Proceedings of the 33rd WIC Symposium on Information Theory in the Benelux
and
The 2rd Joint WIC/IEEE Symposium on Information Theory and Signal Processing in the Benelux

Boekelo, The Netherlands
May 24–25, 2012

Binary palmprint representation for feature template protection

Meiru Mu Qiuqi Ruan Xiaoying Shao Luuk Spreeuwers Raymond Veldhuis

Institute of Information Science, Beijing Jiaotong University, 100044, P.R. China
University of Twente, Faculty of EEMCS
P.O. Box 217, 7500 AE Enschede, The Netherlands

mumeiru@yahoo.com.cn

Abstract

The major challenge of biometric template protection comes from the intra-class variations of biometric data. The helper data scheme aims to solve this problem by employing the Error Correction Codes (ECC). However, many reported biometric binary features from the same user reach bit error rate (BER) as high as 40%, which exceeds the error correcting capability of most ECC (less than 25%). Therefore, a novel palmprint binary feature extraction method is proposed in this paper. The real-valued features are firstly extracted. Then one-bit quantization and reliable bits selection are processed. For verification multiple samples are required to be enrolled while training is not necessary. Experiments have been carried out on the HongKong PolyU Palmprint database. Results show that our method achieves much lower BER, lower verification error rate and allows a secret key long enough for security.

1 Introduction

It has been widely known that the typical biometrics system encounters some security and privacy problems such as identity fraud, limited-renewability, cross-matching, and leaking sensitive personal information [1]. Biometric template protection system, as a countermeasure to these security and privacy threats, has become an important issue, which requires that biometric data is firstly quantized into a fixed-length binary string as template. Aiming to protect the binary template, the Helper Data Scheme is regarded as a promising way by combing a secret key into the biometric template during the enrollment phase. To identify a query user during the verification phase, the secret key has to be recovered without any error. Due to the intra-class variance of biometric binary templates, Error Correcting Codes (ECC) are employed to correct the error bits. Assuming two binary templates (length of n) from the same user are denoted as S and S', the variance between them can be measured by Hamming distance $\frac{S \oplus S'}{n}$, which we defined as Bit Error Rate (BER). So far, most of the reported biometric binary templates achieve BER of above 40%, which greatly exceeds the error correcting capability of most ECC (around 25%) [2]. To apply the system successfully, we have to extract a biometric binary representation of lower BER, or design ECC of higher error correcting capability [2, 3]. In addition, in order to be an accurate and secure system, lower verification error rate should be achieved and longer secure key needs to be allowed to combine.

In this paper, we aim to propose a novel binary palmprint representation method, which allows for the combination of palmprint verification and template protection system. Firstly, the real-valued features are extracted from palmprint images based on the texture statistical features. Then one-bit quantization and user-specific reliable

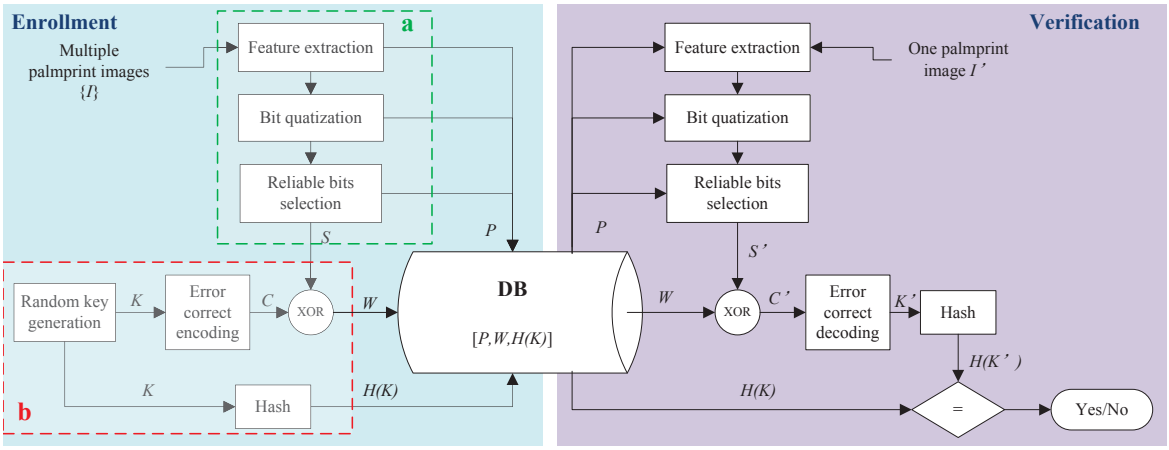


Fig. 1. The considered palmprint verification system under the Helper data scheme. (a) The proposed binary feature extraction method; (b) Error correct coding and hashing. During the enrollment phase, multiple samples are acquired from one user. P denotes the relevant parameters for feature extraction module. For each user, a secret key K is randomly generated and encoded into the codeword C. The second part of helper data is given by $W = C \oplus S$. The secret key K is hashed into $H(K)$ by a one-way hash function, which is the third part of the helper data. All of these three parts will be stored in the database during the enrollment phase. During the verification phase, one noisy image I' of a query palmprint with its claimed identity is firstly captured and processed by the binary string extraction module to get its binary representation S'. Then $C' = S' \oplus W$ is computed. By correcting the errors and decoding K' is obtained. Finally, by compare $H(K')$ with $H(K)$), a positive or negative decision for the query palm will be given.

bits selection procedures are carried out to get a fixed-length binary string as the final palmprint representation. We evaluate the performance of our method by assuming that it works under the Help Data Scheme as Figure 1 shows [4]. Therefore, the verification error rate, BER and the allowed maximal secret key length that our method can provide will be our main concerns.

The main contribution of this paper include: (1) we propose a novel method of palmprint feature extraction and quantization that gives a solution of combining the palmprint verification with the template protection system. It does not require a training phase; (2) The extracted binary string achieves low BER that is within the range of error correcting capability of ECC; (3) Under the Helper Data Scheme, our proposed reliable bits selection step makes it possible to achieve a good balance among the verification error rate, BER and the allowed maximal secret key length.

The paper is organized as follows. Section 2 presents the real-valued palmprint feature extraction method. In Section 3 we describe the one-bit quantization and user-specific reliable bits selection algorithms in detail. The experimental results are given in Section 4. Section 5 concludes the paper.

2 Palmprint feature extraction

So far, there have been many palmprint feature extraction methods reported with high verification accuracy in the classical verification system. The most promising methods are coding based, such as PalmCode, Ordinal Code, BOCV and so on [5]. These methods represent a palmprint image as several binary matrices, and the similarity measurement is based on the pixel-to-pixel matching by Hamming distance. A registration stage during matching is required for coding based methods, which is not

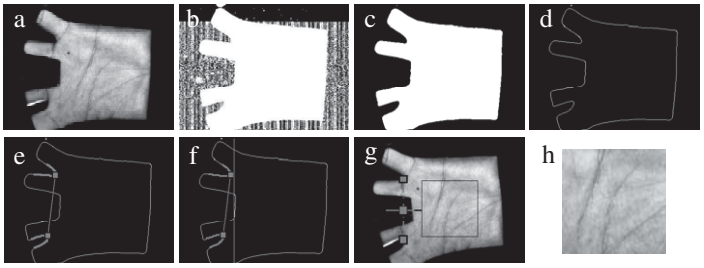


Fig. 2. (a) A typical palmprint image from HongKong PolyU Palmprint Database; (b)-(f) show our used registration and region-crop method.

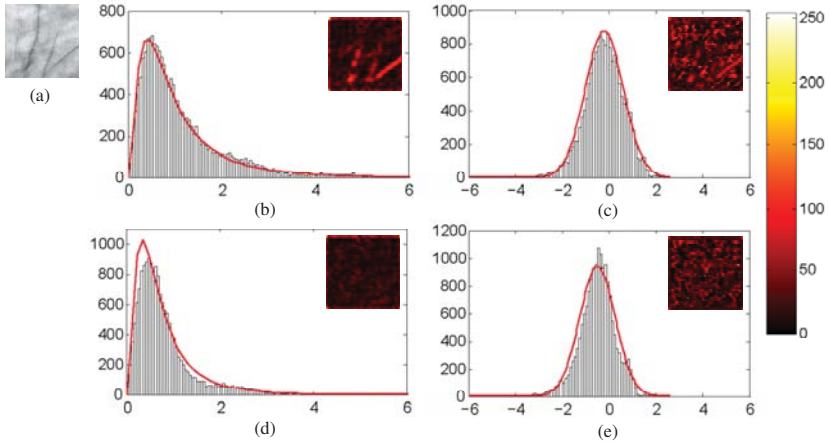


Fig. 3. Examples of histogram fitting. (a) The original palmprint image. (b) and (d) hist Gabor magnitudes from two different Gabor parameters. (c) shows the logarithmic transform of (b). (e) is the logarithmic transform of (d).

allowed in the template protection system.

Therefore, we propose a new method of real-valued palmprint representation based on the texture statistical analysis of Gabor filtered responses [6]. Figure 2 shows a typical palmprint image in HongKong PolyU Palmprint Database and our used registration method.

The Gabor filter family performs a joint spatial-frequency multi-channel representation, which provides optimal localization of image details. The generally used Gabor function can be expressed as follow:

$$g_{q,r}(x,y) = \frac{1}{2\pi\sigma^2}\exp\left\{\frac{-(x^2+y^2)}{2\sigma^2}\right\} \times \exp\{2\pi i(u_q x\cos\theta_r + u_q y\sin\theta_r)\} \qquad (1)$$

u_q is the frequency of sinusoidal wave along directional θ_r 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 $g_{q,r}(x,y)$ with the parameters (u_q,θ_r,σ) is commonly transformed into a discrete Gabor filter and its direct current is turned to zero, which can be denoted by $\tilde{g}_{q,r}(x,y)$. Given an image $I(x,y)$ size of $W\times H$, its Gabor-filtered images are defined as follow: $J_{q,r}(x,y) = \sum_{x_1}\sum_{y_1} I(x_1,y_1)\tilde{g}_{q,r}(x-x_1,y-y_1)$. $J_{q,r}(x,y)$ is a complex number. The Gabor magnitude response (GM) can be denoted by $GM_{q,r}(x,y) = \| J_{q,r}(x,y) \|$, where $\| \bullet \|$ denotes the modulus operator of a complex number. GM will be used to construct the real-valued features of palmprint.

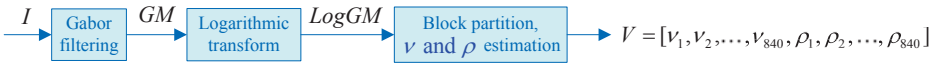


Fig. 4. The proposed method of real-valued feature extraction.

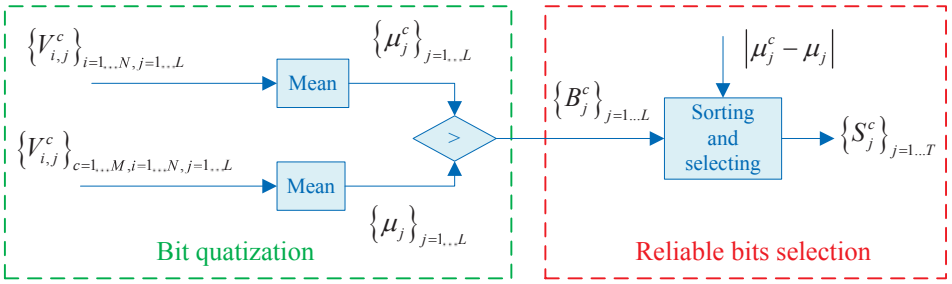


Fig. 5. The flow chart of palmprint binary string extraction, which include bit quantization, and reliable bits selection.

By investigating the histogram distribution of each GM, we found that the log-normal densities fit the GMs very well, and the sub-blocks of each GM are also close to lognormal distribution. Figure 3 gives an example of GM histogram fitting. After lognormal transformation of each GM, we obtain some Gaussian distributions, which can be expressed as $LogGM_{q,r}(x,y) = \log(GM_{q,r}(x,y))$. Since a Gaussian sequence can be represented specifically by its mean and standard deviation, we construct the palmprint feature representation by these Gaussian parameters, which can be formulated as follows:

$$\nu_{q,r} = \frac{1}{W \times H} \sum_x \sum_y LogGM_{q,r}(x,y)\,, \tag{2}$$

$$\rho_{q,r} = \sqrt{\frac{1}{W \times H} \sum_x \sum_y (LogGM_{q,r}(x,y) - \nu_{q,r})^2} \tag{3}$$

Assuming the Gabor filter bank has Q scales and R orientations, and each GM is partition into A sub-blocks. Then the final real-valued palmprint representation can be formulated as

$$V = [\nu_{q,r,a}, \rho_{q,r,a}] \quad q = 1,2,\ldots,Q; r = 1,2,\ldots,R; a = 1,2,\ldots,A. \tag{4}$$

Following the experimental results in Ref. [6], the best verification performance is achieved when $Q = 5, R = 8, A = 21$. Then the length of final real-valued feature vector is 1680. Figure 4 illustrates our method.

3 Quantization and Bits selection

Feature quantization and reliable bits selection strongly affects the performance of the template protection scheme. In this section, we introduce the quantization and bits selection method on the real-valued features presented in section 2, the flow chart of which is shown in Figure 5.

Our method requires that multiple samples for each subject are captured during the enrollment phase. Assuming that we get a real-valued feature vector length of L for each enrollment sample, and there are M different palms and N samples are captured

for each palm in the enrollment set, then we get a feature set $\{V_{i,j}^c\}_{c=1...M,i=1...N,j=1...L}$ after the feature extraction module described in section 2.

For quantization, the mean feature vector $\{\mu_j^c\}_{j=1...L}$ of palm c and the mean $\{\mu_j\}_{j=1...L}$ of all enrollment palms are firstly computed as follows:

$$\mu_j^c = \frac{1}{N}\sum_{i=1}^{N} V_{i,j}^c, \quad \mu_j = \frac{1}{M}\sum_{c=1}^{M} \mu_j^c, \quad j = 1 \dots L \tag{5}$$

The quantization rule can be expressed as:

$$B_j^c = Q\{V_{i,j}^c | i = 1 \dots N\} = \begin{cases} 1, & \texttt{if} \quad \mu_j^c \geq \mu_j; \\ 0, & \texttt{if} \quad \mu_j^c < \mu_j. \end{cases} \tag{6}$$

Where μ_j^c is an estimation of the real-valued template of user c, and the μ_j is the threshold of one-bit quantization.

For the robustness of the system, we require to select some reliable bits from the achieved binary string as the final palmprint representation. The stability of B_j^c depends heavily on the relative distance between μ_j^c and μ_j. Therefore, we can assume that the larger $|\mu_j^c - \mu_j|$, the more reliable of its corresponding bit B_j^c. In the palmprint enrollment phase, we sort the binary string $\{B_j^c\}_{j=1...L}$ for each class by descending order, and select the first n bits as the final binary representation $\{S_j^c\}_{j=1...n}$ for each palm. The number of bits regarded as reliable needs to be determined empirically.

4 Experimental results

The HongKong Polytechnic University (PolyU) palmprint database is used to test our proposed method [7]. They were captured by a CCD camera from 386 different palms and collected in two sessions with different illumination conditions. The resolution of original captured images is 384×284 pixels at 75 dpi.

For the considered template protection system, the verification procedure contains two steps: enrollment and verification. In the enrollment step, the reference strings S is constructed and a secret key K is combined. In the verification step, the query string S' is constructed. By error correct decoding, the secret key K' is released. By comparing the hashed K and K', the verification result is given. Assuming the length of S is n, and the employed ECC can correct at most t bits, by varying t different verification False Rejection Rates (FRR) and False Acceptance Rates (FAR) will be given. It has the same effect as assigning a threshold $\frac{t}{n}$ to the Hamming Distance Classifier (HDC) in the unprotected verification system. The point where FAR equals to FRR is normally called Equal Error Rate (EER), which determines a corresponding Bit Error Rate (BER) the binary strings achieves. EER indicates the verification accuracy and BER shows the robustness of the considered system to some extent, both of which should be as low as possible. In the following experiments, all the random splits of data set for the enrollment and verification respectively are repeated for six rounds, and the averaged results are listed or plotted in the tables or figures shown below.

In the first experiment, the effect of different binary string length (n) on the EER and BER performance is evaluated. The images from session one are used. N samples are randomly selected from each palm for enrollment. The remaining samples are for test of verification performance. Table 1 lists the performance of the proposed method when no reliable bit selection procedure is carried out and the enrollment sample number N for each palm is varying from 3 to 8. As can be seen, both of the

Table 1
Verification performance when all the bits after the bit quantization, without carrying out the reliable bits selection procedure, are directly used as the palmprint binary representation. N for each palm varies from 3 to 8.

N	3	4	5	6	7	8
EER (%)	0.36	0.30	0.22	0.23	0.20	0.22
BER (%)	31.9	31.2	30.8	30.8	30.5	30.6

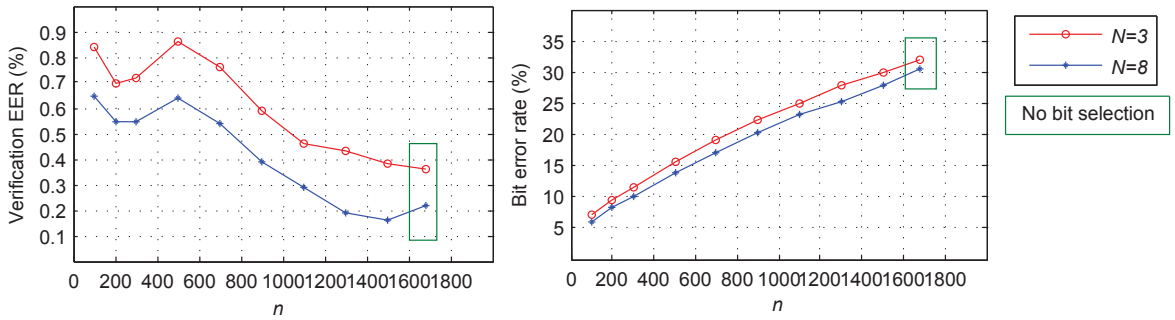


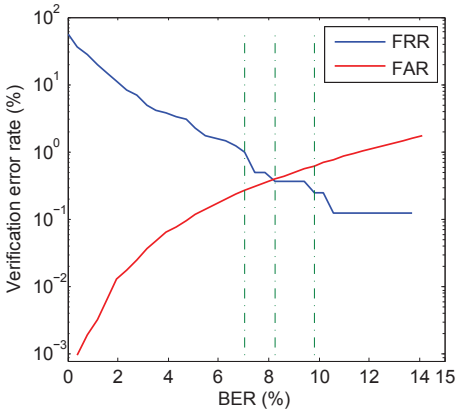
Fig. 6. Verification performance (EER and BER) when the length of selected reliable bits vary.

EER and BER are almost decreased as N increases. When the achieved binary string after bit quantization is directly used as the feature template, the EER is about 0.3%, and BER is around 31%. When the reliable bit selection is processed, the EER and BER performance is examined by varying n from 100 to 1500. Figure 6 plots the EER and BER performance as n varies. As can be seen from it, the verification performance is heavily depended on the selected reliable bits number. As n increases, the BER increases uniformly while EER decreases when n is larger than 500. The performance is showed in Figure 6 as well when no bit selection is processed. It can be seen that the lower BER is achieved at the expense of higher EER by processing the reliable bit selection step. There is a tradeoff between BER and EER for our system.

The ECC generally used is the BCH code, which is commonly described by (n, k, t) [8]. where n (an integer of the form $2^m - 1$ for some integer $m > 2$) denotes the binary template length, k (a positive integer less than n) denotes the maximal length

Table 2
Comparisons of the averaged verification performance (EER and BER). Assuming BCH(n, k, t) is used for error correcting, k can be determined by the values of n and BER. N denotes the number of enrollment samples for each palm.

	$N = 3$				$N = 8$			
n	127	255	511	1023	127	255	511	1023
EER (%)	0.74	0.77	0.86	0.55	0.59	0.51	0.61	0.25
BER (%)	7.8	11.0	15.8	24.4	6.7	9.2	13.7	21.4
Key length k	64	71	76	11	71	91	76	46



BCH (n, k, t)	BER (%)	FAR (%)	FRR (%)
$(255, 123, 19)$	7.06	0.27	1.00
$(255, 107, 22)$	8.24	0.39	0.37
$(255, 91, 25)$	9.80	0.63	0.25

Fig. 7. Verification performance when $n = 255$. The table shows three kinds of BCH coding examples with their corresponding BER, FAR and FRR, which are marked by the green dash lines on the left figure.

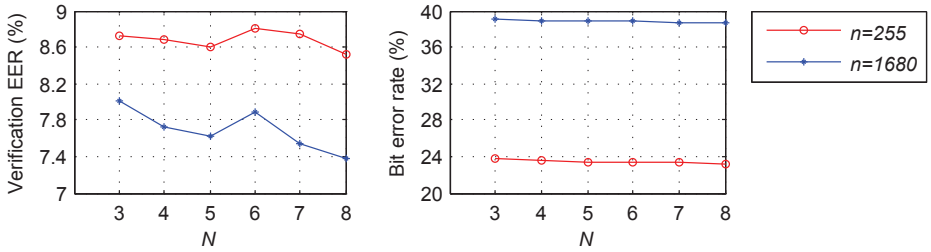


Fig. 8. Verification performance when the sessions for enrollment and test differ in illumination condition. N denotes the number of enrollment samples for each palm. n is the length of the binary feature string for each sample.

of the allowed secret key, and t denotes the maximal length of error bits that can be corrected. In the second experiment, we investigate how the verification EER, BER, and k depend on the chosen BCH code. The considered n values are set to 127, 255, 511 and 1023 respectively. Table 2 lists the resulting EER, BER, and k values when the number of enrollment samples per palm (N) is set to 3 and 8 respectively. As we know there is a tradeoff between EER and BER. When the binary feature string is of length 511, the system achieves the worst verification EER. When $n = 1023$, EER is the best while the BER is the worst and the length of secret key (k) is not enough long to be secure. Therefore, for the proposed method, the system performs best when 255 bits are selected to construct the feature template. When $N = 8$, the EER is about 0.51%, and the corresponding maximal length of secret key that can be combined is up to 91. Figure 7 plots the curves of the verification FAR and FRR versus the BER when $n = 255$, on which three groups of FAR, FRR, and BER performances are marked resulted from employing there kinds of BCH codes.

In the last experiment, the images from two sessions are used. N samples of each palm are randomly selected from session one for enrollment. All the samples in session two (in total 3863 images) are for test. It must be denoted that the samples captured from different sessions differ significantly in illumination conditions. Figure 8 plots the verification EER and BER performance as N varies from 3 to 8. As it shows, when no bit selection is processed ($n = L = 1680$), the EER is about 7.8%, and the BER is close to 40%. When 255 reliable bits are selected to construct the feature template, the EER is around 8.7%, while the BER is decreased to less than 24%.

5 Conclusion

In this paper, we introduce a new palmprint feature extraction and quantization method for template protection system. The extracted binary strings from same subject achieves lower BER that within the error correction capability of ECC (less than 25%). The real-valued features are firstly extracted from each sample. For quantization, multiple samples from the same subject are required to enroll. More samples per palm are enrolled, better performance will be achieved. The number of reliable bits selected influences the system performance, which is determined empirically in this paper considering a good balance among verification EER, BER and the allowed maximal secret key length. Furthermore, our method does not involve a training procedure, which is realistic for template protection system. However, when some distinctive illumination changes exist among the samples captured in different sessions, the proposed method does not obtain desirable performance. Therefore, binary palmprint representation, which is robust to illumination variance, is the point of our further research.

Acknowledgement

This work is supported partly by the National Grand Fundamental Research 973 Program of China under Grant No. 2004CB318005, and the Fundamental Research Funds for the Central Universities (Grant No. KKJB11034536).

References

[1] A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP Journal on Adwances in Signal Processing, no. 113, 2008.

[2] X. Shao, H. Xu, R.N.J. Veldhuis and C.H. Slump, "A Concatenated Coding Scheme for Biometric Template Protection," in: 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), March 2012, Japan.

[3] C. Chen, R.N.J. Veldhuis, "Extracting biometric binary strings with minimal area under the FRR curve for the hamming distance classifier," Signal processing, vol. 91, no. 4, pp. 906–918, 2011.

[4] P. Tuyls, A. Akkermans, T. Kevenaar, G. Schrijen, A. Bazen, and R. Veldhuis, "Practical biometric authentication with template protection," in Proc. Audio- and Video-Based Biometric Person Authenticaton (AVBPA 2005), (NY, USA), pp. 436–446, 2005.

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

[6] M. Mu, Q. Ruan, "Mean and Standard Deviation as Features for Palmprint Recognition Based on Gabor Filters," Int. J. Patt. Recog. Art. Intel., vol. 25, no. 4, pp. 491–512, 2011.

[7] http://www.comp.polyu.edu.hk/ biometrics/

[8] R.E. Richard, "Theory and practice of error control codes," Addison-Wesley Publishing Company, Inc., 1983.