-probability-interval quantization as we described when $b_i = 2$.

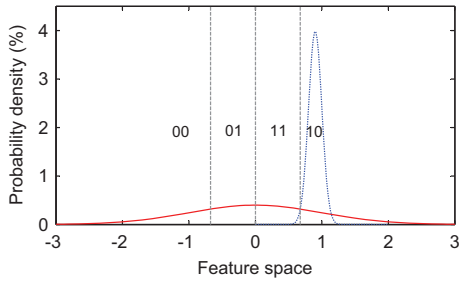

Figure 2: Illustration of the two-bit equal-probability-interval quantization for one feature component v_i. Gray codes are used for coding each interval. The background PDF $p_b(v_i, 0, 1)$ (solid line); the genuine user PDF $p_g(v_i, \mu_w, \sigma_w)$ (dot line, $\mu_w = 0.9$, $\sigma_w = 0.1$ is taken as an example here); the quantization intervals (dash line).

Empirically we know that the stability and discriminability differ for different feature components, *i.e.* p_g differs in (μ_w, σ_w) as v_i varies. Therefore, we choose to allocate more bits for the more stable and discriminative components and less for the others, in case the binary string length is fixed. The quantization performance of v_i with b_i-bit quantization can be defined as the theoretical FAR α_i, FRR β_i and the corresponding detection rate δ_i by the following expressions:

$$\alpha_i(b_i) = \int_{Q_{\text{genuine},i}(b_i)} p_b(v_i)dv_i \quad (2)$$

$$\delta_i(b_i) = \int_{Q_{\text{genuine},i}(b_i)} p_g(v_i)dv_i \quad (3)$$

$$\beta_i(b_i) = 1 - \delta_i(b_i) \quad (4)$$

where $Q_{\text{genuine},i}(b_i)$ represents the genuine user interval when b_i-bit quantization is carried out.

In this paper, about the LogGM feature V, we have m feature components. For b_i-bit quantization, $b_i \in \{0,1,2,3\}$ is considered. Let n denote the number of selected reliable bits, $n \in \{127, 255, 511, 1023\}$ is investigated complying with the string form of BCH error correcting code, and $70 < n < 1680$ is expected. In this paper, 2^{69} security is sought, *e.g.* the secret key k size is expected to be larger than 70. That is why $n > 70$ is expected. According to the DROBA principle, the optimal bit assignment $\{b_i^*\}$, which indicates the number of quantization bits for every single feature $\{v_i\}, i = 1, ..., m$, can be expressed as:

$$\{b_i^*\} = \arg\max_{\sum_{i=1}^{m} b_i = 1} \delta(b_1, ..., b_m) \quad (5)$$

Assuming that all the m feature components are indepen-

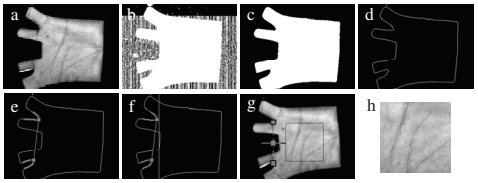

Figure 3: (a) A typical palmprint image from HongKong PolyU Palmprint Database; (b)-(f) illustrate the registration and region-crop processes we carried out.

Table 1: Examples of the BCH codes and their corresponding error correcting capability. Codeword size (n), secret key length (k), and the correctable bits (t).

BCH (n, k, t) [bits]	Error correcting capability ($\frac{t}{n}$)
$(127, 71, 9)$	7.09 %
$(255, 71, 29)$	11.37 %
$(511, 76, 85)$	16.63 %
$(1023, 76, 187)$	18.28 %

dent, Eq. 5 can be rewritten as:

$$\{b_i^*\} = \arg \max_{\sum_{i=1}^{m} b_i = 1} \prod_{i=1}^{m} \delta_i(b_i) \qquad (6)$$

To solve this optimization problem, we applied the Greedy Search approach presented in Ref. [6]. With regards to the calculation of detection rate $\delta_i(b_i)$, we firstly subtract the mean and normalize the standard deviation on the entire enrolled samples so that p_b approximate $G(v_i, 0, 1)$ density. Then the mean μ_w and the standard deviation σ_w are estimated from the enrolled samples for each palm respectively.

Finally, following the knowledge of $\{b_i^*\}$, for each feature component, we carry out the b_i-bit ($b_i \in \{0, 1, 2, 3\}$) equal-probability-interval quantization by coding interval with the Gray code, and then concatenate them to generate a binary string $B = \{0, 1\}^n$ of length n as our proposed binary palmprint representation.

4. Experiments

4.1. Experimental setup

The HongKong Polytechnic University (PolyU) palmprint database is used to test our proposed method [7]. They were captured by a CCD sensor from 386 different palms and collected in two sessions with two different illumination conditions. There are 3889 images in session one and 3863 samples in session two respectively. There is one palm which has only one sample captured in session two. So we take it out. The other 385 palms are used for our experiments. The resolution of original captured images is 384×284 pixels at 75 dpi. By preprocessing each image (as shown in Fig. 3), the central region size of 128×128 is cropped for feature extraction.

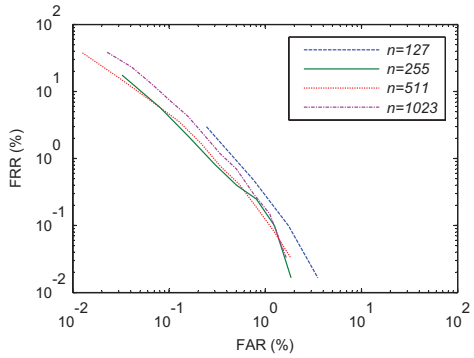

Figure 4: The ROC performances of the proposed binary string extraction method when the string length n is set to 127, 255, 511, and 1023 respectively.

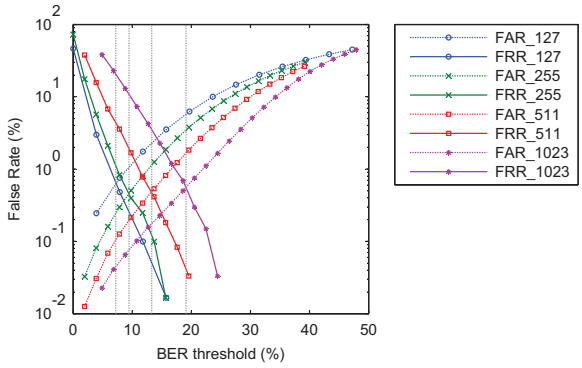

Figure 5: The FAR and FRR performances of the proposed binary string extraction method when the string length n is set to 127, 255, 511, and 1023 respectively.

For the training-evaluation-set split in all the experiments, 185 palms are randomly chosen for training and the remaining 200 palms for evaluation, which is repeated six times. For training, all the samples (around ten) from the same palm in session one are used. For evaluation, all the samples are from session two. About the enrollment-test split on the samples from one palm, five samples are randomly selected for enrollment and the remaining ones for test. All the test samples in the test set are matched with the enrolled samples by Hamming distance so that totally we get 6043 genuine scores and 1,202,557 imposter scores.

Table 2: Performance of the proposed method when the string length n varies. Key size (k). Correctable bits (n).

n	EER (%)	BER threshold $\frac{t}{n}$ @ EER point	Allowed maximum k @ EER point	FRR (%) @ FAR=0.1%	BER threshold $\frac{t}{n}$ @ FAR=0.1%	Allowed maximum k @ FAR=0.1%
127	0.62	7.09 %	71	12.89	1.57 %	106
255	0.45	9.41 %	99	3.97	4.71 %	163
511	0.49	13.31 %	76	4.68	7.05 %	241
1023	0.58	19.26 %	46	7.81	10.56 %	228

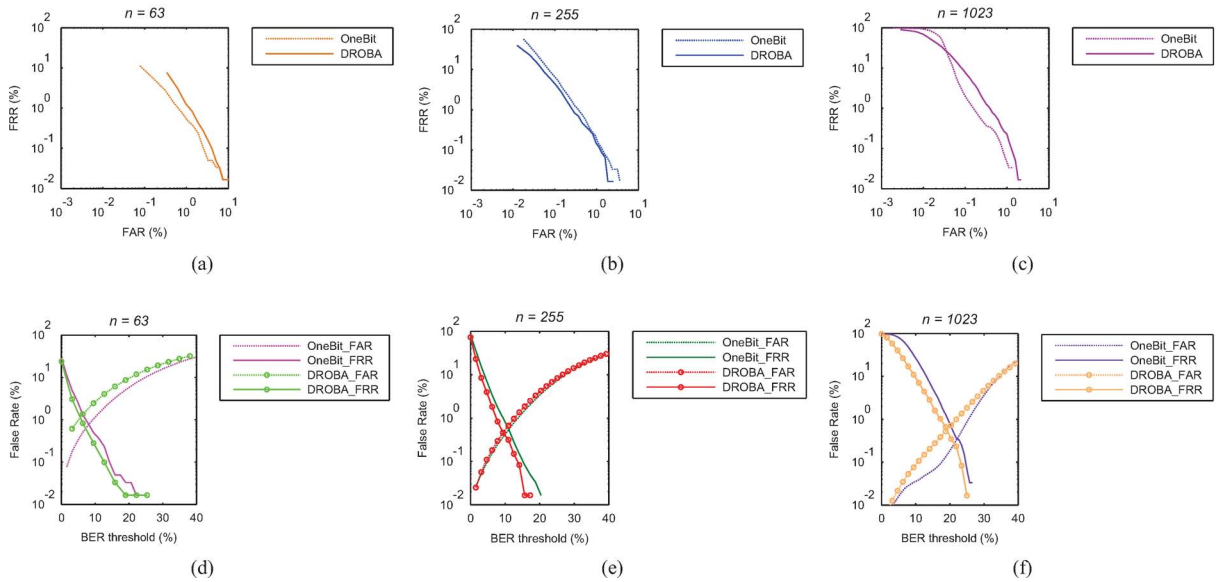

Figure 6: Performance comparison between one-bit quantization and DROBA based multi-bit quantization (our proposed method) on the same LogGM features. The binary string length n is set to 63, 255 and 1023 respectively.

4.2. Performance evaluation

To evaluate the key-retrieval capability of our proposed binary palmprint representation (denoted by LogGM_DROBA) when utilized for template protection system, we assume the Helper Data Scheme with the BCH code for error correcting is carried out. Table 1 shows some examples of (n, k, t) settings for BCH code. n is an integer of the form $2^N - 1$ for some integer $N > 2$. To ensure higher security of the key, the BCH codes with $k > 70$ are considered in our experiments. Note, t increases as n grows but lies lower than 20% of the binary vector. The stability and discriminability of the LogGM_DROBA string are dependent on the number of selected reliable bits. To investigate the impact of the binary string length on the FAR, FRR, and k size, we evaluated the verification performances at various binary string lengths.

The ROC curves are shown in Fig. 4 for the proposed binary representation method, given n is set to 127, 255, 511, and 1023 respectively. As can be seen from it, the performance of bit discriminative ability firstly improves and then starts to degrade as n increases from 127 to 1023. The improvement could be because more discriminant information is exploited when more real-valued LogGM feature components are selected for extracting bits. However, as the number of selected feature components for bit extraction increases, the discriminability of binary string decreases. It could be explained that the computed detection rate following Eq. 3 is less accurate when the selected feature component for bit extraction is less reliable, i.e. its statistical density is more far away from the Gaussian model assumption. The results shown in Fig. 4 suggest that the moderate string length n can be 255 or 511. Besides the discriminability, the stability of bit string is the other important factor, which can be indicated by BER of the genuine matching. Given the string length n, the smaller the BER is, i.e. the less error bits, the larger the allowed key size is. Figure 5 plots the FAR and FRR performances versus the BER threshold

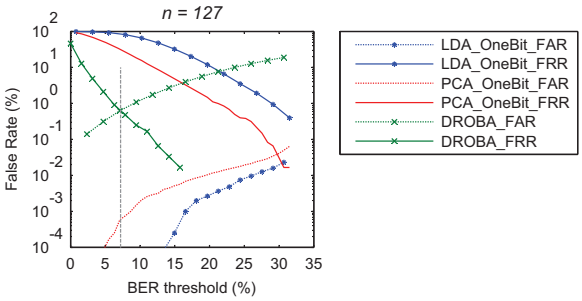

Figure 7: Performance comparison of FAR/FRR and BER. Here, the binary string length n is set to 127 for all of the compared methods.

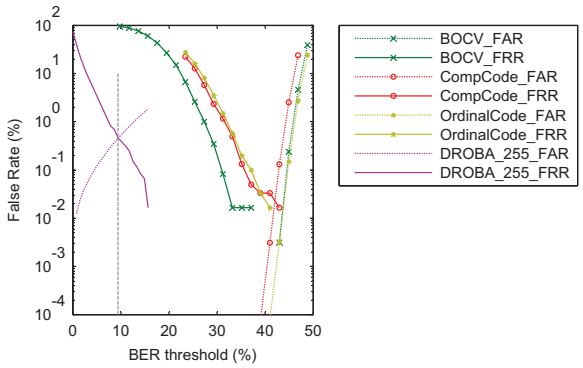

Figure 8: Performance comparison of FAR/FRR and BER between the proposed method and there coding based methods. Here, the binary string length n is set to 255 for the proposed method (denoted by DROBA_255). For others, $n = 32 \times 32 = 1024$.

which is depended on the ECC module and bounded by the applied BCH codes. As can be seen from it, the BER threshold increases as n grows from 127 to 1023 at their corresponding equal error rate (EER) points, where FAR is equal to FRR. However, the error correcting capability also increases as n grows. Corresponding to the results shown in Fig. 5, we tabulate the performance comparison in Table 2. As it shows, the proposed method achieves the best performance at $n = 255$, where the EER is 0.45% corresponding to 9.41% of the BER threshold. By consulting the BCH code dictionary, it is figured out that the allowed maximum key size is $k = 99$. In reality, FAR is required to be much lower for security. Here, the performance at the point of FAR=0.1% is also listed in Table 2. As it shows, our method can achieve the lowest FRR (3.97%) at $n = 255$, where the maximum $k = 163$ according to the BCH codes.

4.3. Compared with other methods

In this section, the results of contrast experiments are presented.

(1) First, we consider the one-bit quantization on the LogGM feature components, for which the reliable bit selection is based on the mean μ_w of genuine PDF after the background PDF is normalized to zero mean and unit standard deviation ($\mu_b = 0, \sigma_b = 1$). Figure 6 shows the comparison of performances between the one-bit quantization and our proposed DROBA based multi-bit quantization when the binary string length n is set to 63, 255, and 1023 respectively. As can be seen from Fig. 6 (a)-(c), given $n = 255$, DROBA based multi-bit quantization outperforms one-bit quantization. But when $n = 63$ and 1023, one-bit quantization achieves better verification performance. From Fig. 6 (d)-(f) we can know that DROBA based multi-bit quantization can achieve better BER performance than one-bit quantization at the same string length n. Accordingly, we can conclude that the proposed method can achieve more steady binary strings than LogGM based one-bit quantization method, given the same n. However, with regards to the discriminability of string, our method performs better only when n is a moderate value.

(2) For our proposed method, the stability and discriminability of binary string are given the top priority. However, dependency of bits is another main concern for security. To obtain independent bits, PCA/LDA projection is widely operated on the real-valued features before quantization [6]. Here, for comparison we carry out PCA and LDA respectively on the LogGM features and then process the one-bit quantization. Due to the LDA process, the number of obtained real-valued feature components is 184 (185 palms for training). Therefore, n ($70 < n < 184$) is set to 127 for all the compared methods in this experiment. As Fig. 7 shows, PCA/LDA process leads to better FAR and FRR performance but worse BER. According to Table 2, we know that BER threshold should be lower than about 7% so that a key could be combined into the binary string. But the PCA/LDA results in a BER of more than 30% at the EER point, which is far beyond the error correcting capability. When the BCH code is operated on the binary string resulted from the features with a PCA/LDA process, the system will derive a large FRR, which is beyond the level acceptable for practical use.

(3) For the unprotected palmprint verification system, many coding based methods have been reported with great FAR/FRR performance such as CompCode [8], Ordinal code [9], BOCV [10] and so on, which represent palmprint by several binary matrices. In order to get the matching score, it is required to shift the whole code matrix by several pixel horizontally and vertically, and match multiple times. In this experiment, each bit matrix is down-sampled by ra-

tio of 4:1 into a plane size of 32×32. The shift range is set to [-2, 2]. Figure 8 shows the comparison of FRR/FAR and BER performance between them and our proposed method. As can be seen from it, in contrast to our proposed method, the coding based methods can achieve lower FRR/FAR but much higher BER (up to 40%). Therefore, although the binary features from coding based methods is highly discriminative, they are not steady enough to be used for template protection system. In addition, the coding based methods require code matrix to shift multiple times for matching score calculation, which challenges the combination of palmprint verification and the template protection.

5. Conclusions and outlook

In this paper a novel binary palmprint feature (bits) extraction method for improving template protection technology is presented. Experimental results demonstrate that the proposed method can achieve high key-retrieval accuracy (i.e. low FRR/FAR) and a long secret key (more than 70 bits) is allowed to be bound for higher security due to its low BER of genuine strings, given a moderate binary string length.

From the contrast experiments, we can conclude that multi-bit quantization on DROBA uniformly achieves lower BER than one-bit quantization in case that both of them are based on LogGM features and the selected reliable bit number is set to the same. However, for the better FRR/FAR performance, the string length n needs to be moderate. A small n leads to weak discriminative ability because many real feature components are not used for bits generation so that some discriminative information is lost. However, a large n also results in poor FRR/FAR performance because some real feature components of less reliable are exploited, whose statistical density might be far away from the Gaussian model assumption so that the computation of detection rate is less correct. LDA/PCA process can provide bits of more independent and better verification accuracy, but leads to worse BER so that a secret key of long length can not be bound. In addition, the well-known coding based methods for unprotected palmprint recognition system have great power to distinguish individuals. But it is challenging to apply them for template protection system because the binary strings from genuine samples they generate provide a high BER which is far beyond the error correcting capability of currently existing ECC technology.

In this paper, emphasis is put on the stability and distinctive ability of extracted bits for template protection system. However, for higher security, the bits independence or correlation issue, the bits error pattern and their corresponding suitable error-correcting codes could be concerned in our future work.

6. Acknowledgments

This work is supported by the Chinese Fundamental Research Funds for Central Universities (Grant No. KKJB11034536), the Chinese Scholarship Council, and the lab of Signals and Systems in University of Twente, The Netherlands .

References

[1] A.K. Jain and K. Nandakumar. Biometric authentication: System security and user privacy. IEEE Trans. Comput., 45(11):87–92, 2012.

[2] P. Tuyls, A. Akkermans, T. Kevenaar, G. Schrijen, A. Bazen and R. Veldhuis. Practical biometric authentication with template protection. In Proc. 5th Int. Conf. Audio- and Video-Based Biometric Person Authentication, volume 3546, pages 436–446, NY, USA, 2005.

[3] F. Hao, R. Anderson and J. Daugman. Combining cryptography with biometrics effectively. IEEE Trans. Comput., 55(9):1081–1088, 2006.

[4] D. Zhang, W. Zuo and F. Yue. A Comparative Study of Palmprint Recognition Algorithms. ACM Comput. Surv., 44(1):2:1–2:37, 2012.

[5] M. Mu and Q. Ruan. Mean and standard deviation as features for palmprint recognition based on gabor filters. Int. J. Patt. Recog. Art. Intel., 25(4):491–512, 2011.

[6] C. Chen, R. Veldhuis, T. Kevenaar, and T. Akkermans. Biometric quantization through detection rate optimized bit allocation. EURASIP Journal on Advances in Signal Processing, 2009:1–16, 2009.

[7] Biometrics Research Centre (BRC) in HongKong. http://www.comp.polyu.edu.hk/ biometrics/

[8] A. Kong and D. Zhang. Competitive coding scheme for palmprint verification. In Proc. 17th Int. Conf. Pattern Recognition, pages 520–523, Cambridge, UK, 2004.

[9] Z. Sun, T. Tan, Y. Wang and S. Li. Ordinal palmprint representation for personal identification. In Proc. IEEE Int. Conf. Computer Vision and Pattern Recognition, pages 279–284, San Diego, CA, USA, 2005.

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