An effective biometric cryptosystem combining fingerprints with error correction codes

Peng Li [a,1], Xin Yang [a,1], Hua Qiao [b], Kai Cao [c], Eryun Liu [c], Jie Tian [a,c,*]

[a] *Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China*
[b] *Satellite and Wireless Communication Lab, Peking University, Beijing 100871, China*
[c] *School of Life Sciences and Technology, Xidian University, Xi'an, Shaanxi 710071, China*

ARTICLE INFO

ABSTRACT

With the emergence and popularity of identity verification means by biometrics, the biometric system which can assure security and privacy has received more and more concentration from both the research and industry communities. In the field of secure biometric authentication, one branch is to combine the biometrics and cryptography. Among all the solutions in this branch, fuzzy commitment scheme is a pioneer and effective security primitive. In this paper, we propose a novel binary length-fixed feature generation method of fingerprint. The alignment procedure, which is thought as a difficult task in the encrypted domain, is avoided in the proposed method due to the employment of minutiae triplets. Using the generated binary feature as input and based on fuzzy commitment scheme, we construct the biometric cryptosystems by combining various of error correction codes, including BCH code, a concatenated code of BCH code and Reed–Solomon code, and LDPC code. Experiments conducted on three fingerprint databases, including one in-house and two public domain, demonstrate that the proposed binary feature generation method is effective and promising, and the biometric cryptosystem constructed by the feature outperforms most of the existing biometric cryptosystems in terms of ZeroFAR and security strength. For instance, in the whole FVC2002 DB2, a 4.58% ZeroFAR is achieved by the proposed biometric cryptosystem with the security strength 48 bits.

1. Introduction

Biometrics has emerged as a convenient and reliable technology to verify the identities of people, in place of traditional passwords or ID cards. As physical or behavioral characteristics, biometrics (such as fingerprint, iris, gait and so on) are not subjected to the worry of being forgotten or lost. And they are difficult to forge. However, the great drawback of biometrics, compared with password or ID cards, is its variational and noisy nature in the process of capturing (Jain, Flynn, & Ross, 2008b). This characteristic makes biometrics can not be authenticated, like the passwords or keys, by means of direct encryption or hashing. Usually pattern recognition methods are utilized in biometrics authentication, and consequently a raw version of biometric data extracted from a sample, named template, must be stored into the template database for the purpose of performing the matching process.

The raw storage of templates may bring serious security and privacy issues, because biometric traits can not be reset or replaced like passwords or ID cards (Jain, Nandakumar, & Nagar, 2008a). For an individual, the biometrics resources are limited, such as one face, ten fingers and two eyes. Once one's biometric sample is obtained by others of ulterior motives, the corresponding biometric trait is lost forever. Given most existing biometric systems equipped without liveness detection module, the lost biometric trait may bring terrible consequences. Biometric cryptosystem (Uludag, Pankanti, Prabhakar, & Jain, 2004) is proposed to solve the above problem. Biometric cryptosystems (Dodis, Reyzin, & Smith, 2004; Juels & Sudan, 2002; Juels & Wattenberg, 1999) utilize cryptographic technology or other particular technologies to "encrypt" the original biometric features into the encrypted domain and then store the "encrypted" templates into the database. Such "encryption" process is irreversible, that is to say, the original biometric features can not be directly obtained from the "encrypted" template. Meanwhile, usually one key of a certain length is involved in the process of designing the "encryption" method and ultimately it is concealed in the "encrypted" template. Only the query sample from the same trait with the template sample is input and the authentication is claimed successful, the right key is released and then used in the cryptographic circumstances. Nevertheless biometric cryptosystems are of single factor security mechanism, and it can not prevent from the attackers obtaining the

---

* Corresponding author at: Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China.

E-mail address: tian@ieee.org (J. Tian).

[1] These authors contribute equally to this work.

user's biometric sample by other means other than tampering the template database. Cancelable biometrics (Bolle, Connell, & Ratha, 2002; Lee, Choi, Toh, & Lee, 2007; Ratha, Chikkerur, Connell, & Bolle, 2007; Savvides, Vijaya Kumar, & Khosla, 2004), a two-factor authentication mode, is also proposed to solve the losing problem of biometrics. An irreversible transformation (Ratha et al., 2007) is the most important element for cancelable biometrics, and usually the transformation involves a personal key. Only both the right biometric sample and the right key are input, a positive verification signal is possible to be output. If one transformed template is lost, the user can promptly cancel it and replace it with another transformed version. The differences between biometric cryptosystems and cancelable biometrics lie in: (1) the former is a single-factor authentication method, but the latter is a two-factor one; (2) the former outputs a key but the latter just outs a Yes/No signal. Sometimes combining biometric cryptosystems with cancelable biometrics is necessary to make use of both of their advantages and construct more effective and secure biometric authentication system.

Fuzzy commitment scheme (FCS) (Juels & Wattenberg, 1999) is a smart biometric cryptosystem framework which can deal with hamming errors happening between different biometric samples. It demands for the binary length-fixed biometric feature b input into the system. Then a codeword c from error correction codes (Moon, 2005) is randomly selected. The XOR operation is conducted to obtain the "encrypted" template: $e = b \oplus c$. Meanwhile, the hash value of c, $h(c)$ (h denotes a hash function), is computed and stored together with e. In the decoding phase, a noisy biometric sample b' is presented and XORed with e to get e': $e' = b' \oplus e = b' \oplus b \oplus c$. Then the decoding algorithm is performed on e' to get codeword c'. If b and b' are both from the same biometric trait and within a certain thresholding in terms of hamming measure, we can have $c = c'$. This can be validated by checking if $h(c) = h(c')$.

In this paper, we attempt to extract discriminating binary length-fixed features from fingerprint images and combine them with various of error correction codes to construct an effective biometric cryptosystem based on FCS. As is well known, minutiae features, which are the most distinguishable among all the fingerprint features, is of set features and do not accord directly with the fuzzy commitment naturally. We propose to generate a binary string from the minutiae triplet set of a fingerprint image, with the assistance of user-specific question sets. The usage of minutia triplet, a translation and rotation non-variant feature, could avoid the procedure of aligning two fingerprint images, which is thought as difficult in the encrypted domain. And then various of coding algorithms are tested to find the best code to construct the effective biometric cryptosystem. The rest of this paper is organized as follows. In Section 2, related works on biometric cryptosystems and relevant feature extraction algorithms of fingerprints are reviewed. Section 3 presents the proposed binary length-fixed fingerprint feature generation method. Various coding strategies, including BCH code, a two-layer coding algorithm and LDPC code, are illustrated to construct an effective biometric cryptosystem in Section 4. Section 5 reports the experimental results on three fingerprint databases (one in-house and two public domain) to compare the performance of different coding strategies, as well as the security strength analysis. And we conclude this paper in Section VII.

2. Related works

Many previous works have been done in the biometric cryptosystem field. Fuzzy commitment scheme (Juels & Wattenberg, 1999) is a pioneer theoretical contribution to combine cryptography and biometrics in the sense of Hamming measure.

Hao, Anderson, and Daugman (2006) applied FCS to iris pattern and derived 140-bit keys from iris images at FRR = 0.47% and FAR = 0%. Zhang, Sun, Tan, and Hu (2009) concatenated Reed–Solomon code and Convolution code to construct iris cryptosystem based on FCS. They obtained the result of FRR = 0.52%(FAR = 0) with the key length of 938 bits. Bringer, Chabanne, Cohen, Kindarji, and Zemor (2008) deduced the theoretical boundary of binary secure sketch and developed a 2-D iterative Min–Sum decoding algorithm to obtain the practical boundary, which is close to the theoretical one. The experiments were conducted on both iris and fingerprint databases in their paper. Soutar, Roverge, Stojanov, Gilroy, and Kumar (1998) proposed to bind a private key with a fingerprint by Fourier Transform and derive it when the fingerprint identification succeeded. Juels and Sudan (2002) proposed a classical framework, named fuzzy vault, to bind a key to a biometric trait. Nandakumar, Jain, and Pankanti (2007) implemented the fuzzy vault for fingerprint and got encouraging results. Li et al. (2010) proposed an alignment-free version of fuzzy fingerprint vault and also obtained promising results. Dodis et al. (2004) generalized most of previous methods and gave a theoretical framework of generating robust key from biometric data and analyzed the security in the information theory sense. Many other researches (Boyen, 2004; Boyen, Dodis, Katz, Ostrovsky, & Smith, 2005; Bringer et al., 2008; Buhan, Doumen, Hartel, & Veldhuis, 2007; Li, Sutcu, & Memon, 2006; Sheng, Howells, Fairhurst, & Deravi, 2008; Sutcu, Li, & Memon, 2007) also concentrated on generating a key from biometric data. However, there are not encouraging experimental results reported in these literatures because of some implementation difficulty. Feng, Yuen, and Jain (2010) proposed to generate cancelable face template based on both biometric cryptosystem and transformation. Fu, Yang, Li, and Hu (2009) analyzed three structures of multibiometric cryptosystem and gave their performance comparison. Ignatenko et al. (2009) discussed the privacy and security issues of biometric systems from the viewpoint of information theory.

It can be found that few literatures reported the results of applying the FCS to fingerprint. The reason that it is a difficult task to extract a global length-fixed feature of high distinguishability from fingerprints. However, many researchers are working towards this task. Xu et al. (2009) proposed to generate length-fixed fingerprint feature from minutiae map by performing 2-D continuous Fourier Transform. But the resultant feature vector is in real number field, thus it can not be directly applied to template protection schemes, including FCS. Chen, Veldhuis, Kevenaar, and Akkermans (2008) proposed an optimal bit allocation method (OBA) to generate a binary string from face biometrics, at a pre-defined length with maximized overall detection rate. This method assumes the original biometric features are in the form of length-fixed real-value vector and this condition can not be easily satisfied for fingerprints. Cappelli, Ferrara, and Maltoni (2010) proposed a novel local binary string generation method of minutiae, called MCC, but it calls for special design of cryptographic framework to accommodate itself. Chang and Roy (2007) proposed a simple but illuminating method to extract binary strings from minutia sets. But only the minutiae locations are utilized and 8 ∼ 10 secret bits are extracted. One drawback of their work is that the algorithm employs the core points of fingerprints to align two corresponding fingerprints, which may lead to alignment inaccuracy because of core point detection errors or noise existing in the fingerprint images. Sutcu, Rane, Yedidia, Draper, and Vetro (2008) improved Chang and Roy (2007)'s method and took use of the minutiae's orientation information. More importantly, they proposed the desired property which need to be satisfied by a binary biometric string transferred in Binary Symmetric Channel (BSC). Nagar et al. (2010) extended Sutcu et al. (2008)'s work and integrate ridge orientation and ridge wavelength features into

the feature transformation process and obtain longer binary feature and better performance. Moreover, in Sutcu et al. (2008), a user-specific cuboid is employed to partition the minutiae set into two parts: the ones inside the cuboid and the ones outside it. And Principle Component Analysis (PCA) is performed on the computed feature vectors to weaken the correlation between the ones from different fingers. However, there are still several imperfections existing in Sutcu et al. (2008) and Nagar et al. (2010), which will be improved in this paper. They are listed as follows:

1. Still a core point is used to compute the alignment parameters. In this paper, we will employ the minutiae triplets as the basic input features, which are not sensitive to rigid transformation and do not need the alignment procedure.
2. The crossover probability p of BSC is still large. And it will be made smaller in this paper by several means, including: (1) replacing PCA with Linear Discriminant Analysis (LDA); (2) storing user-specific thresholding information. As well, the usage of the minutiae triplets accounts for the dropping of p to some extent.
3. Lacking performance comparison between different Error Correction Codes (ECC). Various of effective ECCs are examined to find the best one which adapts to the proposed binary string generation method in this paper.
4. Experimental results reported is on an in-house fingerprint database. The proposed method in this paper will be tested on two more public fingerprint databases to show its good performance.

3. Binary length-fixed fingerprint feature generation

Minutiae triplet is a kind of fingerprint feature with high distinguishability (Bhanu, Tan, & Member, 2003; Chen, Tian, Yang, & Zhang, 2006), as is illustrated in Fig. 1. It will be employed as the basic feature in this paper. A six-dimension vector, $(l_1, l_2, l_3, \theta_1, \theta_2, \theta_3)$, is computed for each triplet. The first step is to select the relatively reliable minutiae triplets from all the combination of 3-minutia tuples in a fingerprint image. The selection criteria is shown as follows:

$$\begin{cases} l_i \geqslant t_{side}, (i = 1, 2, 3) \\ S(m_1, m_2, m_3) \geqslant t_{area} \end{cases} \tag{1}$$

where, t_{side} denote the thresholding of side length and S denotes the thresholding of the area of the triangle formed by m_1, m_2, m_3. It is obvious that the six dimension feature is a relative feature, which means the alignment procedure can be avoided when it is employed as the input of feature transforming process, just as the way Chang and Roy (2007) and Sutcu et al. (2008) did.

Before describing our proposed feature transformation method, we have to point out that one main contribution of Sutcu et al. (2008) is the concept of transforming minutiae map to feature
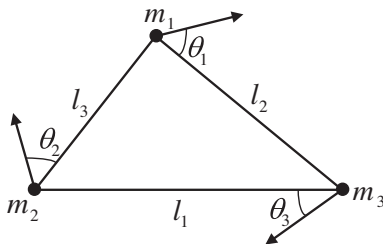

Fig. 1. A fingerprint minutiae triplet. Where, $m_i(i = 1, 2, 3)$ denotes three arbitrary minutiae in a fingerprint; $l_i(i = 1, 2, 3)$ denotes the ith side opposite the corresponding minutia; and $\theta_i(i = 1, 2, 3)$ denotes the ith angle. Taking θ_1 as an example, it is the smaller angle formed by m_1's direction and l_2, other than l_3.

vectors explicitly matched with error correction codes for BSC. The corresponding properties desired by BSC are summarized in Sutcu et al. (2008) and elaborated as: (1) a bit is equally likely to be 0/1; (2) different bits in a given feature vector are independent of each other; (3) feature vectors from different fingers are independent of each other; (4) two feature vectors from the same finger are statistically related by a BSC-p.

In this paper, we follow the above defined rules, but propose a feature vector generation method which is more compact with the rules. In Sutcu et al. (2008), the authors used two smart techniques: user-specific questions and 0/1 decision by Bernoulli tries. We borrow the concept of "questions" which stands for the operation of counting the number difference between the minutiae inside a cuboid and the minutiae outside it. But the "question" in this paper refers to a super plane according to the MT feature vector $V = (l_1, l_2, l_3, \theta_1, \theta_2, \theta_3)$. The "question" vector can be defined as $Q = (s_1, s_2, s_3, a_1, a_2, a_3)$. The MT feature vector V is "asked" a question Q as the way Eq. (2) shows.

$$Q(V) = \sum_{i=1}^{3} \left(\frac{l_i}{s_i} + \frac{\theta_i}{a_i} \right) \tag{2}$$

meanwhile, the following empirical equation must be satisfied:

$$\begin{cases} 0 < s_i \leqslant 8.6 \times (w^2 + h^2), & i = 1, 2, 3, \\ 0 < a_i \leqslant 1105, & i = 1, 2, 3, \end{cases} \tag{3}$$

where, $s_i(i = 1, 2, 3)$ are parameters for side length $l_i(i = 1, 2, 3)$, and $a_i(i = 1, 2, 3)$ for angles $\theta_i(i = 1, 2, 3)$; w and h denotes the width and height of fingerprint images, respectively; 8.6 and 1105 are empirical values and these two values can ensure the generated random super planes are relatively discriminating and uncorrelated. Given a minutia triplet set $V = \{v_i, i = 1, 2, \ldots, n\}$ and a random question q, we compute the numbers of feature vectors, num_1 and num_2, which make $q(v_i) \geqslant 1$ and $q(v_i) < 1$, respectively. Thus the output of the question q is the resultant difference $d = num_1 - num_2$.

It is obvious that some random questions could be more reliable than others. Given a question for one fingerprint, if the resultant difference d is removed far from the average value of this question on many fingerprints from the same finger, it is thought as reliable; otherwise it is unreliable. Considering that the final feature vector should be a binary string, another immediate issue is how to decide the output real-value of a question to be binarized to 0 or 1. As Sutcu et al. (2008) did, the selection of reliable questions and the expected 0/1 decision of a question are also considered in this paper. But the methods we developed are different. The difference will be detailed in the following paragraphs.

The overall feature generation process comprises two parts: training process and feature generation process.

3.1. Training process

The overall flowchart of the training process is illustrated as Fig. 2. The detailed steps of the training process are as follows.

1. For the ith user in the training process, its p fingerprint samples are input and processed by fingerprint enhancement algorithms like (Jain, Hong, & Bolle, 1997). Then the minutiae are extracted from the enhanced images and the minutiae triplet sets $\{T_{ij}^t, j = 1, \ldots, p\}$ are obtained by Eq. (1), where $T_{ij}^t = \{t_{ij1}^t, t_{ij2}^t, \ldots, t_{ijn}^t\}$ and n denotes the number of triplets in the jth training sample of the ith user, and the superscript t denotes that the sets T_{ij}^t are from template fingerprints.
2. Corresponding to user i, a set of random questions $Q_i = \{Q_{ik}|k = 1, \ldots, q\}$ are generated according to Eqs. (2) and
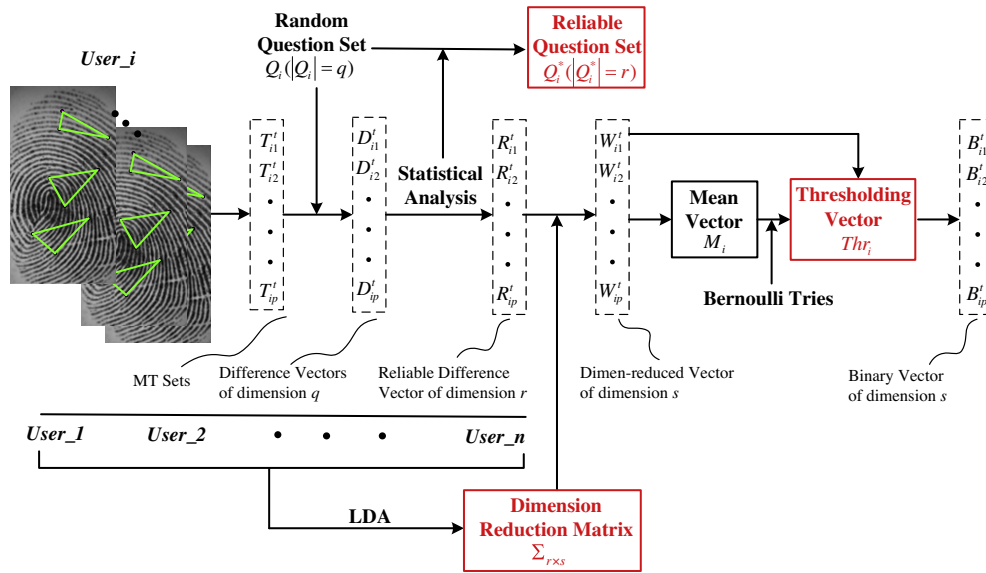
Fig. 2. The overall flowchart of the training process of binary length-fixed feature generation. The red items need be stored in the central database or user's personal token and will be used in the verification process.

(3). Using one question Q_{ik} to "ask" the minutiae triplet set T_{ij}^t, the "answer" is the number difference of the triplets locating different sides of the super plane. Therefore applying Q_i to T_{ij}^t will yield a vector D_{ij}^t of dimension q.

3. Calculate the variation vector Var_i of user i by the difference vectors $\left\{D_{ij}^t, j = 1, \ldots, p\right\}$. Then select the r smallest values in Var_i as what we want to reserve and record their indexes in the vector. These indexes correspond the most reliable questions in Q_i, which compose of $Q_i^*\left(|Q_i^*| = r\right)$, a reliable question set corresponding to the user i. The entries of D_{ij}^t in the corresponding positions are picked out to constitute reliable difference vectors R_{ij}^t of dimension r. Note that we call the feature generation process by the way of selecting reliable user-specific questions "user-specific question way". Correspondingly, the way that a set of common questions are used by all the users is named as "common question way".

4. Here we can fix a certain number of users among all the N users, say n, taking part in the training process, i.e., $n \leqslant N$. After the resultant reliable difference vectors $\left\{R_{ij}^t | i = 1, \ldots, n; j = 1, \ldots, p\right\}$ are obtained, the linear discriminant analysis (LDA) is used to reduce the vector dimension and eliminate the correlation between the feature vectors from different users. The dimension reduction matrix obtained is denoted as $\Sigma_{r \times s}$. And then $\left\{R_{ij}^t | i = 1, \ldots, n; j = 1, \ldots, p\right\}$ of dimension r is transformed to $\left\{W_{ij}^t | i = 1, \ldots, n; j = 1, \ldots, p\right\}$ of dimension s, by multiplication with $\Sigma_{r \times s}$. Here the fixed n, smaller than N, can make the dimension reduction matrix $\Sigma_{r \times s}$ keep relatively unchanging, eliminating the need of updating it with the increase of the number of users, N, in the training process.

5. The next step is to binarize $\left\{W_{ij}^t | i = 1, \ldots, n; j = 1, \ldots, p\right\}$ using a certain thresholding value. To make the probability of 0/1 happening in the resultant binary vectors as equal as possible, we propose to set the user-specific thresholding for each user. First, for the user i, the mean vector M_i of $\left\{W_{ij}^t | j = 1, \ldots, p\right\}$ is computed. Then s times of Bernoulli tries are conducted to get the expected binary vector $E_i = \{E_{ij}, j = 1, \ldots, s\}$. Thus, the binarization thresholding Thr_{ij} of user i is defined as:

$$Thr_{ij} = \begin{cases} \frac{1}{2}M_{ij}, & E_{ij} = 1 \quad \text{and} \quad M_{ij} \geqslant 0, \\ 2M_{ij}, & E_{ij} = 1 \quad \text{and} \quad M_{ij} < 0, \\ 2M_{ij}, & E_{ij} = 0 \quad \text{and} \quad M_{ij} \geqslant 0, \\ \frac{1}{2}M_{ij}, & E_{ij} = 0 \quad \text{and} \quad M_{ij} < 0, \end{cases} \tag{4}$$

where, j covers $1, \ldots, s$.

6. W_{ij}^t can be binarized to obtain B_{ij}^t by the following equation:

$$B_{ij}^t = \begin{cases} 1, & W_{ij}^t \geqslant Thr_{ij}, \\ 0, & W_{ij}^t < Thr_{ij}. \end{cases} \tag{5}$$

Given $Thr_{ij} \equiv 1$, Eq. (5) yields to the binarization method by common thresholding. We call these two binarization methods as "user-specific thresholding way" and "common thresholding way", respectively.

It is worth note that after the training process is finished, three parts of important user-specific helper data (i.e., HD in Fig. 4) are stored into the central database or personal token, including Reliable Question Set Q_i^*, Dimension Reduction Matrix $\Sigma_{r \times n}$ and Thresholding vector Thr_i, which are emphasized using red color in Fig. 2.

3.2. Feature generation process

The overall flowchart of the feature generation process is illustrated as Fig. 3. Its detailed steps are described as follows.

1. Given z query fingerprint samples of user i, the same fingerprint pre-processing, enhancement and minutiae extraction algorithms as in the training process are performed to obtain the query minutiae maps. Then minutiae triplets $\left\{T_{ij}^q, j = 1, \ldots, z\right\}$ are selected by using Eq. (1), where $T_{ij}^q = \left\{t_{ij1}^q, t_{ij2}^q, \ldots, t_{ijz}^q\right\}$ and z denotes the number of triplets in the jth query sample of the ith user, and the superscript ^{q} denotes that the sets T_{ij}^q are from query fingerprints.

2. Apply the user-specific Reliable Question Set $\{Q_i^*(|Q_i^*| = r)\}$, obtained in the training process, to T_{ij}^q and then obtain the resultant reliable difference vectors R_{ij}^q of dimension r.
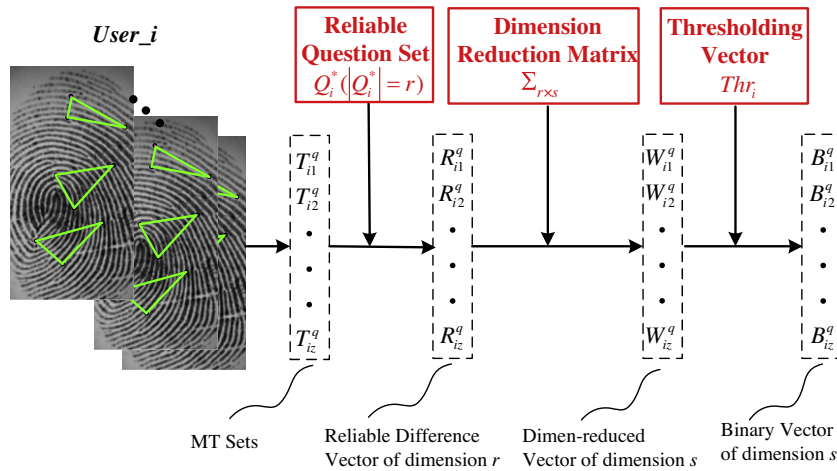
Fig. 3. The overall flowchart of the binary length-fixed feature generation process. The red items need to be retrieved from the central database or user's personal token. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

3. Multiply R_{ij}^q with $\Sigma_{r \times n}$ to obtain dimension-reduced vectors R_{ij}^q of dimension s.
4. Binarize R_{ij}^q using user-specific thresholding Thr_i by Eq. (5) to output binary feature vectors B_{ij} of dimension s.

Please note that, if the common question set or/and the common thresholding are adopted, the above steps need to be modified according to the real scenario.

4. Biometric cryptosystem construction using ECCs

After the binary length-fixed feature vectors are obtained, the following task is to construct a biometric cryptosystem using the proposed feature generation method. We base this task on the known scheme of fuzzy commitment (Juels & Wattenberg, 1999), which is designed specifically for binary biometric feature vectors and the Hamming measure. The overall block diagram of the biometric cryptosystem based on FCS is shown in Fig. 4. The operation details of FCS have been depicted in Section 1. In the overall operation process, error correction code (ECC) is the important factor to construct an efficient and robust biometric cryptosystem. There have been several effective ECCs developed or investigated by the researchers (Bringer et al., 2008; Hao et al., 2006; Sutcu et al., 2008). Because it is difficult to find the exact error pattern of our proposed feature generation method, we will implement several biometric cryptosystems using different effective ECCs and compare their performances based on large scale experimental

results in this paper. They are including: BCH code, two-layer concatenated code of Reed–Solomon code and BCH code, and LDPC code.

4.1. BCH code

A BCH code is a polynomial code over a finite field with a particularly chosen generator polynomial. It is a cyclic code. Here we adopt the narrow sense BCH code (Moon, 2005).

A narrow sense BCH code over $GF(q)$ of length n capable of correcting at least t errors is specified as follows:

1. Determine the smallest m such that $GF(q^m)$ has a primitive nth root of unity β.
2. Write down a list of $2t$ consecutive powers of β:

$$\beta, \beta^2, \ldots, \beta^{2t}.$$

Determine the minimal polynomial with respect to $GF(q)$ of each of these powers of β.
3. The generator polynomial $g(x)$ is the least common multiple (LCM) of these minimal polynomials. The code is a $(n, n - deg(g(x)))$ cyclic code. Where, $deg(g(x))$ denotes the degree of polynomial $g(x)$.

When it comes to decoding, there are many methods, for example, calculating the syndrome values for the received vector and so on.
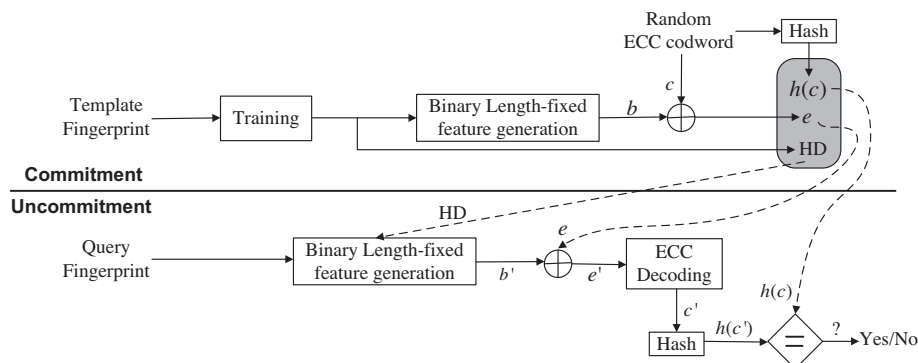

Fig. 4. The overall block diagram of the biometric cryptosystem based on FCS. The symbol "$\oplus$" denotes the operation of exclusive or. The three items in the grey frame are what need to be stored in the central database or personal token. "HD" in the diagram refers to helper data obtained from the training process.

Usually we use $BCH(n,k,t)$ to denote a BCH code, where n is the code length of bits, k the message length of bits and t the error correction capability.

4.2. Two-layer concatenated code

Hao et al. (2006) proposed a two-layer concatenated code ("Conc. code" for short) of Hadamard code and Reed–Solomon code to correct the random errors happening on IrisCode. And they claimed to have achieved good results on an in-house iris database. Here we propose to employ the similar method to correct the errors of our proposed binary fingerprint features. The difference lies in that the BCH code, instead of Hadamard code, is used in the inner layer. In the outer layer, we still employ Reed–Solomon code.

Reed–Solomon code is a kind of linear block code. It is a special case of BCH code (Moon, 2005). Let α be a primitive element in $GF(q^m)$ and let $n = q^m - 1$. Let $m = (m_0, m_l, \ldots, m_{k-1}) \in GF(q^m)^k$ be a message vector and let $m(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1} \in GF(q^m)[x]$ be its associated polynomial. Then the encoding is defined by the mapping $\rho : m(x) \mapsto c$ by

$$(c_0, c_1, \ldots, c_{n-1}) \triangleq \rho(m(x)) \triangleq (m(1), m(\alpha), m(\alpha^2), \ldots, m(\alpha^{n-1})). \tag{6}$$

That is, $\rho(m(x))$ evaluates $m(x)$ at all the non-zero elements of $GF(q^m)$. We use $RS(n,k)$ to denote a Reed–Solomon code, and the corresponding error correction capability $t = (n - k)/2$.

In practice, we need to use the Reed–Solomon code specially according to the limitation of the dimension of binary feature vectors. For example, for binary feature vectors of dimension 255, one designed method of concatenated code is $BCH(15,7)$ plus $RS(17,11)$. But $RS(17,11)$ does not exist indeed. We need to use $RS(127,121)$ at least, because $RS(n,k)$ over $GF(2^7)$ must satisfy that $n \geqslant 127$. The special usage of $RS(17,11)$ requires padding a 110-zero block in the error correcting process. In fact, we only use a part of the whole Reed–Solomon code, which is called RS code after deletion.

4.3. LDPC code

LDPC codes are capacity-approaching codes, which means that practical constructions exist that allow the noise threshold to be set very close (or even arbitrarily close on the BEC) to the theoretical maximum (the Shannon limit) for a symmetric memory-less channel. The noise threshold defines an upper bound for the channel noise up to which the probability of lost information can be made as small as desired. Using iterative belief propagation techniques, LDPC codes can be decoded in time linear to their block length. LDPC codes are defined by a sparse parity-check matrix. This sparse matrix is often randomly generated, subject to the sparsity constraints. These codes were first designed by Gallager in 1962.

We use some specially designed Quasi Cyclic LDPC code (QC-LDPC) (Qiao, Guan, Dong, & Xiang, 2008) to construct biometric cryptosystems in this paper. These QC-LDPC codes are designed

Table 1
Error correcting success rates of LDPC codes of 10000 random binary vectors with various amounts of random bit errors.

Random error number	42	45	50
LDPC (255,75)	0.6882	0.4118	0.0870
LDPC (255,70)	0.8452	0.6639	0.2355
LDPC (255,65)	0.9143	0.8046	0.4970
LDPC (255,55)	0.9898	0.9723	0.8651
LDPC (255,50)	0.9959	0.9911	0.9540
LDPC (255,45)	0.9981	0.9964	0.9846

based on circulant permutation matrices. The method chooses the position of each non-zero sub-matrix in the bipartite graph based on blocks. Then the circulant permutation value of each sub-matrix is decided. It can be seen as structural construction method of LDPC codes. Unlike BCH code and Reed–Solomon code, LDPC code is a probability coding strategy to some extent. $LDPC(n,k)$ represents an LDPC code with code length n and information bit length k. To examine the error correction capability of the LDPC codes used in this paper, we randomly generate 10000 binary vectors of dimension 255 and randomly produce a certain amount of bit errors. Afterwards, we use the LDPC codes to correct these binary vectors with random errors and get the error correcting success rates, which are shown in Table 1.

5. Experimental results and analysis

5.1. Databases and evaluation indicators

We select three fingerprint databases to evaluate the performance of the proposed biometric cryptosystems, including: (1) FX3000 database (FX3000 for short), a subset of Fingerpass Cross-matching Database; (2) FVC2002 DB1 (DB1 for short) and 3) FVC2002 DB2 (DB2 for short). FX3000 is an in-house database with 720 fingers and 12 samples for each finger, and it is adopted for the convenience of training and showing the promising results. DB1 and DB2 are both public-domain databases. Their characteristics are summarized in Table 2. With regard to the partition of training set and test set, for FX3000, the first 8 samples of each finger are used for the training purpose and the first 4 ones of DB1 and DB2 for training. Then the remaining samples of each finger for these three databases are utilized for the testing purpose.

To evaluate the distinguishing ability of the binary feature, we use Equal Error Rate (EER) of matching them in the term of hamming distance. Moreover, like Sutcu et al. (2008), the crossover probability p is used to assess the applicability to BSC of the binary feature. And the histogram of numbers of 1's in the features is employed to show the statistical independence of the bits. When it comes to the overall biometric cryptosystem, the False Reject Rate (FRR), when False Accept Rate (FAR) equals 0 i.e., ZeroFAR, is the main indicator to assess its performance. In addition, the system security strength, in terms of bit length, is employed to assess the probability of the system being attacked successfully by brute force.

Table 2
Summary of databases used in our experiments.

	FX3000	DB1	DB2
Resolution	569 dpi	500 dpi	569 dpi
No. of fingers	720	110	110
No. of impression per finger	12	8	8
Sensor	Biometrika FX3000 (Optical)	Identix TouchView II (Optical)	Biometrika FX2000 (Optical)
Image Size	400×560	388×374	296×560
Image Quality	Good	Medium	Medium

5.2. Analysis of the binary length-fixed feature

According to the way of selecting questions and thresholding, we categorize the feature generation process into four types: (1) the type of User-specific Questions and User-specific Thresholding (UQUT way); (2) the type of User-specific Questions and Common Thresholding (UQCT way); (3) the one of Common Questions and User-specific Thresholding (CQUT way); (4) the one of Common Questions and Common Thresholding (CQCT way). In the following experiments, we will compare the EER results under these four hypothesis and show the advantage of the proposed feature generation method.

5.2.1. Feature length issue

Due to the difference of sensors and fingerprint image quality, the optimal binary feature lengths for different databases vary correspondingly. Without loss of generality, we select the UQUT hypothesis for determining the optimal feature length for three databases. Fig. 5 shows the EERs of the resultant binary feature vectors of different length in the terms of hamming distance. From the first figure, i.e., the FX3000 database, it can be seen that the EERs with feature length smaller than 400 almost equal. For convenience, the length 255 is selected for the experimental test and comparison. In fact, feature vectors of length equalling other numbers smaller than 400 are also applicable in the practical system. For the second and third figures, the optimal feature lengths are 230 and 220 for DB1 and DB2, respectively; because the corresponding EERs are lowest. In the following experiments, we will fix the feature lengths to these optimal numbers.

5.2.2. Classification performance comparison under four hypothesis and performance under attack scenario

In this sub section, we will select the FX3000 database to conduct EER comparison experiments under four decoding hypothesis: UQUT, CQUT, UQCT and CQCT, as well as the attack experiment, which is based on the hypothesis that the user's personal helper data is stolen by the attacker who knows our system and method very well. Please note, as is depicted in Section 3.1, that just 200 fingers are used in the phase of training the dimension reduction matrix. It is out of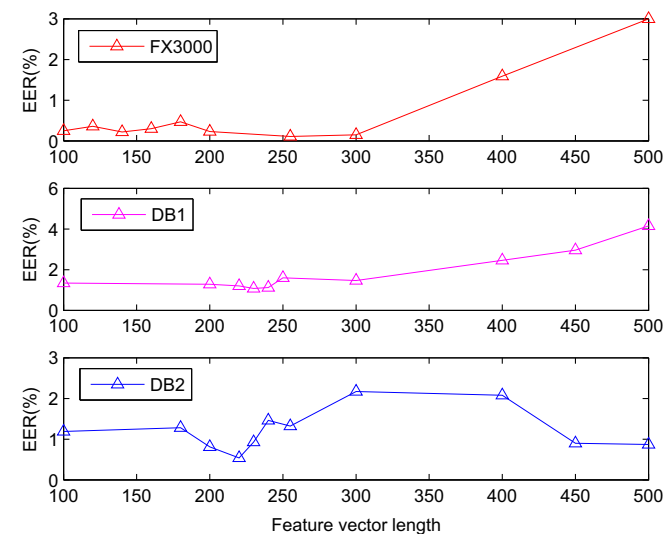 consideration for the practical application. In fact, if all the fingers of the database are used for training the matrix, the results will be better.

Fig. 6 shows the distributions of genuine and imposter matching under four hypothesis: (a) and (b) are training results and test results respectively under UQUT, (c) and (d) are subjected to CQUT; while (e) and (f) are under UQCT, (g) and (h) are subjected to CQCT. The vertical dashed lines denote the thresholding point where the value of EER is computed. And at the top of the dashed lines, we give the EER value, and the crossover probability p which is computed on the genuine matchings. The EER values can be used to qualitatively speculate the FAR value of the constructed biometric cryptosystem. The crossover probability can be defined as the number of bit errors happening in the binary vectors from the same finger to the vector length. And the value of p can be qualitatively used for estimating the FRR value. Given appropriate error correction codes, lower EER and smaller p make the FAR and FRR low, respectively. The details about the crossover probability will be depicted in the next sub section.

In particular, from Fig. 6, we can see that both the user-specific question set and user-specific thresholding strengthen the distinguishability of the binary feature at the same time. That is because the performances under both UQCT and CQUT are much better than CQCT. Take the test EER for instance, CQCT's EER is 22.7%, and UQCT's EER and CQUT's EER are 0.63% and 5.06%, respectively. Moreover, the performance improvement by UQCT is larger than CQUT. This is can be explained by that the user-specific question set plays a more important role in augmenting the distinguishability of the obtained binary feature than the user-specific thresholding.

Fig. 7 illustrates the EERs in the attack scenario, in which it is assumed that the legal user's personal question set and thresholding are stolen by the attacker. From Fig. 7, we can see that the attack distribution curve shifts towards the right. That is to say that the difficulty for the attacker with the stolen helper data is similar with the attacker without the legislated user's helper data. Even if the user's helper data is lost, the performance of the system has just a tiny decrease, which can assure the user's privacy from leaking to a large extent.

5.2.3. 1's Number and the crossover probability

As stated in Sutcu et al. (2008), the resultant binary feature vectors should have approximately equal numbers of 1s and 0s. Thus the vectors can accord with the ECCs working on the BSC more tightly. Here we examine the 1's number under four decoding hypothesis: UQUT, UQCT, CQUT, and CQCT. Fig. 8 gives the training and test distribution of the 1's numbers, under those four hypothesis above respectively. Note that the length of the feature vector is 255, that is to say, the most ideal distribution is like that, in which overwhelming majority of the 1's locate near 127 or 128. It is easy to see that the UQUT test distribution performs the best among the four test scenarios. And both the UQCT test distribution and the CQUT test distribution perform better than the CQCT test distribution. It can be inferred that both the user-specific question technology and the user-specific thresholding technology helps to make the 1's number well-distributed, and their combination can produce the best distribution.

From Fig. 6, we can see that the crossover probability p's of test scenarios under UQUT, UQCT and CQUT are 0.06, 0.024 and 0.074, respectively. It can be inferred that the user-specific is of great help in decreasing the cross probability, which is very useful for lowering the FRR of the biometric cryptosystem. Because the crossover probability of UQCT is more smaller than that of UQUT, it can be found that the personal thresholding technology goes against lowering the crossover probability. However, the smaller crossover probability only affects the FRR. And the user-specific thresholding technology is beneficial to obtain lower FAR. Therefore, based on comprehensive consideration, the user-specific question technol-

Fig. 5. EERs of the resultant binary feature vectors of different length in the terms of hamming distance. The first figure, i.e., the red line, denotes the results of FX3000 database. And the second and the third denote the results of DB1 and DB2, respectively. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)
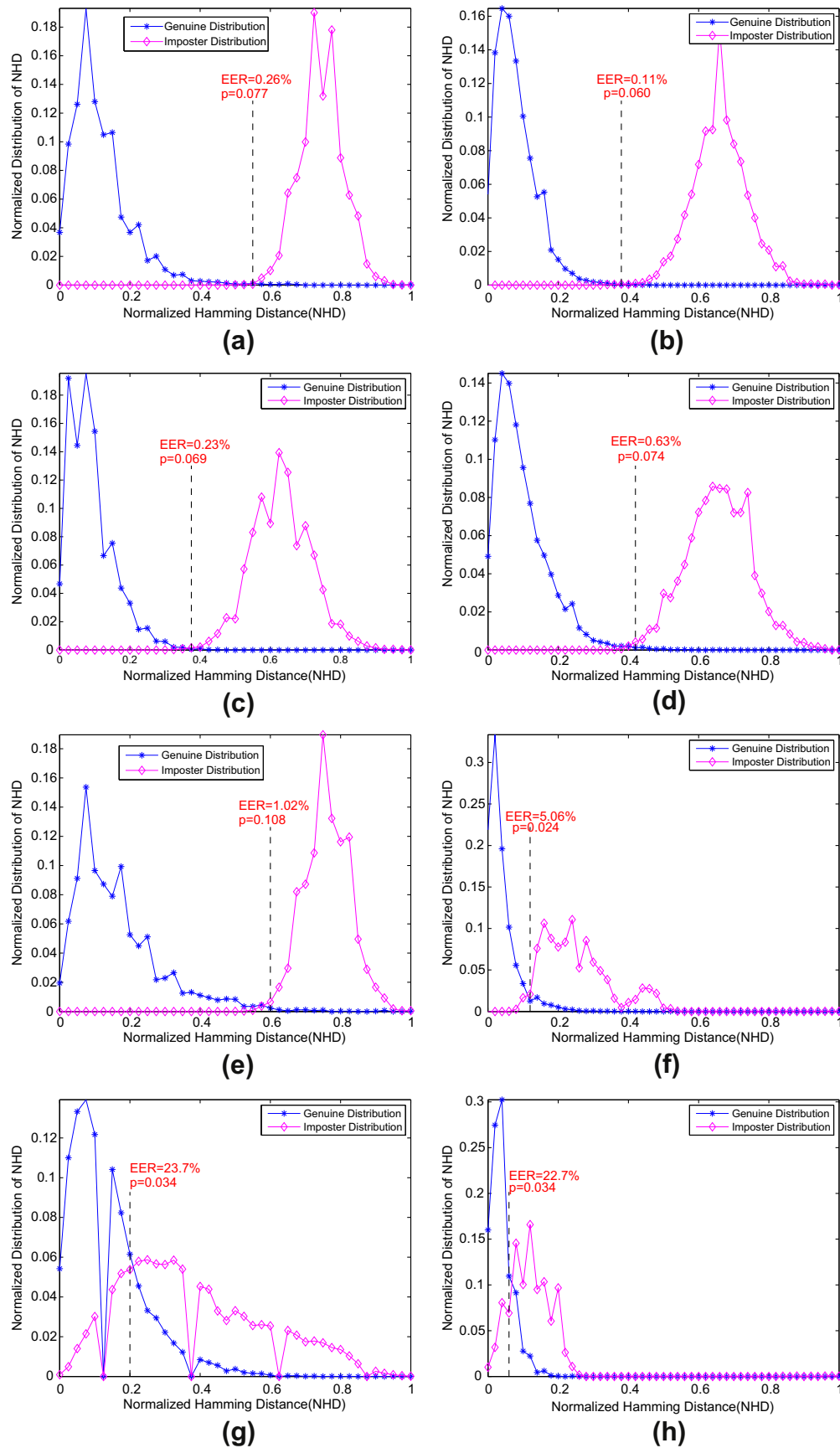
Fig. 6. EER comparison under four hypothesis. (a) and (b) are training EER and test EER, respectively, under UQUT; (c) and (d) under UQCT; (e) and (f) under CQUT; (g) and (h) under CQCT.
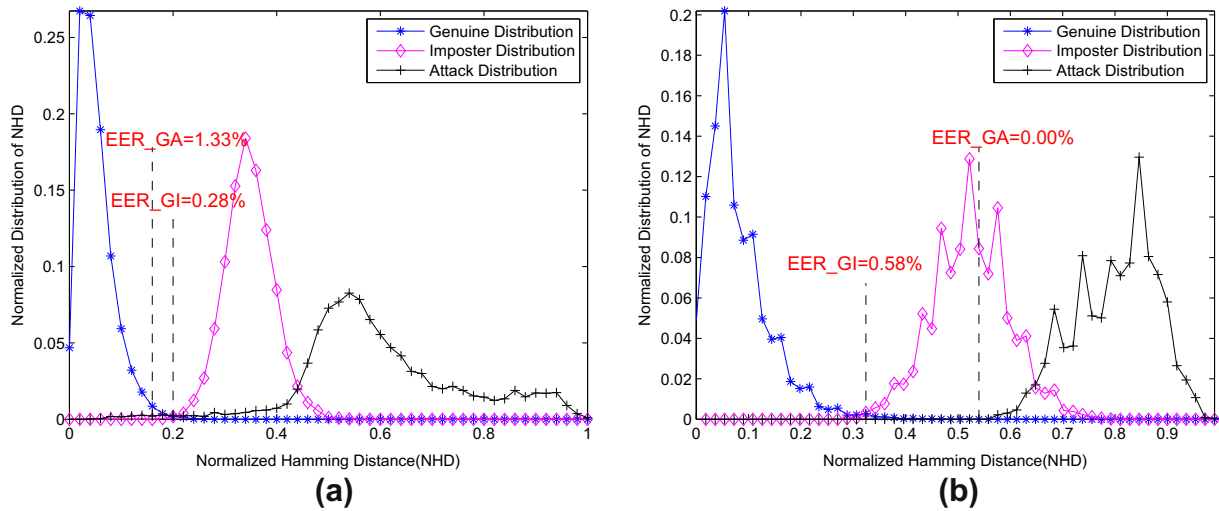
Fig. 7. EER comparison between normal scenario and attack scenario. Fig. 6(a) denotes the training case and Fig. 6(b) the test case. EER_GI denotes the EER of the genuine distribution and the imposter distribution, while EER_GA denotes the one of the genuine distribution and the attack distribution. Due to the difference of the hamming distance normalization and the step selection in EER computation, the EER_GI here has a little difference from the EER in Fig. 6(a) and Fig. 6(b).
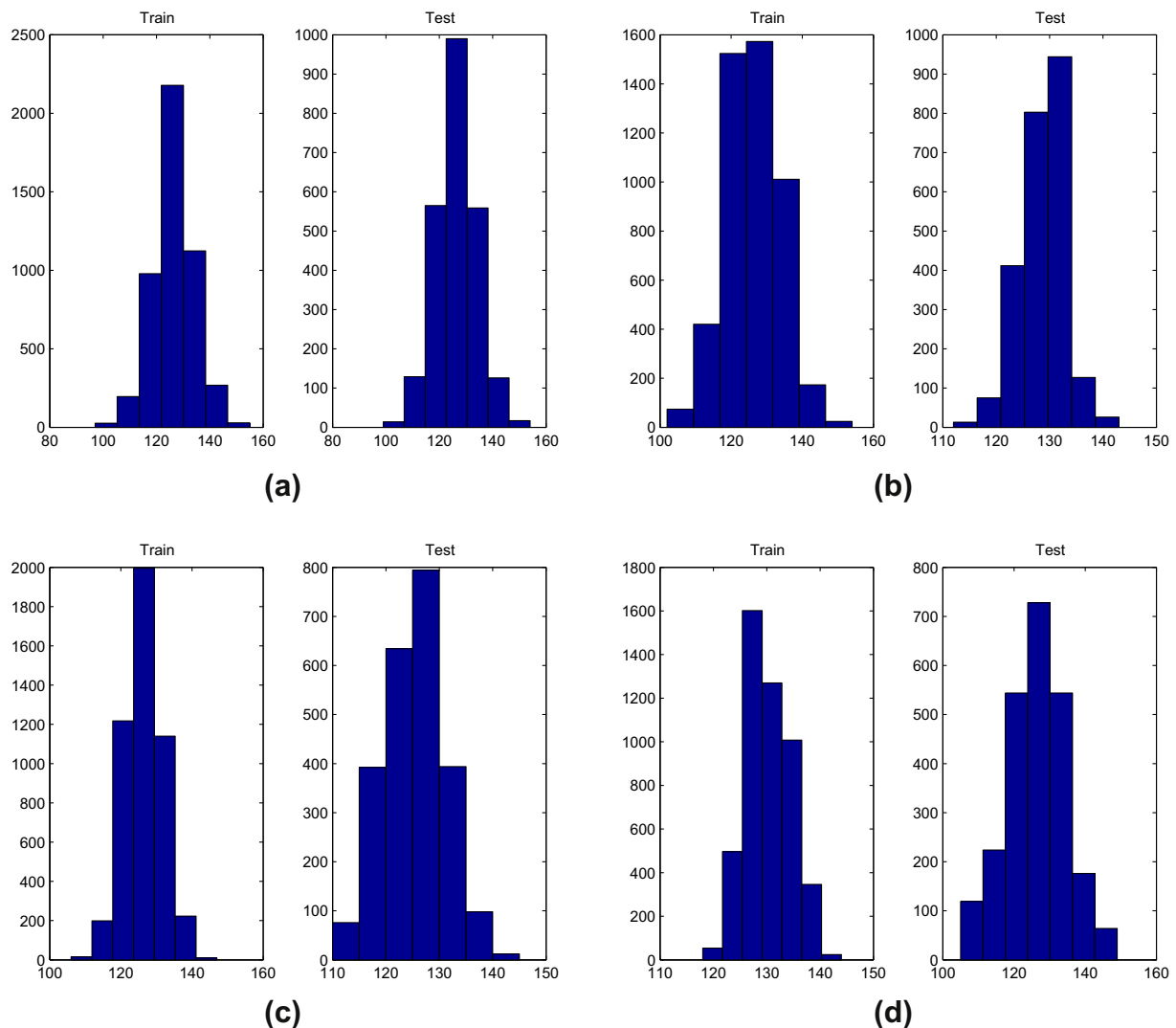

Fig. 8. 1's number distributions of training set and test set under four different hypothesis. The horizontal axis is the 1's number, and the vertical axis is the number of the feature vectors of a certain length. (a) UQUT hypothesis; (b) UQCT hypothesis; (c) CQUT hypothesis; (d) CQCT hypothesis.

Table 3
Experimental results of biometric cryptosystems by BCH code on FX3000 database.

BCH	(n,k,t)	(255,63,30)	(255,55,31)	(255,47,42)	(255,45,43)	(255,37,45)
	FRR (%)	9.51	8.37	2.76	**2.43**	1.82
UQUT	FAR (%)	0	0	0	**0**	0
	FRR (%)	18.4	18.2	8.67	**8.52**	7.58
UQCT	FAR (%)	0	0	0.01	**0.01**	0.02
BCH	(n,k,t)	(255,139,15)	(255,123,19)	(255,91,25)	(255,55,31)	(255,37,45)
	FRR (%)	14.10	8.23	3.31	1.63	0.24
CQUT	FAR (%)	2.624	6.87	18.98	37.12	78.64
BCH	(n,k,t)	(255,215,5)	(255,179,10)	(255,139,15)	(255,123,19)	(255,91,25)
	FRR (%)	80.6	56.3	42.7	34.8	10.9
CQCT	FAR (%)	5.72	11.6	16.9	22.8	30.5

ogy and user-specific thresholding technology are both employed in the biometric cryptosystem.

Based on the above experiments and analysis, it can be concluded that the user-specific question technology plays a more important role in improving the classification ability of the binary feature, and the user-specific thresholding technology contributes more in lowering the crossover probability of the features and making 1's numbers of the features well-distributed.

5.3. Performance comparison of biometric cryptosystems constructed by different ECCs

In this section, we will conduct intensive experiments to test the performances of the biometric cryptosystems constructed by the methods described in Section 4, and compare them according to the results. Several ECC coding strategies described previously are adopted, including BCH code, concatenated codes of RS code and BCH code, and LDPC code. In the performance test experiments, FX3000 database, as well as two public-domain databases, DB1 and DB2, are employed. The main indicator used here is False Reject Rate (FRR) and False Accept Rate. But note that usually the measure of FRR (when FAR = 0), i.e. ZeroFAR, is used to assess the performance of a biometric cryptosystem. In fact, the main purpose of this section is to find a relatively optimal coding scheme which can satisfy the error correction need of the proposed binary feature extraction method. Taking Fig. 6(b) for instance, the normalized hamming distance, where the EER line locates, is around 0.38. That is to say, the optimal ECC is one EEC of code length $n = 255$ and error correction capability $c \approx 0.38$. Compounded by the security consideration, i.e., the code rate r of the ECC should not be too small, so it is a difficult task to find such an optimal ECC. For those ECCs working on BSC, for example BCH code, the error correction capability depends on the length of information bits. Therefore the resultant performances after error correcting are fixed, if given binary feature vectors. But for those on Gaussian channel, for example LDPC code, the error correction capability is not only determined by the information bit length, but also by the distribution of errors in the vector. For a certain amount of errors, whether an LDPC can decode them successfully is a probability problem. This can be seen in Table 1.

5.3.1. Results on FX3000 database

Tables 3–5 detail the FAR and FRR results of the biometric cryptosystems constructed by the four kinds of ECCs mentioned before on FX3000 database, respectively. In each table, four decoding hypothesis, UQUT, UQCT, CQUT and CQCT, are considered and compared. It is obvious that the performances under UQUT hypothesis are the best, and the ones under UQCT the second best. With the increase of the length of the message bits of ECCs, FAR decreases and FRR increases. However, in all the cases under UQUT and most cases under UQCT, FAR remains 0. The FRRs under CQUT and CQCT are much larger than UQUT and UQCT. That is because the hamming distances of imposter matches are relatively small, according to Fig. 6(f) and Fig. 6(h). Like what we expects, the experimental results under UQUT perform best among all the cases. It is can be explained by that both the proposed user-specific question technology and user-specific thresholding technology account for the outstanding performance. Moreover, LDPC codes perform best among the three coding strategies. The best result under UQUT hypothesis is obtained by LDPC (255,45) and achieved Zero-FAR = 0.9%. Although the image quality of FX3000 is indeed good, it is still an excellent result, whether for traditional fingerprint recognition algorithm or biometric cryptosystems of fingerprint. This can also be validated in the experiments conducted on DB1 and DB2, which are two public domain databases.

5.3.2. Results on DB1 and DB2

Based on the results on FX3000 database, we only consider the UQUT and UQCT hypothesis in the experiments conducted on DB1

Table 4
Experimental results of biometric cryptosystems by concatenated code of RS code and BCH code on FX3000 database.

BCH	(n_1,k_1,t)	(15,7,2)	(15,5,3)
RS	(n_2,k_2)	(17,11)	(17,11)
	FRR (%)	13.0	**2.94**
UQUT	FAR (%)	0	**0**
	FRR (%)	22.5	**9.37**
UQCT	FAR (%)	0	**0**
	FRR (%)	2.96	0.317
CQUT	FAR (%)	10.38	48.36
	FRR (%)	43.7	31.6
CQCT	FAR (%)	21.2	20.8

Table 5
Experimental results of biometric cryptosystems by LDPC code on FX3000 database.

LDPC	(n,k)	(255,75)	(255,70)	(255,65)	(255,55)	(255,50)	(255,45)
	FRR (%)	4.27	3.35	2.57	1.69	1.20	**0.90**
UQUT	FAR (%)	0	0	0	0	0	**0**
	FRR (%)	11.4	9.72	8.31	6.41	5.40	**4.50**
UQCT	FAR (%)	0	0	0	0	0	**0**
LDPC	(n,k)	(255,159)	(255,151)	(255,143)	(255,135)	(255,119)	(255,103)
	FRR (%)	1.63	2.08	2.94	4.09	8.23	12.9
CQUT	FAR (%)	18.93	11.45	8.47	3.62	0.44	0.23
	FRR (%)	5.68	7.36	8.06	10.5	21.28	34.21
CQCT	FAR (%)	35.23	28.31	20.54	14.23	8.26	6.27

Table 6
Experimental results of biometric cryptosystems by BCH code on DB1 and DB2.

	BCH	(n,k,t)	$(255,63,30)$	$(255,55,31)$	$(255,47,42)$	$(255,45,43)$	$(255,37,45)$
		FRR (%)	37.1	35.6	20.0	**18.6**	16.7
DB1	UQUT	FAR (%)	0	0	0	**0**	0
		FRR (%)	49.2	47.7	35.3	34.1	33.2
DB1	UQCT	FAR (%)	3.32	3.67	9.44	10.19	11.59
		FRR (%)	22.0	20.5	8.79	**8.03**	6.82
DB2	UQUT	FAR (%)	0	0	0	**0**	0
		FRR (%)	35.0	33.6	21.5	20.5	19.2
DB2	UQCT	FAR (%)	0.37	0.53	3.27	3.79	4.60

and DB2. The The optimal feature lengths for DB1 and DB2 are 230 and 220, respectively. And the corresponding EER values on DB1 and DB2 under UQUT hypothesis are 1.08% and 0.54%. And the crossover probability values of these two databases are 0.202 and 0.156, both of which are larger than FX3000 database. It is because that the fingerprint quality in DB1 and DB2 is worse than FX3000. Tables 6–8 give the performances of the biometric cryptosystems constructed by BCH code, concatenated code of RS code and BCH code, and LDPC, respectively, on DB1 and DB2. For the convenience of experiments and analysis, we adopt the same ECCs as in the experiments on FX3000 database. However, the ECCs for FX3000 database are designed for the codewords of length 255, which is longer than the optimal feature lengths of DB1 and DB2. So we need to perform zero padding to make a 255-bit codeword both in the encoding and decoding phases.

The results on DB1 and DB2 are accordance with the ones on FX3000. The UQUT case performs better than the UQCT case, for all three coding strategies. And LDPC code performs the best, BCH code the second and the concatenated code of RS code and BCH code the last. The best ZeroFARs obtained on DB1 and DB2 are 4.85% and 10.3%, respectively, both under UQUT hypothesis and by LDPC code. These results are promising in the field of biometric cryptosystem.

5.4. Security analysis

We will analyze the security strength of the proposed biometric cryptosystem in this subsection. Here we assume that the attacker

Table 7
Experimental results of biometric cryptosystems by concatenated code of RS code and BCH code on DB1 and DB2.

	BCH	(n_1,k_1,t)	$(15,7,2)$	$(15,5,3)$
	RS	(n_2,k_2)	$(17,11)$	$(17,11)$
		FRR (%)	45.0	**23.5**
DB1	UQUT	FAR (%)	0	**0**
		FRR (%)	54.1	37.4
DB1	UQCT	FAR (%)	2.752	9.358
		FRR (%)	30.9	**12.3**
DB2	UQUT	FAR (%)	0	**0**
		FRR (%)	43.6	24.7
DB2	UQCT	FAR (%)	0.05	2.10

can obtain all the personal information stored in the template of the legal user, i.e., the user-specific questions, the user-specific threshold values, the XORed binary vector and the hash value of the random codeword, as well as the dimension reduction matrix.

It is impossible for the attacker to guess the original fingerprint minutiae information from the stored XORed template. Even if from the original binary feature vector, such guessing task is not feasible at all either, because the proposed feature generation process is irreversible. Therefore, the attack through the normal input of the system, i.e., inputting guessed minutiae template, can be thought infeasible.

The masquerade attack which would happen inside the system should be considered primarily. According to the flowchart shown in Fig. 4, the most possible attack could happen in the points of b' and c'. The attack on b' means to find a feature vector b_g, subjected to the hamming distance between it and the template feature vector b within the error correction capability t of the ECC. Before computing the attack strength on the point b', we must calculate the entropy of the binary feature. We adopt the method used in Daugman (2003) to simulate a fractional binomial distribution employing the imposter normalized hamming distances. Then the mean value p and variation σ^2 are computed according to the fractional distribution. The entropy N of the binary feature can be computed by $N = p(1 - p)/\sigma^2$. For instance, experimentally the entropy of the binary feature of length 255 from FX3000 database is computed to be 188 bits, correspondingly the entropy of the binary feature from DB1 and DB2 of the optimal length is 96 bits and 128 bits respectively.

For a biometric cryptosystem constructed by the proposed binary feature and $ECC(n,k,t)$, according to the sphere-packing bound, the strength of the brute force attack on this system can be computed as:

$$s = \frac{2^N}{\sum_{i=0}^{t}\binom{N}{i}} \simeq \frac{2^N}{\binom{N}{t}}, \tag{7}$$

where N denotes the entropy of the binary feature and t the correction capability of the ECC.

In addition, the attack on c' means to find such a codeword that its hash value equals the stored one $h(c)$. Therefore the brute force

Table 8
Experimental results of biometric cryptosystems by LDPC code on DB1 and DB2.

	LDPC	(n,k)	$(255,75)$	$(255,70)$	$(255,65)$	$(255,55)$	$(255,50)$	$(255,45)$
		FRR (%)	24.5	22.3	20.6	15.0	13.6	**10.3**
DB1	UQUT	FAR (%)	0	0	0	0	0	**0**
		FRR (%)	39.4	38.3	35.3	30.8	30.6	28.3
DB1	UQCT	FAR (%)	7.76	8.74	11.0	14.1	15.3	17.0
		FRR (%)	13.0	11.7	9.24	6.52	**4.85**	4.39
DB2	UQUT	FAR (%)	0	0	0	0	**0**	0.02
		FRR (%)	25.3	23.2	22.3	17.6	15.6	15.0
DB2	UQCT	FAR (%)	1.62	2.59	3.85	5.56	7.86	9.32

Table 9
Summary of performances and security strength values of different databases equipped with different coding strategies.

	FX3000			DB1			DB2		
	BCH	Conc. codes	LDPC	BCH	Conc.codes	LDPC	BCH	Conc. codes	LDPC
ZeroFAR (%)	2.43	2.94	0.90	18.6	23.5	10.3	8.03	12.3	4.85
Security (bits)	45	55	45	39	55	39	45	55	48

Table 10
Comparison between the proposed biometric cryptosystem and the state-of-the-art.

	Modality	Database type	Key length (bits)	Security (bits)	FRR (%)	FAR (%)
Hao et al. (2006)	iris	in-house	140	44	0.47	0
Maiorana (2010)	signature	public domain	29	21	6.95	6.95
Feng et al. (2010)	face	public domain	–	–	3.34	3.34
Bringer et al. (2008)	fingerprint	FVC2000	42	–	2.73	5.53
Nandakumar et al. (2007)	fingerprint	FVC02 DB2 Sample 1 and 2	$16(n+1)$	33	14	0
Nagar et al. (2008)	fingerprint	FVC02 DB2 Sample 1 and 2	$16(n+1)$	47	7	0
Li et al. (2010)	fingerprint	FVC02 DB2 Sample 1 and 2	$32(n+1)$	53	7	0
Sutcu et al. (2008)	fingerprint	in-house	30	30	11	0.01
Nagar et al. (2010)	fingerprint	FVC02 DB2 Sample 1 and 2	–	–	11	0.01
Proposed method	fingerprint	FVC02 DB2	**50**	**48**	**4.85**	**0**

attack strength is 2^k. Overall, the attack could select the minimum one between $2^N / \binom{N}{t}$ and 2^k. For instance, for a biometric cryptosystem equipped with $LDPC(255,45)$, whose error correction capability can be approximately thought as 50 bit errors according to Table 1, the strength values of attacks on b' and c' are 2^{72} and 2^{45}, respectively. So the system security strength is measured by the minimum one 2^{45}, i.e., 45 bits.

Particularly, for the concatenated codes of $BCH(n_1, k_1, t)$ and $RS(n_2, k_2)$, the length of information bits is $k_1 \times k_2$. The concatenated codes can correct for $(n_2 - k_2)/2$ block errors and up to t errors in the other blocks. Thus the error correction capability is about $t(n_2 + k_2)/2 + n_1(n_2 - k_2)/2$, but the errors must be subjected to some certain distribution, which is suitable to be corrected by the concatenated codes. We can see that the experimental results of concatenated codes are inferior to the ones of BCH codes and LDPC codes. Although the concatenated codes have strong error correction capability, they do not adapt to the error patterns of the proposed binary feature generation method.

5.5. Comparison with other biometric cryptosystems

Here we first summarize the performance and security strength of the proposed biometric cryptosystems equipped with different coding strategies, just as detailed in Table 9. We can see from that both the performance and security strength values achieved by the proposed cryptosystem can satisfy the current security mechanism. Table 10 compares the performance and security strength of the proposed biometric cryptosystems with the state-of-the-art. Our proposed biometric cryptosystem outperforms others in terms of ZeroFAR and security strength, except Hao et al. (Hao et al., 2006).

6. Conclusion

Information security receives great challenges in modern society and becomes more and more important. Both cryptographic authentication method and biometrics-based identification have their shortcomings, yet biometric cryptosystem, which combines biometrics and cryptography, may provide another effective method to protect people's sensitive information. In this field, fuzzy commitment scheme is a pioneer and effectively theory in the hamming space, therefore it calls for binary and length-fixed input. Unfortunately, as the most wide used biometric trait, fingerprint is not suitable to extract binary length-fixed feature. The most representative feature, minutiae, is a kind of of set feature. And moreover, for the minutiae as the basic feature, the alignment in the encrypted domain is also an unavoidable and difficult task. This paper proposes a new method to effectively transform the minutiae set to the binary length-fixed feature vectors in an alignment-free manner. The proposed user-specific question technology and user-specific thresholding technology make the resultant binary feature more random and applicable to the binary symmetric channel (BSC). The experimental results verifies this point. Afterwards, the binary feature is used to construct biometric cryptosystem based on FCS, combining three kinds of ECCs, BCH code, concatenated codes of BCH code and Reed–Solomon code, and LDPC code. It is worth note that the LDPC code we employ is specially designed Quasi Cyclic LDPC code (QC-LDPC) based on circulant permutation matrices. We conduct extensive experiments on three fingerprint databases, including one in-house and two public domain. The results show that the hypothesis of UQUT outperforms the others among all the four hypothesis, and LDPC code performs the best among all the three kinds of ECCs. For example, in the whole FVC2002 DB2, the proposed system achieves *ZeroFAR* = 4.85%, which is a leading performance in the biometric cryptosystem field. And security analysis indicates that the security strength of the proposed biometric cryptosystem can satisfy the need of current security circumstances.

Considering that LDPC code is more suitable to the longer codeword (e.g., 1024, 2048 and so on), the future direction is to enlarge the code length of the binary feature vectors and test the performance combining them with LDPC codes or more effective ECCs. Moreover, smarter attack methods which can explore the characteristic of the binary feature are also in the future consideration.

Program of the Chinese Academy of Sciences during the 11th Five-Year Plan Period under Grant No. INFO-115-C01-SDB4-30.

References

Bhanu, B., Tan, X., & Member, S. (2003). Fingerprint indexing based on novel features of minutiae triplets. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 25*, 616–622.

Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002). Biometric perils and patches. *Pattern Recognition, 12*, 2727–2738.

Boyen, X. (2004). Reusable cryptographic fuzzy extractors. In *ACM CCS 2004. ACM* (pp. 82–91). ACM Press.

Boyen, X., Dodis, Y., Katz, J., Ostrovsky, R., & Smith, A. (2005). Secure remote authentication using biometric data. In *EUROCRYPT* (pp. 147–163). Springer.

Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., & Zemor, G. (2008). Theoretical and practical boundaries of binary secure sketches. *IEEE Transactions on Information Forensics and Security, 3*(4), 673–683.

Buhan, I., Doumen, J., Hartel, P., & Veldhuis, R. (2007). Fuzzy extractors for continuous distributions. In *Proceedings of the 2nd ACM symposium on information, computer and communications security (ASIACCS), Singapore* (pp. 353–355). ACM.

Cappelli, R., Ferrara, M., & Maltoni, D. (2010). Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 32*, 2128–2141.

Chang, E. -C., Roy, S. (2007). Robust extraction of secret bits from minutiae. In *Proceedings of second international conference on biometrics, Seoul, South Korea* (pp. 750–759).

Chen, C., Veldhuis, R., Kevenaar, T., Akkermans, A. (2008). Biometric binary string generation with detection rate optimized bit allocation. In *IEEE computer society conference on computer vision and pattern recognition workshops, CVPRW '08* (pp. 1–7).

Chen, H., Tian, J., Yang, X., & Zhang, Y. (2006). An algorithm for distorted fingerprint matching based on local triangle feature set. *IEEE Transactions on Information Forensics and Security, 1*(2), 169–177.

Daugman, J. (2003). The importance of being random: Statistical principles of iris recognition. *Pattern Recognition 36* (2), (pp. 279–291). (URL http://www.sciencedirect.com/science/article/B6V14-458WVY9-1/2/747c0e472ee87bfb0df249fb45631ec7)

Dodis, Y., Reyzin, L., & Smith, A. (2004). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *Advances in crypology-eurocrypt* (Vol. 3027, pp. 523–540). Springer-Verlag.

Feng, Y. C., Yuen, P. C., & Jain, A. K. (2010). A hybrid approach for generating secure and discriminating face template. *IEEE Transactions on Information Forensics and Security, 5*(1), 103–117.

Fu, B., Yang, S., Li, J., & Hu, D. (2009). Multibiometric cryptosystem: Model structure and performance analysis. *IEEE Transactions on Information Forensics and Security, 4*(4), 867–882.

Hao, F., Anderson, R., & Daugman, J. (2006). Combining crypto with biometrics effectively. *IEEE Transactions on Computers, 55*(9), 1081–1088.

Ignatenko, T., & Willems, F. (2009). Biometric systems: Privacy and secrecy aspects. *IEEE Transactions on Information Forensics and Security, 4*(4), 956–973.

Jain, A. K., Flynn, P., & Ross, A. A. (2008b). *Handbook of biometrics*. Springer.

Jain, A., Hong, L., & Bolle, R. (1997). On-line fingerprint verification. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 19*, 302–314.

Jain, A., Nandakumar, K., & Nagar, A. (2008a). Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 17. Article ID 579416.

Juels, A., Sudan, M. (2002). A fuzzy vault scheme. In *IEEE international symposium on proceedings of information theory* (p. 408).

Juels, A., & Wattenberg, M. (1999). A fuzzy commitment scheme. In *Proceedings of 6th ACM conference on computer and communication security* (pp. 28–36). ACM Press.

Lee, C., Choi, J.-Y., Toh, K.-A., & Lee, S. (2007). Alignment-free cancelable fingerprint templates based on local minutiae information. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, 37*(4), 980–992.

Li, Q., Sutcu, Y., & Memon, N. (2006). Secure sketch for biometric templates. In *Asiacrypt* (pp. 99–113). Springer-Verlag.

Li, P., Yang, X., Cao, K., Tao, X., Wang, R., & Tian, J. (2010). An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *Journal of Network and Computer Applications, 33*(3), 207–220. recent Advances and Future Directions in Biometrics Personal Identification.

Maiorana, E. (2010). Biometric cryptosystem using function based on-line signature recognition. *Expert Systems with Applications, 37*(4), 3454–3461.

Moon, T. K. (2005). *Error correction coding-mathematical methods and algorithms.* Hoboken, New Jersey: John Wiley & Sons Inc.

Nagar, A., Nandakumar, K., Jain, A. (2008). Securing fingerprint template: Fuzzy vault with minutiae descriptors. In *Proceedings of 19th international conference on pattern recognition, ICPR 2008* (pp. 1–4).

Nagar, A., Rane, S., A.Vetro. (2010). Alignment and bit extraction for secure fingerprint biometrics. In *Proceedings of SPIE, electronic imaging, media forensics and security XII.*

Nandakumar, K., Jain, A., & Pankanti, S. (2007). Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security, 2*(4), 744–757.

Qiao, H., Guan, W., Dong, M., & Xiang, H. (2008). Construction of ldpc codes based on circulant permutation matrices. *Journal of Electronics and Information Technology, 30*(10), 2384–2387.

Ratha, N., Chikkerur, S., Connell, J., & Bolle, R. (2007). Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 29*(4), 561–572.

Savvides, M., Vijaya Kumar, B., & Khosla, P. (2004). *Cancelable biometric filters for face recognition, 3*, 922–925.

Sheng, W., Howells, G., Fairhurst, M., & Deravi, F. (2008). Template-free biometric-key generation by means of fuzzy genetic clustering. *IEEE Transactions on Information Forensics and Security, 3*(2), 183–191.

Soutar, C., Roverge, D., Stojanov, S.A., Gilroy, R., Kumar, B.V.K.V. (1998). Biometric encryption using image processing. In *Proceedings of SPIE-Optical Optical Security and Counterfeit Deterrence Technology. Vol. 3314* (pp. 178–188).

Sutcu, Y., Rane, S., Yedidia, J., Draper, S., Vetro, A. (2008). Feature transformation of biometric templates for secure biometric systems based on error correcting codes. In *IEEE computer society conference on computer vision and pattern recognition workshops CVPRW '08* (pp. 1–6).

Sutcu, Y., Li, Q., & Memon, N. (2007). Protecting biometric templates with sketch: Theory and practice. *IEEE Transactions on Information Forensics and Security, 2*(3), 503–512.

Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. (2004). Biometric cryptosystems: Issues and challenges. *Proceedings of the IEEE, 92*(6), 948–960.

Xu, H., Veldhuis, R., Bazen, A., Kevenaar, T., Akkermans, T., Gokberk, B., et al. (2009). Fingerprint verification using spectral minutiae representations. *IEEE Transactions on Information Forensics and Security, 4*(3), 397–409.

Zhang, L., Sun, Z., Tan, T., Hu, S. (2009). Robust biometric key extraction based on iris cryptosystem. In *Proceedings of The 3rd international conference of biometrics, ICB'09* (pp. 1060–1069).