International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.7, No.3 (2014), pp.223-236
http://dx.doi.org/10.14257/ijsip.2014.7.3.18

Finger Multi-biometric Cryptosystem using Feature-Level Fusion

Li Lu[1] and Jialiang Peng[2,*]
[1]*School of Electrical Engineering, Shanghai Dianji University, Shanghai 200240, China*
[2]*Information and Network Administration Center, Heilongjiang University, Harbin 150080, China*
lulihappy@163.com, jialiangpeng@hlju.edu.cn

Abstract

In this paper, we propose a new finger multi-biometric cryptosystem using feature-level fusion to simultaneously protect multiple templates of fingerprint, finger vein, finger knuckle print and finger shape traits as a single secure sketch. We theoretically analyze the feature-level fusion for finger multi-biometric cryptosystem with respect to their impact on security and recognition accuracy. The comparative experimental results ascertain that finger multi-biometric cryptosystem outperforms the uni-biometric counterparts in terms of verification performance and template security.

Keywords: *Finger, Multi-biometrics Cryptosystem, Template protection, Feature Fusion*

1. Introduction

Recently, many applications using finger biometrics are adapted to the increasing demand of personal identification. These systems rely on the personal finger physiological traits, such as fingerprint, finger vein; finger knuckle print and finger shape [1-4]. However, finger uni-biometric systems have several inherent problems such as large intra-class variations, non-universality and suffer from spoofing attacks [5, 6]. Finger multi-biometrics [7-9] is, therefore, attracting the attention of researchers to effectively overcome most of the above weaknesses in finger uni-biometric systems. Finger multi-biometric system usually contains two or more finger sources and combines them together for personal identification. The performances of finger multi-biometric systems are superior to uni-biometric approaches, such as higher accuracy, noise resistance, universality, anti-spoof attacks, and robustness [10]. However, there is no sufficient attention paid to the security of finger multi-biometric systems. Since the biometric trait is permanently related to a specific user, it can not be changed when it is compromised, either through lost, stolen or unauthorized copies. In this sense, the secure use of biometric data is fundamental in biometric systems. Though a biometric system can be compromised in a number of ways, the leakage of biometric template information constitutes a serious security and privacy threatening to individuals [11]. Therefore, the fusion approach and the security for finger multi-biometrics should be considered deliberately.

For multi-biometric recognition, the fusion at feature level can preserve the discriminability of features from different modalities and provide higher recognition accuracy and security than the score-level or decision-level fusion [11]. In this paper, therefore, we aim to analyze the security of feature-level fusion for finger multi-biometric cryptosystem, which combines finger vein, fingerprint, finger knuckle print and finger shape. The main reasons for

* Corresponding author: jialiangpeng@hlju.edu.cn

ISSN: 2005-4254 IJSIP

the fusion of four finger traits can be summarized as follows: First, finger veins are hidden structures and extremely difficult to be stolen with a high degree of privacy. The use of finger vein patterns can offer strong anti-spoofing capabilities, which ensures live-ness in biometric verification process. Second, human fingerprints are easier to present and provide with a variety of traits that are convenient to be recognized. Third, the finger knuckle prints refer to the skin patterns of the upper surface around the phalange joints also have high discriminative ability to be utilized in the personal identification. Fourth, finger shape recognition, its non-intrusive, low cost characteristics and less data storage requirement, make it easy to select most likely candidates in authentication applications for coarse matching appropriately. Finally, the fusion of above biometric traits can further improve the biometric performance, reliability, and population coverage. However, compared to conventional biometric systems based on a single finger trait, multiple sources of finger, *i.e.*, more biometric reference templates have to be stored for each subject enrolled within a finger multi-biometric system. It definitely raises the need for the security of multi-biometric templates. In addition, the template protection scheme should be suitable for the fusion approach that overcomes the large intra-class variability among multiple biometric traits of the same user to obtain high recognition accuracy.

There are some researches on the multi-biometric template protection systems. For instance, Yanikoglu and Kholmatov [12] proposed a biometric authentication framework which fuses two separate fingerprints of the same individual obtain a non-unique identifier to address privacy concerns. Sutcu, *et al.*, [13] presented the minutiae-based fingerprint features and the SVD-based face features, which are both transformed into binary strings and concatenated as feature-level fusion to a Fuzzy Commitment Scheme [14]. Nandakumar, *et al.*, [15] provided the Fuzzy Vault Scheme [16] to secure fingerprint minutiae and iriscode templates of the same user at feature-level fusion. The results demonstrate that the combination of biometric modalities leads to higher accuracy and security. Kanade, *et al.*, [18] implemented a multi-biometric system based cryptographic key generation scheme, which combines data from iris and face to obtain a longer cryptographic key with high entropy. Nagar, *et al.*, [11] contributed a feature-level fusion framework to simultaneously protect fingerprint, face and iris templates based on Fuzzy Commitment Schemes or Fuzzy Vault Schemes. They offer the practical implementation of the feature-level fusion system with multi-biometric template protection, and make the trade-off between multi-biometric accuracy and security. Fu, *et al.*, [18] investigated two fusion approaches corresponding to feature-level and decision-level fusion with respect to privacy and recognition accuracy, but limiting to theoretical analysis without experimental results.

Generally, the aforementioned works show that multi-biometric cryptosystems have higher security and verification performance than uni-biometric cryptosystems. For the sake of multi-biometric template security, it should be guaranteed the non-invertibility (computationally difficult from one given secure template to obtain its original biometric features) and the revocability (computationally hard to identify two secure templates derived from the same biometric data). Meanwhile, the multi-biometric systems always have large intra-class variations, which make the traditional uni-biometric template protections fail to be applied directly. In this paper, we propose multi-biometric cryptosystem to combine multiple finger traits at feature-level fusion. We investigate how finger multimodal fusion can be applied in multi-biometric cryptosystem and to what extent the recognition accuracy and template security can be increased. To the best of our knowledge, there is no multi-biometric cryptosystem based on the multiple finger biometric traits until now.

The remainder of the paper is organized as follows. Section 2 introduces the proposed finger multi-biometric cryptosystem based on feature-level fusion. Section 3 is devoted to the

security analysis of the proposed finger multi-biometric cryptosystem. Section 4 represents the experimental setup and results of performance evaluation. Finally, Section 5 concludes this paper.

2. Proposed Finger Multi-Biometric Cryptosystem based on Feature-Level Fusion

2.1. Biometric Cryptosystem using Fuzzy Commitment Scheme

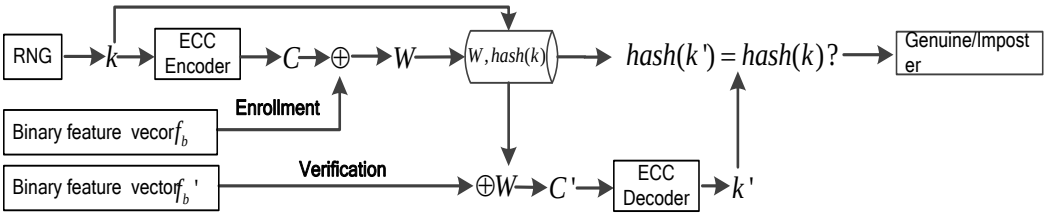


Figure 1. The Fuzzy Commitment Scheme

As a representative biometric cryptosystem, Fuzzy Commitment Scheme (FCS) comprises procedures for enrollment and authentication shown in Figure 1. These procedures of FCS combine the Error Correcting Code (ECC) with a cryptographic Hash function in both the enrollment and verification phase. ECC are used to deal with bit errors, which are referred to as the Hamming distance $d_H(f_b, f_b')$ between the enrolled binary vector f_b and the query binary vector f_b'. In the enrollment phase, the random key k is selected as a binary secret based on the Random-Number-Generator (RNG) module. An ECC codeword C is obtained to encode k in the ECC Encoder module. Here, we use the "Bose, Ray-Chaudhuri, Hocquenghem" (BCH) code as the ECC, which is specified by the codeword length (n), message length (m), and the corresponding number of bits that can be corrected (t), in short $[n, m, t]$. The codeword C is XOR-ed with f_b to obtain the secure sketch W, where the symbol $\oplus$ indicates XOR operation. The sketch W is stored into the database along with the Hash value of k, where $hash(\ )$ is a cryptographic Hash function. In the verification phase, a new codeword C' is obtained from the query binary vector f_b' by XOR-ing W, namely, $C' = W \oplus f_b' = C \oplus f_b \oplus f_b'$. This code word C', generally a corrupted version of the original codeword C due to measurement noise and biometric variability, can be decoded to get the key k' in the ECC Decoder module. If the Hamming distance between f_b and f_b' is not greater than the error correcting capacity of the BCH code t, k would be the same as k' and the matching will be successful. There is an acceptance when the Hamming distance is smaller than t, $d_H(f_b, f_b') = || f_b, f_b' || \le t$. The final decision of genuine or imposter is based on whether $hash(k)$ and $hash(k')$ are bitwise identical. Thus, the Fuzzy Commitment Scheme can be considered as a Hamming distance classifier with threshold t [19].

2.2. Finger Multi-biometric Cryptosystem based on Fuzzy Commitment Scheme

The use of finger multi-biometric cryptosystem, where reference templates are only available in protected form, makes it necessary to reconsider how biometric data from different finger modalities can be fused together. We consider the case that a set of finger biometric feature real representation $f = \{f_v, f_p, f_k, f_s\}$ are used, where f_v , f_p , f_k , f_s represents the feature corresponding to the finger vein, fingerprint, finger knuckle and finger shape modality of a user, respectively. Meanwhile, the fused features via feature-level fusion can be compared with the protected templates within the multi-biometric cryptosystem to make a decision on whether to accept or reject the identity claim of the subject.

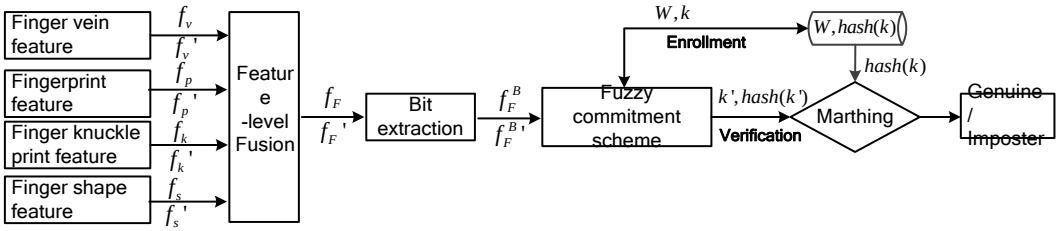


Figure 2. Finger Multi-Biometric Cryptosystem using Feature-Level Fusion

In Figure 2, finger multi-biometric cryptosystem based on feature-level fusion is straightforward, and the real feature vectors f_v , f_p , f_k , f_s are obtained from four finger modalities during enrollment are combined to form a new feature vector f_F , which is given as input to FCS in the enrollment phase. To compute the sketch W and $hash(k)$ of FCS, it needs to transform the fused feature from real into binary representation f_F^B by Bit extraction module. We use a simple bit quantization scheme based on reliability and discriminability of real component within f_F . Moreover, the process of binarization needs to extract the corresponding binary vectors from biometric features with minimum degradation of verification performance. In Algorithm.1, we introduce a more detailed description of this bit extraction. Similarly, during verification phase, f_v', f_p', f_k', f_s' are extracted from the four probe finger modalities and are fused to form a new feature vector f_F' . This feature vector f_F' is also transformed to f_F^B' , which is input to the FCS along with W and computes $hash(k')$ to verify against $hash(k)$.

In multi-biometric cryptosystem using feature-level fusion, the fused feature vectors can preserve the discriminability of features from different modalities and be considered to provide higher recognition results. However, the feature-level fusion is difficult to achieve in practice due to the potential incompatibility of feature spaces formed by different biometric modalities. Compared to conventional feature fusion method simply concatenate features together (namely, serial feature fusion [20]), we provide the feature fusion approach from our previous work called Multi-set Canonical Correlations Analysis (MCCA) [21] to fuse multiple finger traits at feature level reasonably and effectively. The MCCA approach is not only able to obtain the discriminative information from original multiple finger features, but also eliminate the redundant information between the features with high recognition performance.

Algorithm 1. Bit Extraction: transform feature representation from real to binary

Input: *Train_r*, the training real feature set; *Test_r*, the testing real feature set; *M*, the length of the real feature; *N*, the bit number for each real feature component.
Output: *Train_b*, the training binary feature set; *Test_b*, the testing binary feature set.
1: All the training and testing real feature vectors in *Train_r* , *Test_r* are normalized into $[0,1]$ range;
2: Divide the range $[0,1]$ by N to obtain the set $L = [1,1-1/N) \cup \cdots \cup (1/N, 0]$ and index the elements of *L as* $[1, 2 \cdots, N]$;
3: For each component of a real feature vector, find which element of *L* belongs to it and locate the index as *I* to generate *B* that is composed of "1" with the number of $Z = N - I$ in front of "0" with the number of *I*;
4: Concatenate all *B* of all components in the real feature vector as a binary vector;
5: For each real feature vector in normalized *Train_r and Test_r* is converted to the binary feature vector according Step 3-4;
6: For each binary substring in the binary feature vector of length *l*, $l = 1 \cdots M * N$, compute its distance of the verification performance indicator *FMR* and *FNMR*, $diff = FMR * FNMR$, where *FMR* and *FNMR* are the verification performance indicators defined in subsection 4.2;
7: Sort the vector of *diff* in descending, and then compute the verification performance for the binary vector of every length of *l* to find the best verification performance result;
8: The optimal binary substring in Step 7 forms the final binary vector;
9: Repeat Step 6-8 to compose the corresponding binary feature set *Train_b* and *Test_b* as output.

3. Security Analysis of the Proposed Approach

In this section, we mainly focus on how difficult to decode an individual Fuzzy Commitment Scheme as the fundamental security analysis for the proposed finger multi-biometric cryptosystem. In the Fuzzy Commitment Scheme, suppose that the attacker uses N_I impostor samples to decode a genuine sketch W for a genuine biometrics template b_e with length of N bits. For an imposter binary feature vector b_i, it can obtain a corrupted codeword $C_i = b_i \oplus W$. We assume that there are r most reliable bits in the biometric template. Here, except for the r reliable bits in the binary feature, the left bits are considered as measurement noises. We denote the reliable binary component of b_e and b_i as b_e^r and b_i^r, respectively. The Hamming difference between b_e^r and b_i^r is denoted as ρ_i^r . For each bit of all the training binary features, we calculate its standard variance and sort bits by their variances in ascending order. We select the former 95% sorted bits as r most reliable bits in our experiments.

There are three different scenarios [11] when the attacker invokes the error correcting decoder for values of r in the range $[N - D_{\min} + 1, N]$, where $D_{\min} = 2t + 1$ is the minimum distance of ECC $[n, m, t]$.

1. If $(N - r)/2 + \rho_i^r \le t$, where $(N - r)$ is the number of noises and ρ_i^r is the number of errors. In this case, the decoder will return the correct key in a fuzzy commitment scheme.
2. If $(N - r)/2 + \rho_i^r > t$, the attacker can try to find m_i^r $(0 \le m_i^r \le (N - r)/2 + \rho_i^r - t)$ bits to make b_i be decoded correctly. If such an m_i^r exists, the probability of successful attack is $p = \binom{\rho_i^r}{m_i^r} \Big/ \binom{r}{m_i^r}$.

3. If the attacker can't find m_i^r, the secure sketch can't be decoded and the corresponding probability of successful attack is considered to be $p = 0$.

Now, the security of Fuzzy Commitment Scheme is evaluated in the form of Shannon entropy by the following *Eq.* (1):

$$\begin{aligned} S_{FCS} &= \min_{r,i}\left(-\log_2 \sum_{j=0}^{m_i^r} \left(\binom{\rho_i^r}{j} \Big/ \binom{r}{j} \right) \right) - \log_2 \left(1/\left(N_i D_{\min} \right) \right) \\ &\approx \min_{r,i}\left(-\log_2 \left(\binom{\rho_i^r}{m_i^r} \Big/ \binom{r}{m_i^r} \right) \right) + \log_2 \left(N_i D_{\min} \right) \end{aligned} \tag{1}$$

Though the length of the template is N bits, the entropy of the template is typically much less than N bits because these bits may not be uniformly distributed. Suppose that the entropy of b_e^r is r_* bits. In this case, the security of fuzzy commitment sketch can be given by Eq. (2).

$$S_{FCS} \approx \min_{r,i}\left(-\log_2 \left(\binom{\rho_{i*}^r}{m_{i*}^r} \Big/ \binom{r_*}{m_{i*}^r} \right) \right) + \log_2 \left(N_i D_{\min} \right) \tag{2}$$

Where $\rho_{i*}^r = r_* \rho_i^r / r$ and $m_{i*}^r = \left((N - r)/2 + \rho_i^r - t \right) r_* / r$.

For a genuine authentication query b_g, the decoding security can be expressed as *Eq.*(3).

$$S_{FCS}^{gen} \approx \min_{r,i}\left(-\log_2 \left(\binom{\rho_*^r}{m_*^r} \Big/ \binom{r_*}{m_*^r} \right) \right) + \log_2 \left(D_{\min} \right) \tag{3}$$

Where ρ_*^r is the effective Hamming distance of b_g and b_e, and $m_*^r = \left((N - r)/2 + \rho_*^r - t \right) r_* / r$.

Based on the above security analysis of Fuzzy Commitment Scheme, the security of proposed multi-biometric cryptosystem is discussed as following:

Feature-level fusion does not allow an attacker to conduct an exhaustive search on any single modality, as the features are combined before the bit strings f_F^B are computed. The multi-biometric cryptosystem is completely based on a single FCS, which verifies the correctness of the fused features by applying the specific error correcting code. It implies that the same entropy computing process like *Eq.* (1)-(3) for the multi-biometric cryptosystem. We denote the security of finger multi-biometric cryptosystem as S^{Mul}, given by *Eq.* (4).

$$S^{Mul} = \min_{r,i}\left(-\log_2 \left(\binom{\rho_{fused}^r}{m_{fused}^r} \Big/ \binom{r_{fused}}{m_{fused}^r} \right) \right) + \log_2 \left(D_{\min} \right) \tag{4}$$

Where the symbols ρ_*^r, m_{fused}^r, r_{fused} and $D_{\min}$ are the same meaning as defined in *Eq.* (3).

4. Experimental Results and Analysis

4.1 Experiments Setup

The proposed finger multi-biometric cryptosystem is evaluated based on a merged multimodal finger biometric database. This database is a virtual database, which contains finger vein, fingerprint, and finger knuckle images from three finger biometric sub-databases,

as shown in Figure 3. Meanwhile, the features for finger shape recognition are derived from finger vein images. For our performance evaluation with the same scale, each sub-database consists of 100 subjects, 6 samples per-subject. The finger vein image sub-database employed in this paper is Hong Kong Polytechnic University Finger Image Database Version 1.0 [22]. There are randomly selected 100 fingers with six vein images per-subject employed for our performance evaluation. The fingerprint image sub-database contains 100 fingers with randomly selected six impressions per-subject from FVC2002 database DB1 set A [23]. The finger knuckle print image sub-database consists of randomly selected 100 fingers with six knuckles images per-subject from PolyU Finger-Knuckle-Print database [24]. So, the merged database has virtually 100 subjects, and each subject use first 3 samples for training to generate the template and last 3 samples for testing in evaluations. There are totally 300 (100*3) genuine matching times and 29700 (100*99*3) imposter matching times for all users considered here.

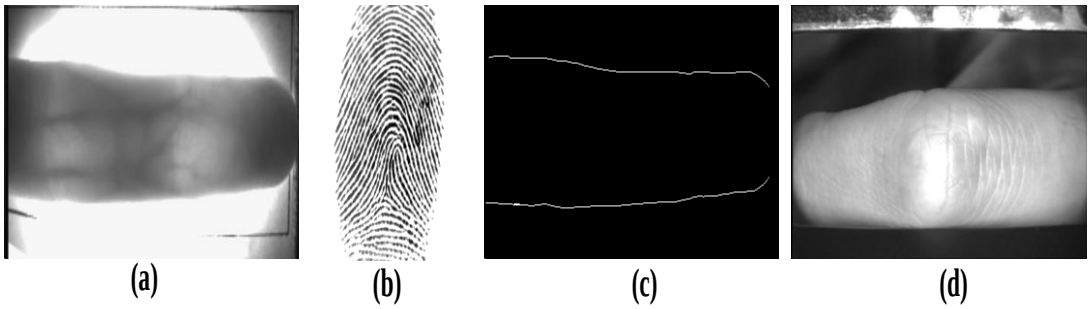


Figure 3. (a) Finger Vein Image Sample (b) Fingerprint Image Sample (c) Finger Knuckle Image Sample (d) Finger Shape Image Sample

The feature extraction methods of different finger modalities in this paper are listed as follows:

- The finger vein features in our pervious work [25] are extracted by Gabor wavelet and Local Binary Pattern (GLBP). GLBP feature representation of finger vein can improve the finger vein recognition performance.
- The fingerprint features are extracted as fixed length Finger Codes [1] by Gabor filters-based algorithm and the finger knuckle print features are extracted by the log-Gabor phase congruency (PC) model [4].
- The finger geometry is obtained by detecting edge lines between the finger region and the background region from the finger vein images by our pervious work [26]. The finger shape features are obtained by the Fourier descriptors (FD) method [2].
- The above four features extracted from multiple finger traits are further fused at feature level by the MCCA approach [21].
- All the values of above features are normalized within the same dimension by PCA method, as shown in Table. 1.
- All the normalized features are further transformed from real into binary representation by Algorithm.1, where the parameter N is set to 20.

Table 1. The Finger Biometric Features on the Merged Multimodal Finger Database

Abbrev	Description
FV	The real 128-dimension GLBP feature of finger vein
FP	The real 128-dimension Finger Code feature of fingerprint
FK	The real 128-dimension PC feature of finger knuckle print
FS	The real 128-dimension FD feature of finger shape
FVPKS-Serial	The real 512-dimension fused features based on serial feature fusion
FVPKS-MCCA	The real 208-dimension fused features based on MCCA fusion
FVB	The binary 270-dimension vector of *FV* feature
FPB	The binary 334-dimension vector of *FP* feature
FKB	The binary 259-dimension vector of *FK* feature
FSB	The binary 87-dimension vector of *FS* feature
FVPKSB-Serial	The binary 950-dimension vector of *FVPKS-Serial* feature
FVPKSB-MCCA	The binary 762-dimension vector of *FVPKS-MCCA* feature

4.2. Performance Evaluations

The evaluation protocols of False Match Rate (FMR), False Non-Match Rate (FNMR), Genuine Matching Rate (GMR, 1-FNMR), and Receiver Operator Characteristic (ROC) curve are used in this paper. We also use Equal Error Rate (EER, the point where FNMR is equal to FMR) to evaluate the performance in the experiments. In addition, the Shannon entropy is computed to evaluate the security of the proposed finger multi-biometric cryptosystem. Note that the lower value of EER shows the better verification performance, however, the higher value of entropy means the better security in biometric systems. We give abbreviations of the proposed finger multi-biometric cryptosystem approach as well as the individual biometric cryptosystems to facilitate the comparison. Each abbreviation is described as in Table 2.

Table 2. The Abbreviations of Different Methods

Abbrev	Description
FCS	Fuzzy Commitment Scheme
FCS-FVB	Finger vein cryptosystem using FCS
FCS-FPB	Fingerprint cryptosystem using FCS
FCS-FKB	Finger knuckle print cryptosystem using FCS
FCS-FSB	Finger shape cryptosystem using FCS
FMC-MCCA	Finger multi-biometric cryptosystem based on MCCA feature fusion
FMC-Serial	Finger multi-biometric cryptosystem based on serial feature fusion

a) Finger biometric verification performances:

We first give the verification accuracy of finger biometrics in real representation by ROC curves in Figure 4(a). The EER performance of *FV*, *FP*, *FK* and *FS* is 0.36%, 1.55%, 2.55%, 2.73%, respectively. After the binary transformation of features, the verification performances are shown in Figure 4(b). The corresponding EER performance of *FVB*, *FPB*, *FKB* and *FSB* is 0.36%, 1.81%, 2.17%, 2.82%, respectively. By comparing the EER performance between real and binary features, we can see that the bit extraction algorithm do not makes the verification performance worse and even improve the verification performance in *FKB* due to the reliable bit extraction.

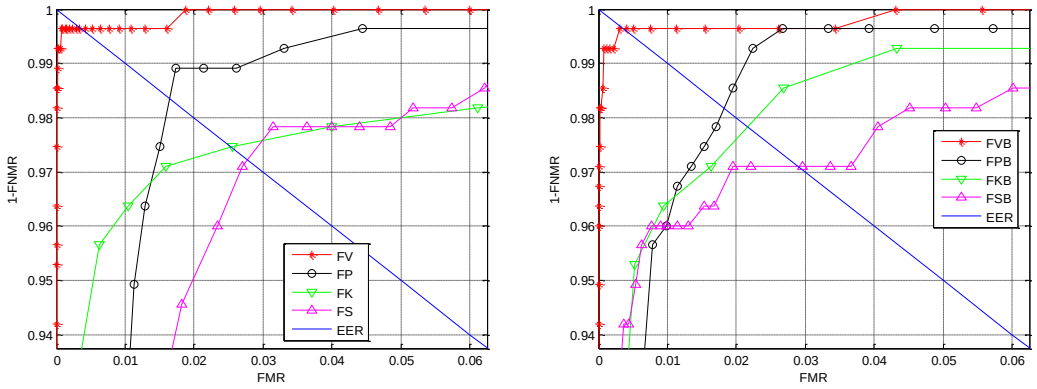


Figure 4. Finger Biometric Verification Performances: (a) the Features in Real Representation (b) the Features in Binary Representation

b) Finger individual Fuzzy Commitment scheme performances:

Before we implement Fuzzy Commitment Scheme (FCS) for each finger biometric traits, we have to determine the optimal BCH ECC codeword $[n, m, t]$ with Hamming distance (HD) and FMR. That is because of that the inter-class errors would be corrected if the ECC has the too high correcting capacity. This in turn will lead to higher false matching and improves FMR. In our system, based on the dimension of *FVB*, *FPB*, *FKB*, and *FSB*, the codeword length n of 511, 511, 511, and 127 are selected, respectively. The distribution of HD between intra-class and inter-class of *FVB*, *FPB*, *FKB*, and *FSB* are shown in Figure 5. The error correcting capacity t of BCH codeword should be chosen reasonably according to the HD threshold of different finger individual biometric traits. We find that the inter-class errors can be corrected with the higher error correcting capacity, however, the intra-class errors can not be corrected with the lower error correcting capacity. However, the entropy has the inverse trend, because of that there are more uncorrected error bits left, which need to be guessed by attackers. Hence, we make the trade-off between t and lower FMR to choose 62, 87, 87, and 31 bits as t of codeword for different individual FCS, respectively (see Table 3). The right column of Table 3 also provides the verification performance and the security of different finger individual FCS. According to *Eq.* 3, the average entropy of each individual FCS is also provided in Table 3. Although the verification performances of finger uni-biometric FCS change to be worse, they have higher security than before the implementation of template protection schemes.

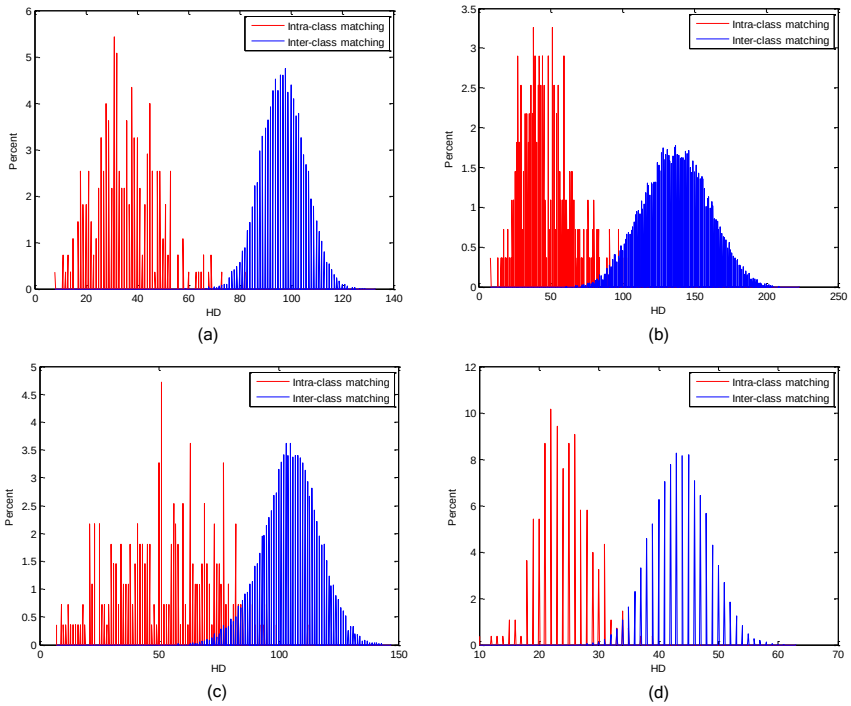


Figure 5. The HD Distribution between intra-class and inter-class of Finger Binary Features: (a) *FVB* (b) *FPB* (c) *FKB* (d) *FSB*

Table 3. The Selections of BCH ECC Codeword in Finger Individual FCS

Feature	Length (bits)	HD threshold (bits)	FMR %	BCH code [*n*, *k*, *t*]	FCS-Entropy (bits)	GMR %
			0.08	[511, 85, 63]	58.87	96.84
FVB	**270**	**66**	**0.01**	**[511, 94, 62]**	**60.73**	**96.37**
			8.76	[511, 76, 85]	41.85	100
			1.15	[511, 67, 87]	74.75	96.01
FPB	**334**	**86**	**0.90**	**[511, 76, 85]**	**78.20**	**96.01**
			1.95	[511, 58, 91]	67.97	96.01
			7.84	[511, 67,87]	26.35	96.73
FKB	**259**	**80**	**5.98**	**[511, 76, 85]**	**29.17**	**96.73**
			12.91	[511, 58, 91]	21.00	96.73
			0	[127, 22, 23]	25.45	46.73
FSB	**87**	**30**	**0.31**	**[127, 8, 31]**	**14.11**	**95.28**
			0.51	[127, 15, 27]	19.49	77.89

c) Finger multi-biometric cryptosystem performances:

For finger multi-biometric cryptosystem, the verification performance and the security are also contradictory, and we should make the tradeoff between them. Due to the dimension of *FVPKSB-Serial* and *FVPKSB-MCCA*, the BCH codeword length n is selected to 1023 for both *FMC-Serial* and *FMC-MCCA*. Furthermore, in Table 4, the trade-off between security

and lower FMR is made by choosing 66, 26 bits as t of codeword for *FMC-Serial* and *FMC-MCCA*, respectively. We compute the entropy of *FMC-Serial* and *FMC-MCCA* with the different error correcting capacity t (see Table 4). We notice that *FMC-MCCA* obtains the better security than *FMC-Serial* in every length of ECC. The best genuine accept rate is 100% and the security entropy is 212.9 bits at FMR of 0 in *FMC-MCCA*.

In fact, the comparative experiments ascertain that the finger multi-biometric cryptosystem based on feature-level fusion approaches can outperform the uni-biometric counterparts in terms of verification performance and security. In particular, the experimental results show that the proposed finger multi-biometric cryptosystem using MCCA feature fusion can be competent to combine different finger modalities effectively with the higher verification accuracy and security.

Table 4. Performance Results of Finger Multi-Biometric Cryptosystem

Scenario	Fusion method	Length (bits)	BCH code [*n*, *k*, *t*]	FMR %	GMR %	Entropy (bits)
FMC-Serial	Serial	950	[1023, 56, 191]	0	98.55	180.1
			[1023, 66, 189]	**0**	**99.79**	**198.68**
			[1023, 76,187]	0	98.19	187.2
FMC-MCCA	MCCA	762	[1023, 16, 223]	0	99.64	199.3
			[1023, 26, 239]	**0**	**100**	**222.9**
			[1023, 36, 247]	0	96.38	240.8

6. Conclusion

In this paper, a novel finger multi-biometric cryptosystems based on feature-level fusion is proposed, which are implemented on the fusion of fingerprint, finger vein, finger knuckle print and finger shape modalities. In addition, we have introduced an efficient bit extraction algorithm for transforming biometric representations and the reasonable choices of BCH codeword for Fuzzy Commitment Scheme. The security analysis methodology based on the BCH ECC correcting capacity has also been conducted elaborately. The experimental results show that the proposed finger multi-biometric cryptosystem has higher verification performance and security entropy.

Acknowledgements

This work is supported by Shanghai Minhang Science and Technology projects (Number: 2011MH073 and 2012MH172) and the Heilongjiang Province Educational Department Funds of China (11511286).

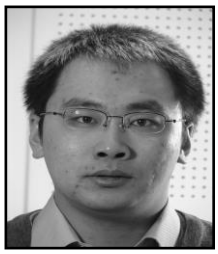
References

[1] K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "Filterbank-based Fingerprint Matching", IEEE Transactions on Image Processing, vol. 9, no. 5. **(2000)**.
[2] B. J. Kang and K. R. Park, "Multimodal Biometric Method based on Vein and Geometry of a Single Finger", Computer Vision, IET, vol. 4, no. 3, **(2010)**.
[3] A. Kumar and Y. Zhou, "Human Identification using Finger Images", IEEE Transactions on Image Processing, vol. 21, no. 4, **(2012)**.
[4] L. Zhang, L. Zhang, D. Zhang and Z. Guo, "Phase Congruency induced Local Features for Finger-knuckle-print Recognition", Pattern Recognition, vol. 45, no. 7, **(2012)**.
[5] J. Feng and A. K. Jain, "Fingerprint Reconstruction: From minutiae to phase", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 2, **(2011)**.

[6] S. Z. Li, "Editor", Encyclopedia of Biometrics, Springer, NJ, USA, **(2009)**.
[7] B. Kang and K. Park, "Multimodal Biometric Method that Combines Veins, Prints, and Shape of a Finger", Optical Engineering, vol. 50, no. 1, **(2011)**.
[8] J. Yang and X. Zhang, "Feature-level Fusion of Fingerprint and Finger-vein for Personal Identification", Pattern Recognition Letter, vol. 33, no. 5, **(2012)**.
[9] L. Q. Zhu and S. Y. Zhang, "Multimodal Biometric Identification System based on Finger Geometry, Knuckle print and Palm print", Pattern Recognition Letter, vol. 31, no. 12, **(2010)**.
[10] A. K. Jain, P. Flynn and A. A. Ross, "Handbook of Multibiometrics", Springer, NJ, USA, **(2008)**.
[11] A. Nagar, K. Nandakumar and A. K. Jain, "Multibiometric Cryptosystems based on Feature-level Fusion", IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, **(2012)**.
[12] B. Yanikoglu and A. Kholmatov, "Combining Multiple Biometrics to Protect Privacy", Proceedings of ICPR-BCTP Workshop, Cambridge, England, **(2004)** August 5-8.
[13] Y. Sutcu, Q. Li and N. Memon, "Secure Biometric Templates from Fingerprint-face Features", Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Minneapolis, United States, **(2007)** June 18-23.
[14] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme", Proceedings of the 6th ACM Conference on Computer and Communications Security, Singapore, Singapore, **(1999)** November 01-04.
[15] K. Nandakumar and A. K. Jain, "Multibiometric Template Security using Fuzzy Vault", IEEE 2nd International Conference on Biometrics: Theory, Applications and Systems, Arlington, United states, **(2008)** September 29-October 11.
[16] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", Designs Codes and Cryptography, vol. 38, no. 2, **(2006)**.
[17] S. Kanade, D. Petrovska-Delacretaz and B. Dorizzi, "Obtaining Cryptographic Keys using Feature Level Fusion of Iris and Face Biometrics for Secure User Authentication", 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition-Workshops, San Francisco, USA, **(2010)** June 13-18.
[18] B. Fu, S. X. Yang, J. Li and D. Hu, "Multibiometric Cryptosystem: Model Structure and Performance Analysis", IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, **(2009)**.
[19] E. Kelkboom, X. Zhou, J. Breebaart, R. Veldhuis and C. Busch, "Multi-algorithm Fusion with Template Protection", IEEE 3rd Int. Conf. Biometrics: Theory, Applications, and Systems, Washington, DC, USA, **(2009)** September 28-30.
[20] J. Yang, J. Y. Yang, D. Zhang and J. Lu, "Feature Fusion: Parallel Strategy vs. Serial Strategy", Pattern Recognition, vol. 36, no. 6, **(2003)**.
[21] J. Peng, Q. Li, Q. Han and X. Niu, "Feature-Level Fusion of Finger Biometrics Based on Multi-set Canonical Correlation Analysis", Lecture Notes in Computer Science, vol. 8232, **(2013)**.
[22] The Hong Kong Polytechnic University Finger Image Database Version 1.0., **(2010),** http://www.comp.polyu.edu.hk/~csajaykr/fvtdatabase.htm.
[23] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, "Handbook of Fingerprint Recognition", (Second Edition), Springer, London, UK, **(2009)**.
[24] PolyU Finger-Knuckle-Print Database, http://www.comp.polyu.edu.hk/˜biometrics, **(2010)**.
[25] J. Peng, Q. Li, A. A. A. El-Latif, N. Wang and X. Niu, "Finger Vein Recognition with Gabor Wavelets and Local Binary Patterns", IEICE TRANS. INF.SYST, vol. 96, no. 8, **(2013)**.
[26] J. Peng, Q. Li, N. Wang, A. A. A. El-Latif and X. Niu, "An Effective Preprocessing Method for Finger Vein Recognition", Fifth International Conference on Digital Image Processing, Beijing, China, **(2013)** Apr 21-22.

Authors

Li Lu, was born in China, on October 1974. She received the M.S degree and Dr. degree in Pattern Recognition and Intelligent System in Shanghai Jiao Tong University, Shanghai, P. R. China in 2006 and 2010, respectively. Now she is working in Shanghai Dianji University. Her research interests include face detection and recognition, gender classification and age estimation, fingerprint recognition, and multi-biometrics recognition. E-mail: lulihappy@163.com.



Jialiang Peng, was born in China, in November 1981. He received the B.S degree and M.S. degree in Computer Science in Heilong Jiang University, Harbin, P. R. China in 2002 and 2005, respectively. Now he is working in Information and Network Administration Center of Heilongjiang University. His research interests include vein recognition, fingerprint recognition, multi-biometrics recognition, template protection and information theory. E-mail: jialiangpeng@hlju.edu.cn.