

# Binary Gabor Statistical Features for Palmprint Template Protection

Meiru Mu\*, Qiuqi Ruan, Xiaoying Shao,  
Luuk Spreeuwers, and Raymond Veldhuis

Institute of Information Science, Beijing Jiaotong University, Beijing, China  
Systems and Signals Group, University of Twente, Enschede, The Netherlands  
{m.mu,x.shao,L.J.Spreeuwers,R.N.J.Veldhuis}@utwente.nl

**Abstract.** The biometric template protection system requires a high-quality biometric channel and a well-designed error correction code (ECC). Due to the intra-class variations of biometric data, an efficient fixed-length binary feature extractor is required to provide a high-quality biometric channel so that the system is robust and accurate, and to allow a secret key to be combined for security. In this paper we present a binary palmprint feature extraction method to achieve a robust biometric channel for template protection system. The real-valued texture statistical features are firstly extracted based on Gabor magnitude and phase responses. Then a bits quantization and selection algorithm is introduced. Experimental results on the HongKong PloyU Palmprint database verify the efficiency of our method which achieves low verification error rate by a robust palmprint binary representation of low bit error rate.

**Keywords:** Palmprint verification, Binary feature extraction, Feature template protection, Gabor filtering.

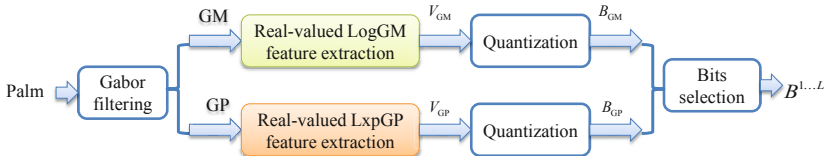
## 1 Introduction

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. For typical (unprotected) palmprint verification systems, there have been many feature representation approaches reported achieving high verification accuracy. Among them there are some coding based methods which generate binary features [2,3]. However, most of them require a template registration during the matching stage, which might be not allowed for template protection system. Further, most of the current reported binary representations give the bit error rates as high as 40% from the genuine matching, which are too noisy to be corrected by the current error correcting coding schemes [4,5].

---

\* Corresponding author.

In this paper, we present a method of binary feature extraction from palmprint image, aiming to achieve robust biometric channel, *i.e.* low bit error rate (BER) for matching channel, and low verification error rate, which we indicate by false rejection rate (FRR), false acceptance rate (FAR) and equal error rate (EER). The robust binary representation gives a solution of combing the typical biometric verification and the template protection. Besides, a fixed-length binary representation also has additional advantages such as small template storage and high matching speed. Since the over-complete information of Gabor filtering responses contributes to the discriminating ability, our method chooses to filter the palmprint image by a group of two-dimensional Gabor functions firstly [2]. Figure 1 shows the flow chart of our proposed binary feature extraction method. As can be seen from it, instead of employing the filtered Gabor magnitude (GM) and Gabor phase (GP) responses directly which are generally high-dimensional, we extract the statistic features from them respectively for real-valued representation (denoted by  $V_{GM}$  and  $V_{GP}$ ), then based on which the one-bit quantization and reliable bits selection are subsequently processed. Finally a binary sequence (denoted by  $B^{1\dots L}$ ) length of  $L$  is achieved as palmprint template for storage and matching. From GM information the global statistical features are extracted which we denote by LogGM [6], while from GP information the local statistical features are extracted after the local XOR pattern (LXP) operating which we denote by LxpGP [7]. After quantizing the global and local statistical features respectively, we fuse the obtained binary bits together and then from them some reliable bits are selected to construct the final binary Gabor statistical features. For verification the Hamming distance is employed as the dissimilarity measurement.



**Fig. 1.** Flow chart of the proposed method

The main contributions of this paper are: a highly efficient scheme is proposed to extract the binary features from the Gabor filtering responses by considering the fusion of the local and global texture statistical information, which provides a high-quality biometric channel achieving low bit error rate for the genuine template matching and the corresponding low verification error rate so as to give a solution of combining the typical palmprint verification system and template protection scheme.

In this paper, we will firstly present the scheme of real-valued Gabor texture statistical representation in Section 2, which includes the statistical analysis of Gabor magnitude and phase responses respectively. Next, the quantization and

reliable bits selection algorithm will be introduced in Section 3. The experimental results will be given in Section 4. Finally, it is the conclusion.

## 2 Gabor Statistical Feature Extraction

In order to represent a palmprint by a binary string for template protection, we need to firstly extract some real-valued features from it. Since the Gabor filtered representation can provide the optimal localization of image details, we choose a group of Gabor functions to perform a joint spatial-frequency multi-channel transform on the palmprint image, which can be expressed as following [2]:

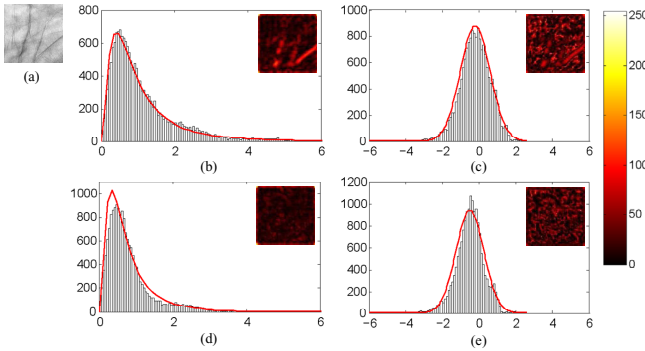
$$g_{m,n}(x,y) = \frac{1}{2\pi\sigma^2} \exp\left\{\frac{-(x^2+y^2)}{2\sigma^2}\right\} \times \exp\{2\pi i(u_m x \cos \theta_n + u_m y \sin \theta_n)\}. \quad (1)$$

$u_m$  is the frequency of sinusoidal wave along directional  $\theta_n$  from  $x$ -axis, and  $\sigma$  specifies the Gaussian envelope along  $x$  and  $y$  axes, which determines the bandwidth of the Gabor filter. Each Gabor function  $g_{m,n}(x,y)$  with the parameters  $(u_m, \theta_n, \sigma)$  is commonly transformed into a discrete Gabor filter and its direct current is turned to zero, which can be denoted by  $\tilde{g}_{m,n}(x,y)$ . Given an image  $I(x,y)$ , its Gabor-filtered images can be defined as follow:  $J_{m,n}(x,y) = \tilde{g}_{m,n}(x,y) * I(x,y)$ , where  $J_{m,n}(x,y)$  is a complex number. The Gabor magnitude and phase angle responses can be respectively denoted by  $GM_{m,n}(x,y) = \|J_{m,n}(x,y)\|$ , and  $\phi_{m,n}(x,y) = \arctan(J_{m,n}(x,y))$ , where  $\|\bullet\|$  denotes the modulus operator of a complex number. To alleviate the sensitivity of Gabor phase to the varying positions, we transform  $\phi_{m,n}(x,y)$  into four different ranges as the Gabor phase (GP) information  $GP_{m,n}(x,y)$  by the following expression:

$$GP_{m,n}(x,y) = p, \text{ if } 90 * (p - 1) \leq \phi_{m,n}(x,y) < 90 * p; \quad p \in \{1, 2, 3, 4\} \quad (2)$$

$GM_{m,n}(x,y)$  and  $GP_{m,n}(x,y)$  will be respectively further processed to construct the real-valued statistical features.

By investigating the histogram distribution of each GM, it has been found that the lognormal densities fit the GMs very well, and the sub-blocks of each GM are also close to lognormal distribution [6]. Figure 2 gives an example of GM histogram fitting. After the lognormal transformation of each GM, some Gaussian distributions are obtained, which can be expressed as  $LogGM_{m,n}(x,y) = \log(GM_{m,n}(x,y))$ . Since a Gaussian sequence can be represented specifically by its mean  $\nu$  and standard deviation  $\rho$ , the palmprint feature representation can be constructed by these Gaussian parameters. Assuming the Gabor filter bank has  $E$  scales and  $F$  orientations, and each GM is partitioned into  $A$  sub-blocks, we will get  $(G \times R \times A)$  pairs of  $\nu$  and  $\rho$  values. By concatenating them together, the final real-valued feature vector can be formulated as  $[\nu_1 \dots \nu_{(E \times F \times A)}, \rho_1 \dots \rho_{(E \times F \times A)}]$ . Following the experimental results in Ref. 6, the best verification performance is achieved when  $E = 5, F = 8, A = 21$ . To obtain more discriminating feature components from which we expect to extract



**Fig. 2.** 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).



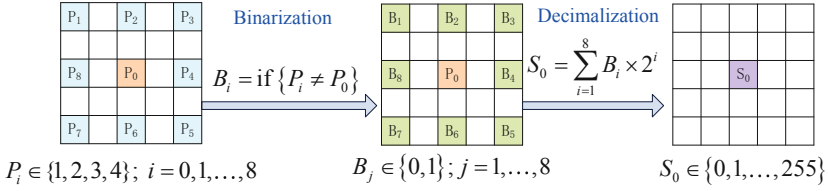
**Fig. 3.** Flow chart of real-valued LogGM feature extraction

bits, the linear discriminant analysis (LDA) projection is applied to get the final real-valued representation  $V_{GM}$  of GM, the process of which we denote by real-valued LogGM feature extraction as Fig. 3 illustrates.

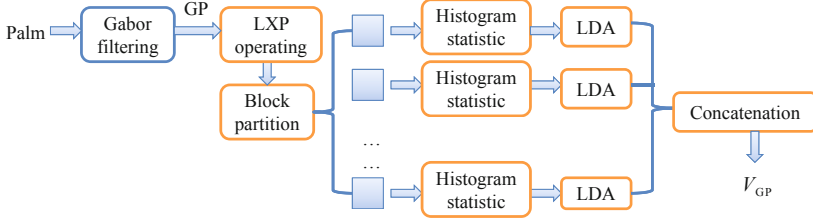
To extract some statistical features from GP, we firstly encode  $GP_{m,n}(x, y)$  by local XOR pattern (LXP) operator [7], which is expressed as  $LxpGP_{m,n}(x, y) = LXP(GP_{m,n}(x, y))$ . As shown in Fig. 4, for each pixel  $P_0$ , its eight neighborhoods with one pixel interval  $P_i \in \{1, 2, 3, 4\}$ ,  $i = 0, 1, \dots, 8$  need to be encoded into  $B_i \in \{0, 1\}$ ,  $i = 0, 1, \dots, 8$  by computing  $B_i = \text{if}\{P_i \neq P_0\}$ . Then  $P_0$  is mapped into a decimal number  $S_0 \in \{0, 1, \dots, 255\}$  by calculating  $S_0 = \sum_{i=1}^8 B_i \times 2^i$ . Finally all the mapped  $S_0$  forms  $LxpGP_{m,n}(x, y)$ . Assuming the Gabor filter bank has  $E$  scales and  $F$  orientations, and each GM is partitioned into  $D$  sub-blocks, the histograms of each sub-block at all the scales and orientations are concatenated. Then  $D$  histograms of  $E \times F \times 256$  bins will be obtained. LDA is applied for each histogram respectively. In this paper, we set  $E = 5$ ,  $F = 8$ ,  $D = 5$  by taking into account the computational complexity and the performance. Finally the features from the  $D$  LDA modulus are concatenated into a vector  $V_{GP}$  as the real-valued representation of GP information, the flow chart of which is shown in Fig. 5.

### 3 Bits Quantization and Selection

Feature quantization and bits selection procedures strongly affect the verification performance of the template protection system. Based on the real-valued features described in Section 2, we introduce our proposed bit quantization and selection



**Fig. 4.** An illustration of local XOR pattern (LXP) operating



**Fig. 5.** Flow chart of real-valued LxpGP feature extraction

method in this section, which is illustrated in Fig. 6. Since  $V_{GM}$  and  $V_{GP}$  are processed in the same way, here we take  $V_{GM}$  as an illustration of the main steps as follows:

(1) Compute the averaged real-valued feature from the enrolled  $N$  samples of one palm;

Assuming  $V_t$  palms are captured for training and  $N$  samples from one palm are enrolled, we will get a feature set  $\{V_{GM,Enroll}^i, i = 1 \dots N\}$  to represent each palm after the LDA projection. The averaged feature vector for each palm needs to be computed as expressed following:

$$\bar{V}_{GM,Enroll} = \frac{1}{N} \sum_{i=1}^N V_{GM,Enroll}^{i,j}, j = 1 \dots (V_t - 1) \quad (3)$$

(2) Quantize the real-valued features by a threshold;

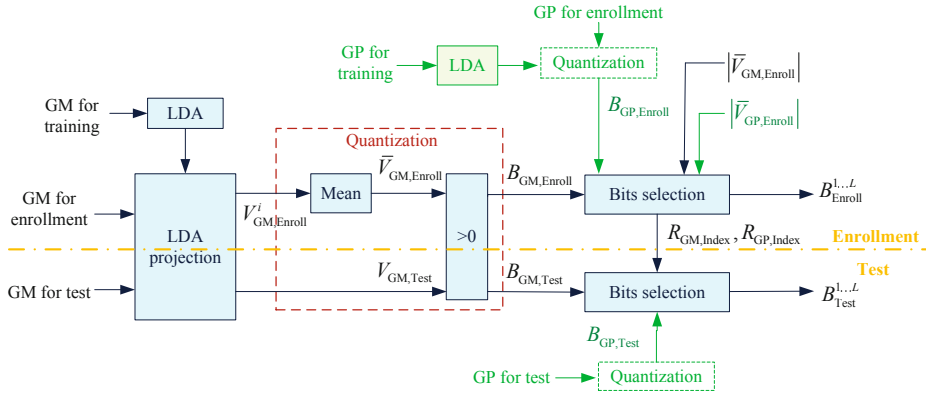
Here the threshold is set to 0. Each component of the real-valued features  $\bar{V}_{GM,Enroll}$  is quantized into one bit  $B_{GM,Enroll}^j, j = 1 \dots V_t - 1$  which can be expressed as following:

$$(B_{GM,Enroll}^j | j = 1 \dots V_t - 1) = \begin{cases} 1, & \bar{V}_{GM,Enroll}^j \geq 0; \\ 0, & \text{otherwise.} \end{cases} \quad (4)$$

By the same process,  $V_{GM,Test}$  from each test sample is quantized into a binary string  $B_{GM,Test}$ .

(3) Select some reliable bits as the final binary feature template.

During the enrollment phase, we assume that the larger  $|\bar{V}_{GM,Enroll}^j|$ , the more reliable of its corresponding bit  $B_{GM,Enroll}^j$ . In the meanwhile, the positions of

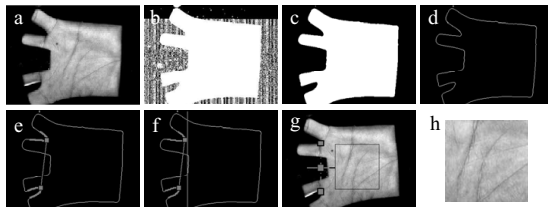


**Fig. 6.** One-bit quantization and reliable bits selection

the most reliable bits need to be recorded as a index vector  $R_{GM,Enroll}$ . For a test sample, the bits are selected by following the position index of  $R_{GM,Enroll}$ . Assuming  $L$  bits are selected then our proposed binary Gabor statistical features are  $B_{Enroll}^{1...L}$  for enrollment palmprint and  $B_{Test}^{1...L}$  for test palmprint respectively.

### 4 Experimental Results

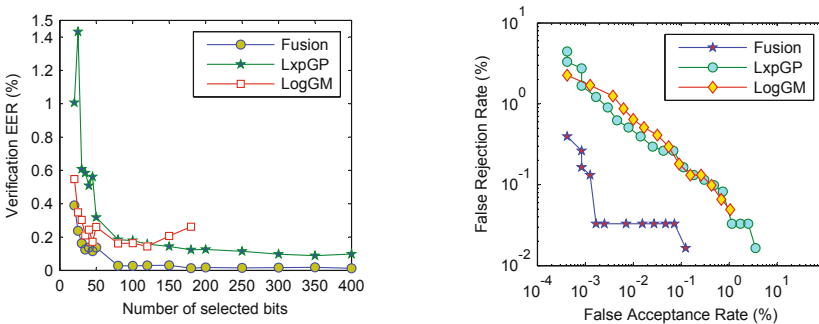
The HongKong Polytechnic University (PolyU) palmprint database is used to test our proposed method [8]. They were captured by a CCD camera from 386 different palms and collected in two sessions with two different illumination conditions. There are 3889 images in session one and 3863 palms in session two respectively. Because there is one palm which has only one sample captured in session 2, we use the other 385 palms for our experiments. The resolution of original captured images is  $384 \times 284$  pixels at 75 dpi. By preprocessing each captured image (as shown in Fig. 7), the central region size of  $128 \times 128$  is used for feature extraction.



**Fig. 7.** (a) A typical palmprint image from HongKong PolyU Palmprint Database; (b)-(f) show our used registration and region-crop method

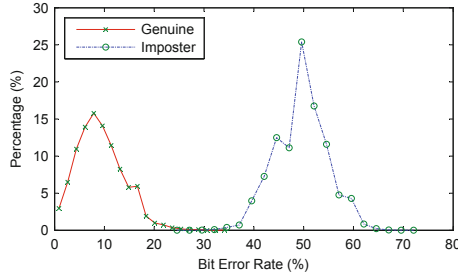
**Experiment I:** Since the verification performance is heavily depended on the number of the selected bits, we test our algorithm by varying the bits number from 20 to 400. For this experiment, the images in session one are used, which are randomly split as the training set (185 palms) and the evaluation set (the remaining 200 palms for enrollment and test), which can be referred as training-evaluation-set split. For training, all the samples are used. For enrollment, five samples are randomly selected and the remaining ones for test. The training-evaluation-set split is performed six times. For matching genuine pairs, we test all the samples in the test set. For matching imposter pairs, the first sample of each palm in the test set is chosen for all the possible imposter combinations. Thus, we have totally 6082 genuine scores and 238,800 imposter scores.

Figure 8 (Left) plots the comparison of the verification equal error rate (EER) among the methods of LogGM (only GM information is used), LxpGP (only GP information is used), Fusion (the proposed method by fusing GM and GP information). As can be seen from it, the EER decreases as the bits number increases. However, since more bits lead to be more noisy string, we determine 120 as the optimal bits number for the proposed fusion method. Figure 8 (Right) plots the comparison of ROC curves. As can be seen, the verification performance can be greatly improved by fusing the bits generated from GM and GP information respectively. Figure 9 shows the percentage distributions of bit error rate (BER) for genuine and imposter matching respectively by the proposed method. As we can see that the proposed method is able to achieve good verification performance by adjusting the BER threshold of error correcting coding (ECC) module to around 30% assuming the system works under the template protection framework.



**Fig. 8.** Verification performance. (Left) Verification EER (%) comparison when the number of selected bits varies from 20 to 400; (Right) ROC curves when the number of selected bits is set to 120.

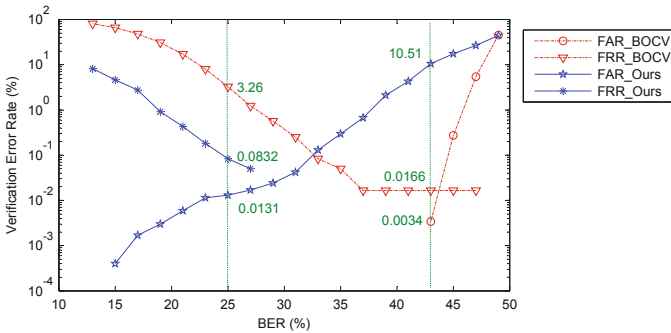
**Experiment II:** Here the proposed method is compared with the binary co-occurrence vector (BOCV) method on the verification error rate and the corresponding BER threshold which is depended on the used ECC module [3,5]. For



**Fig. 9.** Percentage distribution of Bit Error Rate (%) for genuine and imposter matching respectively by the proposed method

this experiment, the samples for training (185 palms) are from session 1 while the ones for evaluation (200 palms) from session 2. Other protocols are the same as those in experimental I. For the BOCV method, no training procedure is needed. Here we set the evaluation protocol the same as that for ours. In total, we have 6013 genuine scores and 236,412 imposter scores. BOCV requires to shift the whole image by several pixel horizontally and vertically and then matches multiple times to get the final matching score. Here each bits plane is down-sampled into a binary matrix size of  $32 \times 32$ . The range of shift is considered as  $[-2, 2]$ .

Figure 10 plots the comparison of verification error rate which is indicated by false acceptance rate (FAR) and false rejection rate (FRR) when adjust the BER threshold of ECC module. As can be seen from it, the proposed method greatly outperforms the coding based method BOCV when the applied ECC module has an error correcting capability of lower than 25%. Besides, for the proposed method there is no need to shift the feature templates multiple times for the final matching score, which is not only time-consuming, but also challenges the combination of palmprint verification and template protection system.



**Fig. 10.** Comparisons of verification error rate (%) and their corresponding BER thresholds between the binary co-occurrence vector (BOCV) method and the proposed method (Ours)



## 5 Conclusion and Discussion

In this paper, we present a binary feature extraction method for palmprint verification under consideration of feature template protection which requires a robust biometric channel. Experimental results demonstrate that fusion of the global and local statistical features extracted from Gabor magnitude and phase responses respectively outperforms that of global or local features represented separately on the verification accuracy. Compared with the popular coding based methods, the proposed approach achieves comparable verification error rate while much lower bit error rate of the genuine matching which gives a solution of combining palmprint verification and feature template protection scheme so that the system could be robust and accurate.

However, the extracted discriminative binary string is still not long enough to be secure. To alleviate the intra-class variations, how to extract the robust binary palmprint features of more bits so that a long key can be combined for security will be the point of our future work.

**Acknowledgments.** This work is supported partly by the National Grand Fundamental Research 973 Program of China (Grant No. 2004CB318005), the Fundamental Research Funds for the Central Universities (Grant No. KKJB110 34536), and China Scholarship Council.

## References

1. Jain, A., Nandakumar, K., Nagar, A.: Biometric Template Security. *EURASIP Journal on Advances in Signal Processing* 113 (2008)
2. Kong, W., Zhang, D., Li, W.: Palmprint Feature Extraction Using 2-D Gabor Filters. *Pattern Recognition* 36, 2339–2347 (2003)
3. Guo, Z., Zhang, D., Zhang, L., Zuo, W.: Palmprint Verification Using Binary Orientation Co-Occurrence Vector. *Pattern Recognition Letters* 30, 1219–1227 (2009)
4. Richard, R.E.: *Theory and Practice of Error Control Codes*. Addison-Wesley Publishing Company, Inc. (1983)
5. Shao, X., Xu, H., Veldhuis, R.N.J., Slump, C.H.: A Concatenated Coding Scheme for Biometric Template Protection. In: 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE Press, Japan (2012)
6. Mu, M., Ruan, Q.: Mean and standard deviation as features for palmprint recognition based on gabor filters. *Int. J. Patt. Recog. Art. Intel.* 25(4), 491–512 (2011)
7. Xie, S., Shan, S., Chen, X., Chen, J.: Fusing Local Patterns of Gabor Magnitude and Phase for Face Recognition. *IEEE Transactions on Image Processing* 19(5), 1349–1361 (2010)
8. Biometrics Research Centre (BRC) in HongKong, <http://www.comp.polyu.edu.hk/~biometrics/>