Chapter 6
Obtaining Cryptographic Keys Using Multi-biometrics

Sanjay Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi

Abstract Multi-biometric systems have several advantages over uni-biometrics based systems, such as, better verification accuracy, larger feature space to accommodate more subjects, and higher security against spoofing. Unfortunately, as in case of uni-biometric systems, multi-biometric systems also face the problems of nonrevocability, lack of template diversity, and possibility of privacy compromise. A combination of biometrics and cryptography is a good solution to eliminate these limitations. In this chapter we present a multi-biometric cryptosystem based on the fuzzy commitment scheme, in which, a crypto-biometric key is derived from multi-biometric data. An idea (recently proposed by the authors) denoted as *FeaLingECc* (*Fea*ture *L*evel Fus*ion* through Wei*g*hted *E*rror *C*orre*c*tion) is used for the multi-biometric fusion. The *FeaLingECc* allows fusion of different biometric modalities having different performances (e.g., face + iris). This scheme is adapted for a multi-unit system based on two-irises and a multi-modal system using a combination of iris and face. The difficulty in obtaining the crypto-biometric key locked in the system (and in turn the reference biometric data) is 189 bits for the two-iris system while 183 bits for the iris-face system using brute force attack. In addition to strong keys, these systems possess revocability and template diversity and protect user privacy.

6.1 Introduction

An important development in the field of biometrics is to combine information from multiple biometric sources (i.e., cues). A system that consolidates the evidence pre-

S. Kanade · D. Petrovska-Delacrétaz (✉) · B. Dorizzi
TELECOM SudParis, CNRS SAMOVAR UMR 5157, Départment Electronique et Physique,
MINES TELECOM, 9 Rue Charles Fourier, 91011 Evry, France
e-mail: Dijana.Petrovska@telecom-sudparis.eu

S. Kanade
e-mail: Sanjay.Kanade@telecom-sudparis.eu

B. Dorizzi
e-mail: Bernadette.Dorizzi@telecom-sudparis.eu

P. Campisi (ed.), *Security and Privacy in Biometrics*,
DOI 10.1007/978-1-4471-5230-9_6, © Springer-Verlag London 2013

sented by multiple biometric cues is known as a multi-biometric system. Such systems offer several advantages over uni-biometric systems, some of which are discussed below.

- Multi-biometric systems can substantially improve the matching accuracy of the system.
- Having multiple information sources increases the size of the feature space available to individual users, thus making it possible to accommodate more individuals in a system.
- Multi-biometrics may address the problem of nonuniversality, e.g., in a speaker recognition system, the individuals who cannot speak cannot be enrolled. But inclusion of another biometric such as iris may enable that person to enroll.
- When multiple biometric traits are involved, it becomes more difficult for an impostor to spoof the system.

However, the main disadvantage of multi-biometric systems is their increased complexity.

Depending on the sources of information combined in it, the multi-biometric system can be called multi-sensor, multi-sample, multi-algorithm, multi-unit (or multi-instance), and multi-modal. The information fusion can be carried out at different levels of the biometric system, such as sensor, feature, score, decision, or rank level [30].

Unfortunately, despite all these advantages over uni-biometric systems, their limitations such as nonrevocability, lack of template diversity, and possibility of privacy compromise are also inherited by the multi-biometric systems. In recent years, a lot of efforts have been made to overcome these issues in uni-biometric systems by using various template protection mechanisms. Some of these mechanisms transform the biometric data in a non-recoverable manner so that the comparison is carried out in the transformed domain. In some other schemes, a stable key is obtained from biometric data and such systems are denoted as biometric cryptosystems [10]. However, the main aim of the biometric cryptosystems is to obtain a key for cryptographic purposes and many of these systems do not possess the property of revocability.

Despite these efforts in case of uni-biometrics, there are very few works in literature that deal with these issues in multi-biometric systems. Multi-biometrics-based cryptosystems, which obtain cryptographic keys using multi-biometrics are a promising solution to this problem. In this chapter, first a review of such multi-biometric cryptosystems is presented. The review is followed by a detailed description of the multi-biometric key regeneration schemes recently proposed by the authors.

This chapter is organized as follows: the state of the art related to multi-biometric cryptosystems is discussed in Sect. 6.2. A generic scheme for multi-biometric template protection based on the fuzzy commitment scheme [12] is described in Sect. 6.3. This is in fact a multi-biometrics-based key regeneration scheme which also provides template protection. Two adaptations of this scheme, a multi-unit type system using two irises and a multi-modal type system using iris and face, along with their experimental evaluation, are then described in Sects. 6.4 and 6.5, respectively. These two systems were recently published in [15] and [16], respectively. Finally, conclusions and perspectives are given in Sect. 6.6.

6.2 Obtaining Cryptographic Keys Using Multi-biometrics: State of the Art

The key regeneration systems described in this chapter combine techniques from biometrics and cryptography. In literature, such systems are generally denoted *biometric template protection schemes* and are classified into two main categories [10]: feature transformation and biometric cryptosystems. In feature transformation type systems, a user specific transformation is applied on the biometric features [14, 20, 29]. The goal of the systems in this category is to induce revocability, template diversity, and privacy protection into biometric systems. The comparison between two biometric samples is carried out in the transformed domain using some distance metric similar to the classical biometric systems. Therefore, using multi-biometrics in these kind of systems is straightforward. Classical fusion techniques, such as feature level and score level fusion, can be applied directly to these systems.

On the other hand, the main aim of the systems from the biometric cryptosystems category is to obtain a stable multi-bit string from biometrics [9, 11, 12]. Such crypto-bio keys are strongly linked to the user's identity and therefore can enhance the security of the system. In fact, many systems in this category were originally designed for obtaining cryptographic keys and did not possess revocability. However, if properly designed, revocability, template diversity, and privacy protection properties can be induced in these systems.

For example, the fuzzy commitment-based key regeneration system [12], which is the most widely studied approach for template protection (and key generation), treats biometric data matching as an error correction issue by considering it as a problem of data transmission through a noisy communication channel. First, a randomly generated key $\mathbf{K}$ is encoded using Error Correcting Codes (ECC) and the variations in the biometric data are transferred onto the encoded key. These variations, treated as errors, are corrected by the ECC to regenerate the random key $\mathbf{K}'$ at the verification step. This system does not store the biometric features or templates as in classical biometric systems. The biometric features are stored in a protected form in the crypto-biometric template. Since there is no stored biometric template, nor are there features, classical biometric comparison cannot be performed in this system and no match score can be obtained. In fact, such systems directly output the regenerated key. The user verification success or failure decision, unlike classical biometric systems, depends on the exact comparison between the crypto-bio keys obtained with the system. Since there is no score, score level fusion cannot be applied for multi-biometric information fusion in key regeneration systems.

The decision level fusion is possible in these systems, but the increase in the key entropy can be a maximum of one bit. The key entropy indicates the difficulty in obtaining the key without having the genuine biometric data which is, in turn, the security of the stored template. In decision level fusion, depending on the verification results of two individual biometric systems, a combined key can be released. If the length and entropy of each of these keys is N and H bits, respectively, the combined key will have a length equal to $2N$ bits but the entropy will increase by only one bit to $H + 1$. The reason behind this is the entropy is measured on logarithmic scale. If an attacker needs 2^H attempts to guess the key, then the entropy is H bits. When two such keys are present, the number of attempts increases to 2×2^H resulting in an entropy of $H + 1$ bits. Thus, the entropy increase in such a case is only one bit.

Therefore, if multi-biometric techniques are to be used for template protection, specific methods for information fusion need to be developed. There are very few systems found in literature that address the issue of multi-biometric template protection which are summarized below.

One of the first systems to use multi-biometrics with template protection is by Sutcu et al. [32] (in 2007). They proposed a method to combine fingerprint and face features in a fuzzy sketch scheme. But they did not carry out experiments with the fused biometric information but rather predicted the results for the multi-biometric system from the two uni-biometric system results.

Nandakumar and Jain [23, 24] (in 2008) proposed a fuzzy vault scheme which combines fingerprints with iris. A significant improvement in verification performance over the uni-biometric systems is observed (e.g., from a Genuine Acceptance Rate (GAR) of 88 % and 78.8 % for individual iris and fingerprint systems, respectively, to 98.2 % for the multi-biometric system). However, despite these improvements in the verification performance, the entropy of the key increases from 40 bits (for uni-biometric system) to 49 bits (in the multi-biometric case) which is still low from a security point of view.

Cimato et al. [5] (in 2008) proposed a multi-modal biometrics-based cryptosystem. Similar to that of Nandakumar and Jain [24], the two modalities employed in their system are iris and fingerprints. Their proposed system is based on the fuzzy extractor concept [3, 7]. They experimentally showed that the performance of the multi-modal system is as good as the best performing single modality system. However, they did not provide security analysis of the system in terms of key entropy.

Kelkboom et al. [17] (in 2009) proposed various ways of combining multi-biometrics with fuzzy commitment-based schemes. Their proposed systems involve multi-algorithmic fusion at feature-, score-, and decision-level. However, their performance evaluation suggests that the improvement due to multi-biometrics occurs only in terms of verification performance. The security of the system does not improve significantly.

Fu et al. [8] (in 2009) proposed theoretical models describing multi-biometric cryptosystems. They proposed fusion at the biometric and cryptographic levels and then derived four models adopted at these two levels. However, this work is theoretical and no actual evaluation of verification performance as well as key entropy is carried out.

In this chapter, a new technique recently proposed by the authors, called *FeaLingECc* (*Fea*ture *L*evel Fus*i*o*n* throu*g*h Weighted *E*rror *C*orre*c*tion), is described. With this technique, the biometric information obtained from different cues can be combined into a fuzzy commitment-based template protection system. We explore the possibilities of using multi-biometrics in a fuzzy commitment-based scheme [12] using two different methodologies:

1. multi-unit (also called multi-instance) type system combining information from left and right irises of a person, and
2. multi-modal type system which combines information from iris and face biometrics.

For both these systems, the information fusion is carried out at feature level, which increases the key entropy. The *FeaLingECc* technique allows to apply different weights to different modalities (or different information sources). The general description of this proposed scheme is presented in the next section.

6.3 Multi-biometrics Based Key Regeneration

The basic structure of our scheme is shown in Fig. 6.1. It is based on the fuzzy commitment scheme [12]. In this scheme, the biometric data variability is treated with error correcting codes. There are two levels of error correction: Level-1, also called inner level, and Level-2, which is the outer level. A randomly generated key **K** is assigned to a user and is then encoded using Level-2 encoder. The output of the Level-2 encoder is then randomized with a shuffling key by applying the shuffling scheme proposed by Kanade et al. [13]. The shuffled output is further encoded by Level-1 encoder. The output of the encoder is called *pseudo code* θ_{ps}. The reference biometric data is XORed with this *pseudo code* to obtain the *locked code* θ_{lock}. The reference biometric data cannot be recovered from the locked code unless the pseudo code or another biometric data sample from the same user is provided.

In the proposed scheme, the biometric data is a combined data from two biometric cues. The biometric information fusion is carried out in the feature domain. The proposed system is based on the fuzzy commitment scheme and therefore requires the feature vectors in binary form. Assuming that the binary feature vector corresponding to the first biometric source is denoted as θ_1 and that to the second biometric source as θ_2, the reference feature code is obtained by concatenating these two feature vectors as, $\theta_{\text{ref}} = \theta_1 \| \theta_2$. This reference feature code θ_{ref} is XORed with the pseudo code θ_{ps} to obtain a locked code θ_{lock},

$$\theta_{\text{lock}} = \theta_{\text{ps}} \oplus \theta_{\text{ref}}. \tag{6.1}$$

This locked code along with the hash value $H(\mathbf{K})$ of the key **K** is the crypto-biometric template. The locked code is required for regeneration of the key **K**, whereas the hash value is required to check the correctness of the regenerated key.

At the time of key regeneration/verification, a multi-biometric test feature vector θ_{test} is obtained by following a procedure similar to that at the enrollment step.

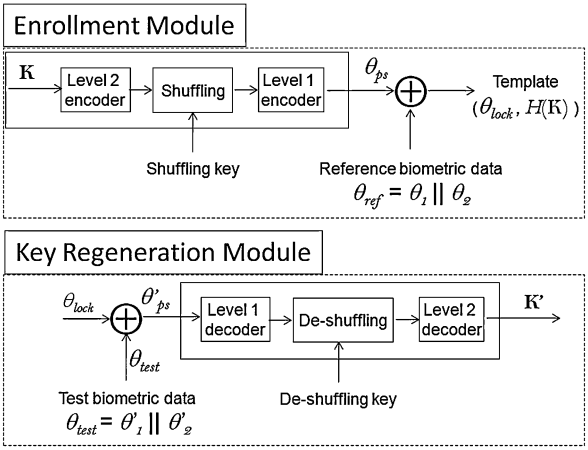


Fig. 6.1 Schematic diagram showing the structure of the proposed multi-biometrics-based cryptographic key regeneration scheme

This test feature vector is XORed with the locked code θ_{lock} to obtain a modified version θ'_{ps} of the pseudo code. This modified version consists of the pseudo code θ_{ps} contaminated with the errors e between reference and test biometric vectors. The Error Correcting Codes (ECC) decoding scheme corrects these errors and retrieves a trial value $\mathbf{K}'$ of the random key $\mathbf{K}$. A comparison between the hash values of the original and the regenerated key is carried out and a positive result indicates key regeneration success;

$$\begin{aligned}\theta'_{\text{ps}} &= \theta_{\text{lock}} \oplus \theta_{\text{test}} \\ &= \theta_{\text{ps}} \oplus \theta_{\text{ref}} \oplus \theta_{\text{test}} \\ &= \theta_{\text{ps}} \oplus e, \qquad (6.2)\\ \mathbf{K}' &= \text{ECC}^{-1}\left(\theta'_{\text{ps}}\right). \qquad (6.3)\end{aligned}$$

The Level-1 error correcting codes perform majority of the error correction. These ECC correct bit-level errors occurring in blocks. If the number of errors in a block is more than the error correction capacity of the Level-1 ECC, that block is decoded incorrectly. Such incorrectly decoded blocks are further treated by the Level-2 codes. Thus, the Level-2 ECC work on block level. In order to cope with the cascading structure of the two ECC, the number of bits in each symbol of the Level-2 ECC must be the same as (or possibly an integer multiple of) the number of bits in Level-1 ECC input block.

6.3.1 FeaLingECc *(***Fea***ture* **L***evel Fus***i***o***n** *Through Weighted* **E***rror* **C***orre***c***tion)*

When feature vectors corresponding to two biometric sources are combined, it is required that the two vectors have a common representation which is not always the case. For example, fingerprint minutiae set consists of minutiae locations and orientation information, while the iris feature vector is a binary string. The minutiae set is an unordered set while the iris code is an ordered set. Therefore, the two feature vectors must be converted into a common representation. Moreover, the dimensions of the feature vectors can also be different and simply concatenating the two feature vectors may not be beneficial. The difference in the dimensionality of the two feature vectors can cause an adverse effect on the system performance. This problem is called the curse of dimensionality [30]. Therefore, in order to deal with this problem, the feature level fusion module is generally followed by a feature selection module in classical multi-biometric systems.

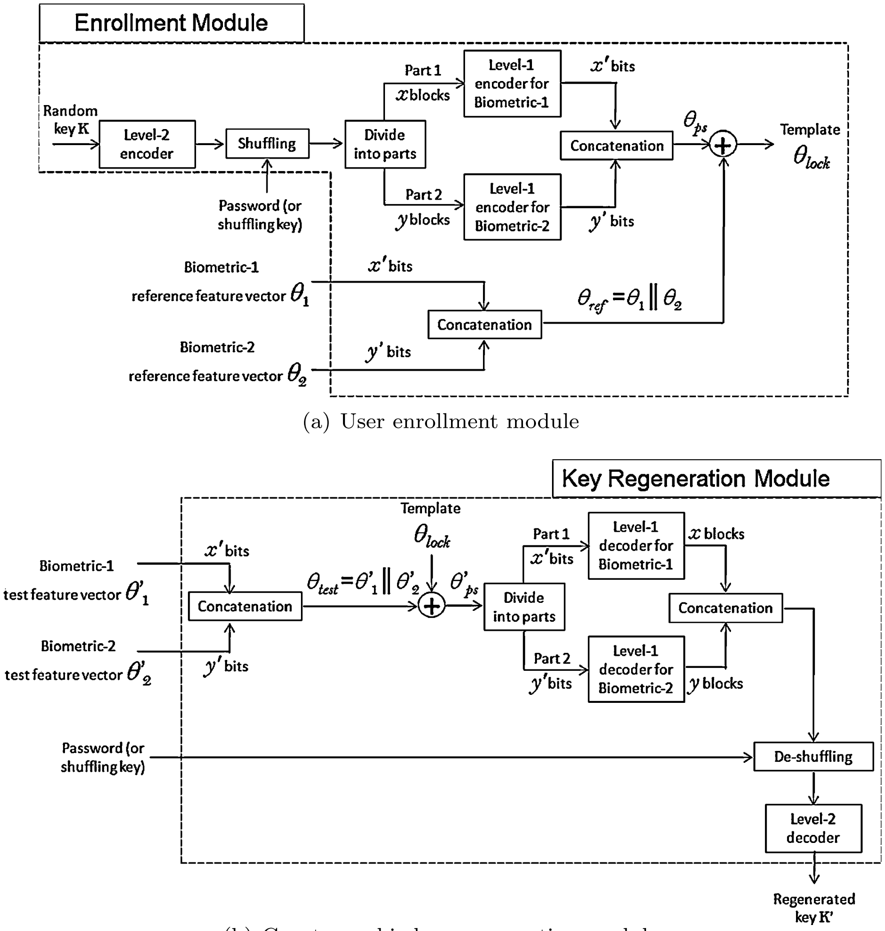
Moreover, one biometric trait may be performing better than the other in terms of verification performance (e.g., in general, iris performs better than face). This knowledge can be exploited in score level fusion systems by applying different weights to the individual biometric traits. In such systems, higher weight is given to the better performing biometric trait in the verification decision process. This kind of weighting can significantly improve the performance of multi-biometric system.

Since the match scores cannot be computed in key regeneration systems, classical score level fusion techniques cannot be used. Therefore, we propose a novel method in which the features are combined in feature domain and the error correction scheme is designed so that different weights can be applied to the individual biometric traits. This scheme also deals with the problem of curse of dimensionality. It can cope with the differences in the dimensions of individual feature vectors by carefully selecting the dimensions of the Level-1 ECC for the individual biometrics and minimize the effect of dimensions mismatch on the verification performance.

The enrollment and key regeneration modules of the proposed system are shown in Fig. 6.2(a) and 6.2(b). The error correction scheme in the proposed system consists of two levels. The Level-1 work on bit-errors occurring in blocks while the Level-2 ECC correct the block errors which are left after the Level-1 ECC action. Since the amount and nature of variations in biometric data are different for different modalities, and they also depend on the acquisition conditions, we need to select different Level-1 ECC for different modalities. The Level-1 ECC and their error correction capacity is selected by observing the Hamming distance distributions for genuine and impostor comparisons for the corresponding trait.

The application of different weights is carried out by assigning different number of blocks of the Level-2 ECC for different biometrics. As shown in Fig. 6.2(a), the output of the Level-2 codes (which is in form of n_s blocks) is split into two parts: Part-1 which consists of x blocks and Part-2 consisting of $y = (n_s - x)$ blocks. Higher weight can be applied to the Biometric-1 by having $x > y$ and vice versa.

The x blocks of Part-1 are further encoded and combined into x' bits by the Level-1 encoder for the first biometric (Biometric-1). The y blocks of Part-2 are encoded and combined into y' bits by the Level-1 encoder for the second biometric (Biometric-2). Here, x' and y' are equal to the number of effective bits in the feature vectors of Biometric-1 and Biometric-2, respectively. The number of bits in each


Enrollment Module
Random key K
Level-2 encoder
Shuffling
Password (or shuffling key)
Divide into parts
Part 1
x blocks
Part 2
y blocks
Level-1 encoder for Biometric-1
Level-1 encoder for Biometric-2
x' bits
y' bits
Concatenation
θ_{ps}
Template θ_{lock}
Biometric-1 reference feature vector θ_1
Biometric-2 reference feature vector θ_2
x' bits
y' bits
Concatenation
$\theta_{ref} = \theta_1 \| \theta_2$
Key Regeneration Module
Biometric-1 test feature vector θ'_1
Biometric-2 test feature vector θ'_2
x' bits
y' bits
Concatenation
Template θ_{lock}
$\theta_{test} = \theta'_1 \| \theta'_2$
θ'_{ps}
Divide into parts
Part 1
x' bits
Part 2
y' bits
Level-1 decoder for Biometric-1
Level-1 decoder for Biometric-2
x blocks
y blocks
Concatenation
Password (or shuffling key)
De-shuffling
Level-2 decoder
Regenerated key K'

(a) User enrollment module

(b) Cryptographic key regeneration module

Fig. 6.2 Schematic diagram of the proposed multi-biometrics-based cryptographic key regeneration scheme using *FeaLingECc* (*Fea*ture *L*evel Fus*i*on through Wei*g*hted *E*rror *C*orre*c*tion)

input block of the Level-1 encoder should be equal to the number of bits in each output block of the Level-2 encoder. Alternatively, the input block size of the Level-1 encoder can be an integer multiple of the output block size of the Level-2 encoder. Concatenation of the outputs of the two Level-1 encoders yields the pseudo code θ_{ps}. This pseudo code is XORed with the multi-biometric reference feature vector θ_{ref} (which is obtained by concatenation of two individual feature vectors θ_1 and θ_2) to obtain the locked code θ_{lock}.

The weights are applied by changing the sizes of Part-1 and Part-2. In order to understand the concept, let us take a closer look into the error correction mechanism that takes place during the key regeneration step (see Fig. 6.3). When a multi-biometric test feature vector θ_{test} (which is obtained by concatenation of

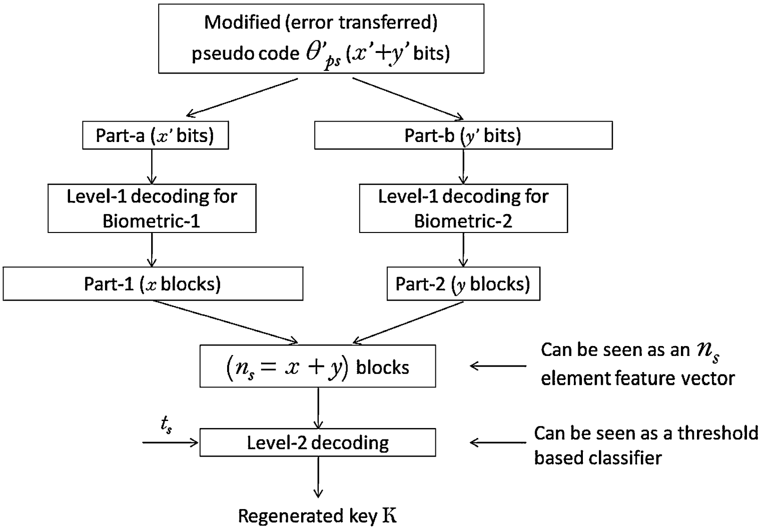

Modified (error transferred) pseudo code θ'_{ps} (x'+y' bits)
Part-a (x' bits)
Part-b (y' bits)
Level-1 decoding for Biometric-1
Level-1 decoding for Biometric-2
Part-1 (x blocks)
Part-2 (y blocks)
($n_s = x + y$) blocks
Can be seen as an n_s element feature vector
t_s
Level-2 decoding
Can be seen as a threshold based classifier
Regenerated key K

Fig. 6.3 Schematic diagram showing the proposed weighted error correction process. Note that *Part-b* is bigger than *Part-a*. When *Level-1* ECC are applied, this relationship changes. *Part-1* becomes bigger than *Part-2* which means that higher weight is applied to the *Biometric-1* than *Biometric-2*

two individual test feature vectors θ'_1 and θ'_2) is XORed with the locked code θ_{lock}, the errors between the reference and test feature codes are transferred onto the pseudo code θ_{ps}. Figure 6.3 shows the process of error correction that follows.

The modified (error transferred) pseudo code θ'_{ps} is divided into two parts: Part-a consists of the first x' bits while the Part-b consists of the remaining y' bits. The Level-1 decoder corresponding to Biometric-1 is applied on the x' bits to correct the bit errors caused by the Biometric-1. This process yields x blocks. Similarly, y blocks are obtained from the y' bits corresponding to the Biometric-2. These two parts are concatenated to form a single codeword which contains $n_s = (x + y)$ blocks. The Level-2 decoder corrects the erroneous blocks present in this codeword to obtain a trial value $\mathbf{K}'$ of the random key $\mathbf{K}$. The Level-2 decoder can correct up to t_s erroneous blocks where t_s is its error correction capacity. This Level-2 decoder can be seen as a threshold-based classifier which operates on an n_s element vector where t_s acts as a threshold. If the number of erroneous blocks are less than or equal to t_s, the key is successfully generated and the verification result is positive. Therefore, if we set $x > y$, a higher weight will be given to Biometric-1 than Biometric-2 in the decision process. The condition $x > y$ (or $x < y$ if required) is achieved by properly selecting the dimensions of the Level-1 ECC. However, this selection needs to take care of the error correction capacity which depends on the Hamming distance distribution of the biometric data.

6.3.2 Adding Revocability

The problem with biometrics is that it lacks the property of revocability and can compromise user's privacy. In order to overcome these drawbacks, some one-way transformations [20, 22, 29] are applied on the biometric data in case of uni-biometric systems. In a similar way, some cancelable mechanism should be used in the multi-biometrics-based system. One simple option is to apply the transformation on the two individual biometric feature vectors. In this way, revocability and privacy protection can be added to the multi-biometrics-based system.

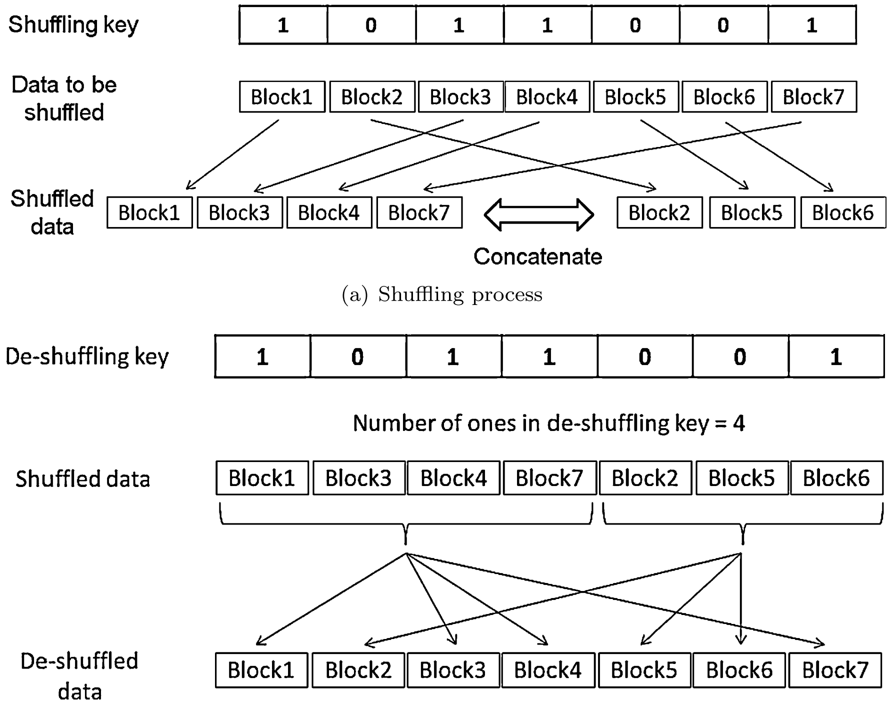
But there is a loophole in this design. This loophole appears if the Level-2 error correcting codes used in the system (e.g., we use Reed–Solomon codes as Level-2 codes in our proposal) are of systematic nature. An error correcting code is said to be systematic in nature if the input to the code is present in its original form in the output. The output of such codes comprises the input data appended by the parity symbols, and thus, the locations of the original data and the parity symbols is known to an attacker. In this case, the attacker can attack the biometric information corresponding only to the data blocks.

For example, consider the case of Table 6.7, where $t_s = 8$. In this particular example, $n_s = 46$ which is the total number of blocks after Reed–Salomon (RS) encoding which are obtained by appending 16 parity blocks to the 30-block input data blocks ($n_s = k_s + 2t_s$). This encoded output is further encoded with the Level-1 encoders. The first 31 blocks of this output correspond to Biometric-1 and the remaining to Biometric-2. Therefore, an attacker can choose to attack only biometric-1 and obtain the 31 blocks, out of which the first 30 blocks constitute the actual key.

Clearly, this kind of attack can suppress the advantage gained by using multiple biometrics. The attacker may need only one set of biometric information to crack the multi-biometric system.

In order to overcome this drawback, we propose to apply the biometric data transformation mechanism (shuffling scheme in our case) after the Level-2 encoding instead of applying it on the biometric data. In this case, even if the Level-2 ECC are systematic, the shuffling process breaks the systematic nature of its output. The shuffled output of Level-2 ECC is further encoded with the Level-1 ECC. At the time of key regeneration, the original order of the Level-2 encoder output must be restored in order for the Level-2 decoder to function correctly. This is done by applying the de-shuffling process. For better understanding, the shuffling and de-shuffling processes are shown together in Fig. 6.4.

One might argue that revocability can be induced into the system by applying classical encryption on the fuzzy commitment (protected template), which is true in principle. However, this type of encryption of templates does not eliminate the security loophole cited above that occurs due to the systematic nature of the ECC. In this case, an attacker needs to decrypt the template and then crack only one biometric source in order to obtain the crypto-biometric key. By employing the shuffling scheme in the above mentioned manner, the attacker needs to crack the shuffling key and both the biometric sources.


Shuffling key
1 0 1 1 0 0 1
Data to be shuffled
Block1 Block2 Block3 Block4 Block5 Block6 Block7
Shuffled data
Block1 Block3 Block4 Block7
Block2 Block5 Block6
Concatenate
De-shuffling key
1 0 1 1 0 0 1
Number of ones in de-shuffling key = 4
Shuffled data
Block1 Block3 Block4 Block7 Block2 Block5 Block6
De-shuffled data
Block1 Block2 Block3 Block4 Block5 Block6 Block7

(a) Shuffling process

(b) De-shuffling process

Fig. 6.4 A schematic diagram showing the shuffling and de-shuffling process. Note that the shuffling and de-shuffling key must be the same to recover the correct data

The generic multi-biometrics-based key regeneration scheme described in this section can be applied to a combination of two sets of biometric information. The pre-requisite for this system is that both the biometric data must be in form of binary vectors. We developed two systems based on this scheme:

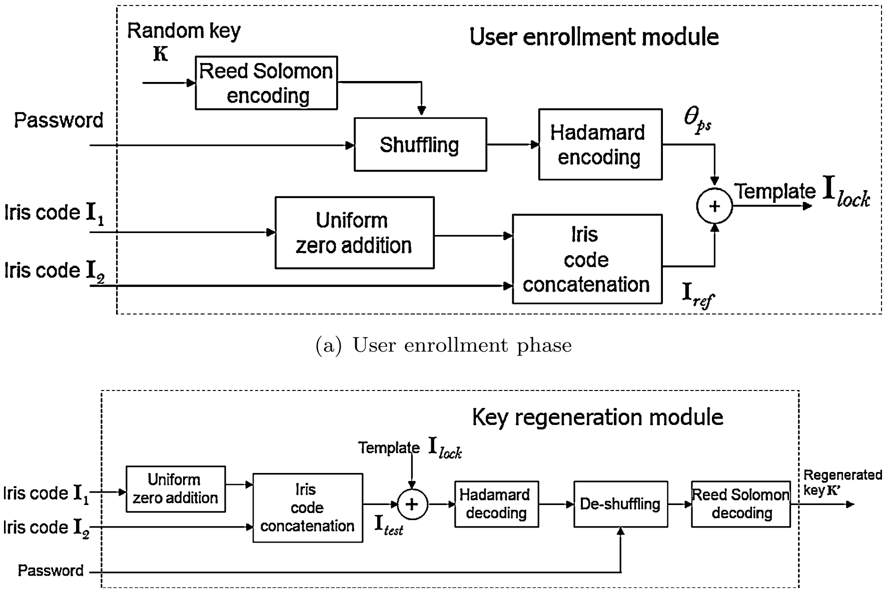
- multi-unit type system that combines information from the left and the right irises of a person, and
- multi-modal type system that combines information from an iris with that from the face.

These systems are described in subsequent sections.

6.4 Multi-unit Type Multi-biometrics Based Key Regeneration

6.4.1 Algorithm for Multi-unit Biometrics Based Key Regeneration

We developed a multi-unit type multi-biometrics system to obtain cryptographic keys. Feature level fusion in multi-unit type systems is comparatively less com-



(a) User enrollment phase

(b) Key regeneration phase

Fig. 6.5 Schematic diagram of the proposed multi-unit type multi-biometrics-based cryptographic key regeneration scheme using feature level fusion, weighted error correction, and password—(**a**) User enrollment phase; (**b**) cryptographic key regeneration phase

plicated than in the multi-modal type systems. The reason is that the feature sets obtained from different sources in a multi-unit system are generally similar in nature and dimensions. Our system incorporates information from left and right irises of a person in a fuzzy commitment-based key regeneration scheme. The information fusion is carried out in feature domain using the weighted error correction approach described in previous section.

The iris codes obtained from different iris images of the same user contain variabilities which are treated as errors. As pointed out by Hao et al. [9], there are two types of errors in iris codes: (1) background errors caused by the camera noise, image capture effects, etc., and (2) burst errors which are a result of specular reflections, occlusions, etc. Both these types of errors are corrected using the two level error correction scheme shown in Fig. 6.1.

The enrollment and key regeneration phases of the proposed multi-unit type system are shown in Fig. 6.5. We used Hadamard codes as Level-1 ECC and Reed–Solomon (RS) codes as Level-2 ECC for our two-iris-based system. A random bit string **K** is generated and assigned to a user and is then encoded using Reed–Solomon (RS) codes, the output of which is further encoded by the Hadamard codes. The Hadamard codes correct the background errors and RS codes correct burst errors. Details about these ECC can be found in [21]. The output of the encoder is called *pseudo code* θ_{ps}. In order to cope with the cascading structure of the two ECC, the number of bits in each symbol of RS and that in the input words of

Hadamard codes is set to be equal ($m = 7$). Iris codes $\mathbf{I}_1$ and $\mathbf{I}_2$ from the right and left iris images, respectively, are concatenated to form a reference (multi-) iris code $\mathbf{I}_{\text{ref}}$. This $\mathbf{I}_{\text{ref}}$ is XORed with θ_{ps} to obtain the locked iris code template $\mathbf{I}_{\text{lock}}$.

In the key regeneration phase, a test (multi-) iris code $\mathbf{I}_{\text{test}}$ is obtained similarly and XORed with $\mathbf{I}_{\text{lock}}$. These XORing operations transfer the errors in the iris codes onto the pseudo code. The Hadamard codes can correct (up to) $2^{(k-2)} - 1$ errors in a 2^k-bit block. If a block has more than $2^{(k-2)} - 1$ errors, that block is not decoded correctly and results in an error. The second level of ECC consists of the RS codes. The output of the Hadamard decoding stage acts as the input to the RS decoder stage. The RS codes correct the errors caused due to the wrong decoding by the Hadamard codes and generate the key $\mathbf{K}'$. If the total amount of errors is within the error correction capacity of the ECC, the errors are corrected and a key $\mathbf{K}'$ is regenerated which is the same as $\mathbf{K}$. If the amount of errors is more than the error correction capacity of the ECC, $\mathbf{K}' \neq \mathbf{K}$.

In the proposed scheme, we apply higher weights to one iris than the other by employing the weighted error correction method described in Sect. 6.3.1. We use a bigger number of RS blocks for one iris than for the other to apply these weights. Kanade et al. [13] have shown that inserting certain amount of zeros in the biometric data can increase the error correction capacity of the Hadamard codes. Using this property, we applied the zero insertion scheme to one iris code in order to increase the error correction for it. Using the Hadamard codes without zero insertion scheme results in high false rejections but zero false acceptances. Thus, the increased error correction for the first iris code helps to increase acceptances while the low error correction for the second iris code increases rejections. The combined effect of the two is the improvement in the verification performance of the key regeneration system. The most important advantage of this scheme is that the feature vector is longer than in uni-biometrics-based system, and therefore, we can obtain longer keys. The biometric information is also larger compared to the uni-biometric systems resulting in higher entropy. Additionally, it experimentally validates our proposal of weighted error correction. The experimental results of this system are reported in the next subsection.

6.4.2 Results and Security Analysis of the Multi-unit (Two-Iris) Type System

In this section, we briefly describe the experimental setup, and then present the results and security analysis of the proposed multi-unit type system.

6.4.2.1 Experimental Setup

We used the OSIRISv1 (Open Source for Iris Recognition) system described in [28] and available online at [27] to extract a 1,188-bit binary string called iris code from

Table 6.1 Baseline biometric system's verification performance in terms of EER in %. Single as well as two-iris tests. Results previously published in [15]

CBS-BiosecureV1 (development)			NIST-ICE (evaluation)		
Left	Right	Both irises	Left	Right	Both irises
3.23	2.90	2.54	2.44	4.81	1.18

an iris image. In this system, the iris region in an image is detected, normalized, and then decomposed using Gabor filters having different scales and orientations. The phase information is then quantized to obtain the binary code. In order to cope with the iris rotations, the normalized test iris image is shifted 10 times in both directions and codes are extracted from them for comparison, leading to 21 comparisons.

The CBS database [28] is used for development to find out the ECC and error correction capacities. The system is then evaluated on the NIST-ICE database [26]. In the NIST-ICE database, there are 132 subjects out of which, only 112 subjects have recorded images of their both eyes. We select images of these 112 subjects for carrying out our tests. The right iris images are coupled with the left iris images for the multi-iris tests. The first such image pair of a person is considered for enrollment and a template is registered for that person. The genuine comparisons are carried out by comparing the remaining image pairs of that subject with the enrollment template leading to 1,099 genuine comparisons. For impostor comparisons, one image pair from each of the remaining subjects is randomly selected and these image pairs are compared with the enrollment template. Thus, for each person, we carry out 111 impostor comparisons. In summary, 1,099 genuine and 12,432 impostor comparisons are carried out on the NIST-ICE database for the two-iris experiment.

6.4.2.2 Experimental Results of the Multi-unit (Two-Iris) Type System

Since the proposed system is based on an iris recognition system, it is worthwhile to report the performance of the baseline biometric system for fair comparison. Such performance results are reported in Table 6.1. Note that the baseline iris system is based on OSIRISv1 with a re-implemented matching module. Classical multi-iris-based biometric system is also tested in which the iris codes are simply concatenated and compared. Note that, as expected, the combination of left and right irises results in reduction in the Equal Error Rate (EER).

For the cryptographic key regeneration system, we first report the results for the simple feature level fusion scheme in Table 6.2. The feature level fusion in this case is by simple concatenation of two feature vectors. For the sake of comparison, the key regeneration results (for CBS database) using single irises are also reported in the same table. The shuffling scheme is not used in any of these tests. It can be observed that the minimum FRR using single iris is 7.37 % with a key length of 6 bits. The combination of two irises reduces the FRR and also leads to longer keys such as 35-bit keys at 4.93 % FRR. In spite of the improvement, the FRR is still too high and hence we did not carry out these tests on the NIST-ICE database.

When the proposed *FeaLingECc* approach is used, a significant improvement is achieved that can be seen in Table 6.3. As is done in the uni-biometrics-based

Table 6.2 Key regeneration system results on the CBS-BiosecureV1 data set when two iris codes are combined using only feature level fusion; no weighting, no shuffling; FRR values are in %; length of key **K** is in bits; FAR is always zero for all these tests. t_s is the error correction capacity of RS codes. Results previously published in [15]

t_s	Left iris		Right iris		Both irises	
	FRR	Length (**K**)	FRR	Length (**K**)	FRR	Length (**K**)
16	9.80	30	14.13	30	4.93	35
17	8.60	18	13.10	18	4.57	21
18	**7.37**	**6**	**12.03**	**6**	**4.27**	**7**

Table 6.3 Key regeneration system results when two iris codes are combined using the proposed *FeaLingECc* method; FAR and FRR values are in %. Results previously published in [15]

t_s	Key length (in bits)	Without shuffling				With shuffling			
		CBS-Bio		NIST-ICE		CBS-Bio		NIST-ICE	
		FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
6	259	0	8.37	0	13.28	0	8.50	0	13.74
9	217	0	5.37	0	5.19	0	5.63	0	5.46
10	203	0	4.50	0.016	3.37	0	4.60	0	3.28
11	189	0	4.10	0.06	2.09	0	4.10	0	2.09
12	**175**	**0**	**3.63**	**0.38**	**1.64**	**0**	**3.67**	**0**	**1.36**
13	161	0.10	3.40	1.49	0.55	0	3.50	0	1.00
14	**147**	**0.70**	**3.30**	**2.98**	**0.27**	**0**	**3.30**	**0**	**0.18**
15	133	1.87	3.13	10.46	0.18	0	3.03	0	0.18
16	119	6.40	2.80	15.86	0.09	0	2.37	0	0.09
21	49	84.47	0.23	91.37	0	0	0.30	0	0

system, we added certain amount of zeros to the right iris code to correct higher amount of errors in it whereas no zeros are added to left iris code. The Hadamard codes operate on 64-bit blocks and there are 49 such blocks resulting in a total amount of error correction equal to 735 bits. It also allows us to obtain much longer keys with low error rates, e.g., we can have 175-bit keys at 0.38 % False Acceptance Rate (FAR) and 1.64 % FRR for the NIST-ICE database.

Finally, the results for the key regeneration scheme with shuffling are presented in Table 6.3. These results are better than any previously published results in literature, e.g., we can generate 147-bit keys at 0.18 % FRR and 0 % FAR for ICE database. In our experiments, the number of blocks at the output of the RS encoder is 49. Hence we use a 49-bit shuffling key to shuffle those blocks. The shuffling key can be protected by a password of eight characters. Note that there is not much decrease in FRR due to the use of shuffling. The main improvement is in the FAR, which becomes zero, which means that the systems become more secure by using the shuffling.

The most appropriate work to compare with the proposed system is that by Nandakumar and Jain [24]. In their system, information from iris and fingerprints is combined and they succeed to obtain keys with 49-bit entropy while the verification error rates are FAR $= 0.02$ % and FRR $= 1.80$ %. For the proposed system, at FAR $= 0$ %, FRR $= 0.18$ % and the key entropy is 147 bits. This security analysis of the proposed system in terms of entropy is presented in the next subsection.

6.4.2.3 Security Analysis of the Multi-unit (Two-Iris) Type System

Since the main aim of the system is to provide security, it is required to analyze the security of the system. The entropy of the key can give us an estimate of the difficulty which an attacker has to face to obtain the key without having the proper credentials. It also indicates the strength of the template protection mechanism because once the attacker has the key, he can inverse the stored template and obtain the reference biometric data. Though the key is generated randomly at enrollment time, a lot of redundancy is added by the ECC and hence its entropy is bound to decrease. We use the same approach as used by Hao et al. [9] to estimate the entropy. They used the sphere packing bound [21] to roughly estimate the number of brute force attempts required for an attacker to guess the key $\mathbf{K}$ correctly. Let N be the number of degrees of freedom in the data being XORed with the pseudo code θ_{ps}, and P is the fraction of this information corresponding to the error correction capacity (i.e., $P = N \times$ error correction capacity). Then the number of brute force attacks an attacker needs to carry out is estimated by Equation (6.4) as

$$\text{BF} \approx \frac{2^N}{\binom{N}{P}}. \tag{6.4}$$

The number of degrees of freedom can be estimated by the procedure given by Daugman [6]. The iris codes used in our experiments are 1,188 bits long. We estimate the degrees of freedom in the iris codes to be 561. Collectively, in two iris codes, we have 1,122 degrees of freedom. In the weighted error correction configuration in the multi-iris system, the total amount of error correction is ≈30 %. If $N = 1{,}122$ and $P = 0.3 \times N \approx 336$, applying (6.4), an impostor needs approximately

$$\text{BF} \approx \frac{2^N}{\binom{N}{P}} \approx \frac{2^{1122}}{\binom{1122}{336}} \approx 2^{140}, \tag{6.5}$$

brute force calculations to successfully get the cryptographic key. Thus the entropy of the key is 140 bits, which is much higher than any other system reported in literature.

The shuffling scheme applied in the two-iris system needs a 49-bit shuffling key. This key is randomly generated and is protected by a password. We propose to use a randomly generated 8-character password which can have 52-bit entropy [4]. The shuffling process is embedded into the error correction process and hence the individual entropies add up together resulting in a total key entropy of $140 + 49 = 189$ bits. Thus the entropy of the key is

$$\text{Entropy} = \min\bigl(\text{Length}(\mathbf{K}), 189\bigr) \text{ bits.} \tag{6.6}$$

Recently, Stoianov [31] has proposed an attack on the iris-based key regeneration scheme of Kanade et al. [13] which targets the zero insertion scheme. This attack takes into consideration the known positions of the zeros inserted into the iris codes. Using this attack, a large amount of errors in the Hadamard codewords can be corrected and hence the crypto-biometric key can be recovered. The same zero insertion scheme is applied in the multi-unit type system described in this chapter. However, in this scheme, the de-shuffling process is done after the Hadamard codes error correction level. Therefore, even if an attacker successfully decodes the Hadamard codewords, he still needs to overcome the security offered by the shuffling/de-shuffling process. Moreover, this scheme involves multiple biometric information sources. The zeros are inserted into only one iris code, while the other iris code is left as it is. This provides another level of protection against the attack reported by Stoianov.

In order to carry out experimental security evaluation, we defined two extreme scenarios: (1) stolen biometric scenario, where an impostor always provides a stolen biometric sample of the genuine user, and (2) stolen key scenario, in which the impostor always provides a stolen shuffling key of the genuine user.

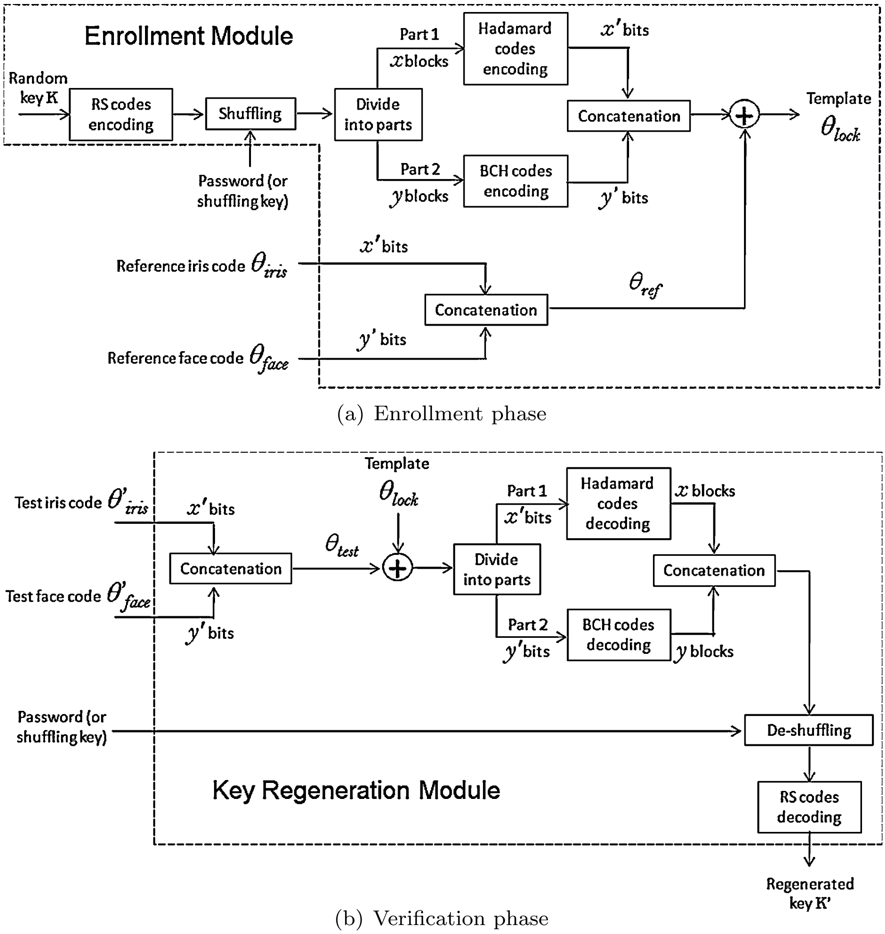
In the stolen biometric scenario, the FAR of the system remains unchanged (i.e., FAR = 0 %). The shuffling process prevents the impostor from being accepted when he provides the correct biometric data but a wrong shuffling key. Thus, use of shuffling completely eliminates the threat caused by compromised biometric data.

In the other security scenario, stolen key scenario, the system still has two iris codes which provide the security. The performance in this situation degrades but it is equivalent to that of the system without shuffling. Moreover, the performance degradation is only in terms of increase in FAR. The FRR remains unchanged even if the shuffling key is stolen. This is a distinct advantage of the proposed system.

6.5 Multi-modal Type Multi-biometrics Based Key Regeneration

6.5.1 Algorithm for Multi-modal Biometrics Based Key Regeneration

Multi-modal biometric systems combine biometric information from different traits. In this case, an attacker who wants to break into the system by creating fake biometric samples needs more efforts. Therefore, having multi-modal biometrics can significantly increase the security of the system. Combination of information from two biometric traits in the feature domain results in increase of the length of the feature vector. Additionally, the entropy of the crypto-bio keys also increases. We adapt the *FeaLingECc* scheme described in Sect. 6.3 in order to combine the information



(a) Enrollment phase

(b) Verification phase

Fig. 6.6 Schematic diagram of the multi-modal biometrics-based template protection scheme using *FeaLingECc*: (**a**) Enrollment phase, (**b**) Key regeneration phase

from an iris and a face image of a person. The length of the iris feature vector is 1,188 bits, while that of the face feature vector is 3,200 bits. Following the notations of the general scheme described in Sect. 6.3, we consider iris as Biometric-1 and face as Biometric-2. Hadamard codes are used as Level-1 ECC for iris while Bose, Ray-Chaudhuri, Hocquengem (BCH) codes are used for face. These ECC are selected according to the Hamming distance distributions of the corresponding biometric data. Reed–Solomon (RS) codes are used as Level-2 ECC, which are common for iris and face. The schematic diagrams of the enrollment and key regeneration phase of the proposed multi-modal biometrics-based system are shown in Fig. 6.6(a) and 6.6(b), respectively.

The basic functioning of this scheme is the same as described in Sect. 6.3. But the involvement of two different types of biometric data raises many design complications. The two biometric data (iris and face) being combined are different in nature. The amount of variabilities, which is treated as errors, is different for iris and face images. In key regeneration systems, the goal is to correct only the intra-user variabilities. The amount of such errors to be corrected is highly dependent on the biometric data set. The error correction capacities for each of the biometric traits need to be set according to their respective Hamming distance distributions for genuine and impostor comparisons.

6.5.2 Experimental Setup—Multi-modal Biometrics Based Key Regeneration System

In this work, we created a virtual database created from two publicly available databases: the NIST-ICE database [26] for iris, and the NIST-FRGCv2 database [25] for face. In this selected data set, there are 175 subjects having five samples each of iris and face images. The face images are taken from the controlled data set of the FRGCv2 database. For each subject, data pairs are formed containing one iris image and one face image corresponding to that subject. Thus, we have five such pairs per subject for 175 subjects. For genuine comparisons, each data pair is compared with every other data pair corresponding to the same subject. Similarly, each data pair is compared with every other data pair of every other subject for impostor comparisons. This protocol results in 1,750 genuine comparisons and 380,625 impostor comparisons. For the sake of fair comparison with uni-biometric systems, similar protocol is followed to test the uni-biometrics-based systems' performance in this chapter.

We used a Gabor filter-based approach to extract features from the face image [19]. The face image is first geometrically normalized using the CSU Face Recognition System [1], and then processed using log-Gabor filters having four scales and eight orientations using the MATLAB source code available at [18]. Magnitude of the filtered output is calculated, downsampled, and concatenated to form a 3,200-element feature vector. The values in this vector are then binarized to obtain a 3,200-bit string called face code. The binarization process used is fairly simple. The median of the values in a feature vector is taken as a threshold for that feature vector. The elements having higher value than the threshold are made one while the remaining are made zeros.

By observing the Hamming distance distributions for genuine and impostor comparisons for iris on the development data set, we know that the iris data need nearly 35 % error correction. For face, we used only the controlled subset of the FRGCv2 data set. The error correction required on this subset is nearly 21 %. Note that these quantities of error correction requirements are specific to the data set concerned and will change according to the modality and acquisition conditions. Also the amount of error correction required for the iris is higher than for the face. However, this does not impact the verification performance. The verification performance depends on the separation between genuine and impostor Hamming distance distributions (see Table 6.4).

As shown in [13], Hadamard codes along with the zero insertion scheme can achieve the 35 % error correction requirement for iris. For face, BCH codes can be applied for correcting the 21 % errors. Therefore, we use Hadamard codes as Level-1 ECC for iris and BCH codes as Level-1 ECC for face. The Level-2 ECC are Reed–Solomon (RS) codes which is a common level for iris and face. But the error correction scheme in the proposed system is a cascaded structure where the dimensions of the Level-1 and Level-2 codes must be compatible. Each of the three ECC used in the system (RS, BCH, and Hadamard codes) has its own dimensional restrictions.

The Hadamard codes (which are used for iris) have a fixed relation between input and output size: a block of m bits is converted into a block of 2^{m-1} bits. The Reed–Solomon codes of block size m bits can have a maximum of 2^{m-1} blocks. The BCH codes having $\approx$21 % error correction capacity are: BCH$(127, 15, 27)$, BCH$(255, 21, 55)$, BCH$(511, 28, 111)$, BCH$(1023, 36, 223)$, BCH$(2047, 56, 443)$, etc. The suitable ECC sizes also depend on the dimensions of the individual biometric feature vectors. For example, the face code is 3,200 bit. It has to be truncated such that its length is an integer multiple of the BCH code output size. Similarly, the effective iris code length must be an integer multiple of the Hadamard code output size (32 or 64 bits). Moreover, from our experiments, we know that the iris system performs better (from biometric recognition point of view) than the face system and hence, it is desirable to apply higher weights to iris than to face. This means that more blocks of RS codes output should be used for iris than for face.

Taking all these requirements into consideration, we fixed the size of the RS codes block to be equal to $m = 7$. The output of the RS codes encoder is also in form of blocks each of which is 7-bit. Hadamard codes of input size $m = 7$ should be used for compatibility. The output of these Hadamard codes is 64-bits. The length of the iris code after zero insertion is 1984 bits and thus there can be 31 blocks of Hadamard codes. This also means that 31 blocks of RS codes output are used for iris. The BCH codes should be selected such that the input size of BCH codes is an integer multiple of seven (7) but also keeping in mind that the total number of RS code blocks required for face remains less than 31. BCH$(127, 15, 27)$ and BCH$(255, 21, 55)$ will require 50 and 36 RS code blocks which is more than that required for iris. Therefore, these codes cannot be employed in the system. Hence we applied the next two possible BCH codes: BCH$(511, 28, 111)$ and BCH$(1023, 36, 223)$.

In case of BCH$(511, 28, 111)$, four RS codes output blocks are concatenated to form a single input block. The 3,200-bit face code is truncated to 3,066 bits which is an integer multiple of 511. There are six such BCH code blocks which require 24 RS codes output blocks. Thus, the total number of output blocks required in the RS codes is $31 + 24 = 55$. The iris part has $31/55 = 56$ % weight in the final verification decision while the face part has 44 % weight.

For the other possible BCH codes, BCH$(1023, 36, 223)$, five RS codes output blocks are concatenated and a zero is appended to it in order to obtain the required 36-bit input block. There can be three such BCH blocks requiring 15 RS

Table 6.4 Baseline biometric systems' user verification performances in terms of EER in % on subsets of NIST-ICE and NIST-FRGCv2 databases; values in bracket indicate the error margins for 90 % confidence interval; Baseline—corresponds to baseline biometric system; Shuffled—the shuffling scheme is applied. Results previously published in [16]

Exp.	Iris	Face	Iris+face
Baseline	1.29 [±0.23]	6.53 [±0.52]	1.06 [±0.22]
Shuffled	0.35 [±0.12]	0	0

code blocks. Thus the total number of RS code blocks is $31 + 15 = 46$. The iris is given 67 % weight in this scenario while the face is given 33 % weight.

It is also possible to combine BCH codes of different dimensions to apply different weights. For example, in a third setting, we applied 61 % weight to iris and 39 % to face. In order to achieve this, we employed one set of BCH$(2047, 56, 443)$ codes in combination of four sets of BCH$(255, 21, 55)$ codes. This requires $(8 + 12 =)20$ RS code blocks.

The experimental performance evaluation along with security analysis of this system is presented in the following subsection.

6.5.3 Results and Security Analysis for the Multi-modal (Iris and Face) Type System

The experimental results and theoretical as well as experimental security analysis are presented in this section.

6.5.3.1 Experimental Results of the Multi-modal (Iris and Face) Type System

For comparison purposes, the baseline biometric systems' verification performances are presented in Table 6.4. The BioSecure tool for performance evaluation [2] is used to calculate the EER and confidence intervals. This tool takes the number of comparisons and the match scores into account to calculate the error bounds on the verification error rates. The high improvement in the face verification system after shuffling is due to the high impact of shuffling on impostor face distribution. Shuffling makes the impostor distribution random. The randomness in un-shuffled iris data is higher than that of the face data, and hence, the impact of shuffling on face data is higher than that on iris data.

As said earlier, we evaluated the multi-modal system with three sets of experiments by applying different weights. In Set-1, RS codes having 55 blocks at the output are used. 31 out of these 55 (i.e., ≈56 %) are used for iris and remaining 24 (i.e., ≈44 %) are for face. The BCH codes used in this set are BCH$(511, 28, 111)$. Since it requires 28-bit input, four RS code blocks are combined to form that block resulting in a total of 24 RS code blocks for face.

Table 6.5 Results for the proposed multi-modal biometrics-based key regeneration system—Set-1 (iris weight = 56 %, face weight = 44 %). FRR and FAR values are in %. $\|K\|$ indicates length of key K in bits; t_s denotes the error correction capacity of RS codes. Results previously published in [16]

t_s	$\|K\|$	Without shuffling		With shuffling	
		FRR	FAR	FRR	FAR
3	343	7.54	2.93	7.54	0
9	259	1.94	20.80	1.94	0
12	217	0.91	36.43	0.91	0
16	161	0.17	62.93	0.17	0

Table 6.6 Results for the proposed multi-modal biometrics-based key regeneration system—Set-2 (iris weight = 61 %, face weight = 39 %). Other signs have the same meaning as in Table 6.5

t_s	$\|K\|$	Without shuffling		With shuffling	
		FRR	FAR	FRR	FAR
3	315	6.46	3.89	6.46	0
6	273	2.74	13.41	2.74	0
8	245	1.66	22.70	1.66	0
10	217	0.86	32.70	0.86	0

In the second setting, Set-2, 61 % weight is applied to iris and 39 % is applied to face. The errors in face data are corrected by a combination of BCH$(2047, 56, 443)$ and BCH$(255, 21, 55)$ codes. BCH$(2047, 56, 443)$ require concatenation of eight RS code blocks while each of the BCH$(255, 21, 55)$ requires three RS code blocks. The total number of RS code blocks required in this setting is 51 out of which, 31 are used for iris and 20 for face.

In the third setting, Set-3, RS codes with 46-block output are selected, and 31 of them are used for iris (i.e., ≈67 %) and remaining 15 blocks for face (i.e., 33 %). BCH codes of higher output size are used so that the number of blocks coming from BCH codes will reduce. We selected BCH$(1023, 36, 223)$ for which the error correction capacity is nearly the same. The 36-bit input required for these BCH codes is obtained by concatenating five RS code blocks appended with a zero. Thus, at the time of decoding, the last bit of the decoded value is discarded.

The results for these three experiments are reported in Tables 6.5, 6.6 and 6.7, respectively. For all the settings, we also carried out experiments without using shuffling, which are also reported.

The improvement in performance over uni-biometrics-based systems is threefold:

- better verification accuracy, e.g., at FRR of 0.91 %, FAR = 0 % for multi-biometric system while for iris-based uni-biometric system, FRR = 0.86 % at

Table 6.7 Results for the proposed multi-modal biometrics-based key regeneration system—Set-3 (iris weight = 67 %, face weight = 33 %). Other signs have the same meaning as in Table 6.5. Results previously published in [16]

t_s	$\|K\|$	Without shuffling		With shuffling	
		FRR	FAR	FRR	FAR
1	308	8.23	1.31	8.23	0
2	294	5.48	3.80	5.48	0
8	210	0.91	29.80	0.91	0
11	168	0.11	49.33	0.11	0

FAR = 0.21 %; similarly, for face-based uni-biometric system, FRR = 7.08 % at FAR = 0,

- longer keys, e.g., 186 and 217 bit keys for uni- and multi-biometric systems, respectively, at accuracies said above,
- higher key entropy, 183-bit for multi-biometric system while 83 for iris-based uni-biometric system.

The security of the multi-modal biometrics-based system is analyzed in the next subsection.

6.5.3.2 Security Analysis of the Multi-modal (Iris and Face) Type System

Theoretical as well as experimental security evaluation of the proposed system is presented in this section. Using the procedure of Daugman [6], the number of degrees of freedom in the iris and face codes are estimated to be equal to 556 and 243, respectively. Note that this estimation depends on the impostor Hamming distance distribution and can change with the data set being used for evaluation. The total number of degrees of freedom in the fused feature vector is $N = 556 + 243 = 799$. In total, the system can correct 27 % errors in this code (i.e., $P = N * 0.27 \approx 216$). Applying (6.4), an impostor needs,

$$\mathrm{BF} \approx \frac{2^N}{\binom{N}{P}} \approx \frac{2^{799}}{\binom{799}{216}} \approx 2^{131}, \tag{6.7}$$

brute force calculations to obtain the key. Thus the entropy contributed by the biometric information is 131 bits. The shuffling scheme, which employs a shuffling key obtained with a password can add up to 52 bits of entropy to this estimate resulting in $131 + 52 = 183$ bits entropy. Therefore, the total entropy estimate for the multi-modal type key regeneration system can be given as

$$\text{Entropy} = \min\bigl(\text{Length}(\mathbf{K}), 183\bigr) \text{ bits}. \tag{6.8}$$

This entropy is significantly higher than that of the uni-biometrics-based system. The entropy of the keys reported for the iris-based uni-biometric system in [13] is 83 bits.

Experimental security evaluation of the multi-modal type key regeneration system is carried out in a way similar to that performed for the two-iris system. In the stolen biometric scenario, the performance of the system remains unchanged. None of the impostors who provide stolen biometric data along with a wrong shuffling key is accepted by the system. However, in the stolen key scenario, the FAR is equal to that of the system without shuffling.

An interesting observation from the results in the stolen key scenarios is that the system can better resist such attacks when higher weight is applied to the better performing modality. For example, in stolen key scenario, the FAR is equal to 36.43 % at FRR = 0.91 % for Set-1 where iris is given 56 % weight. At a similar FRR (0.86 %), the FAR is 32.70 % in the Set-3 when iris is given 61 % weight in Set-2. While at the FRR = 0.91 %, the FAR is equal to 29.80 % for Set-2 where iris is given 67 % weight.

6.6 Conclusions and Perspectives

Using multi-biometrics has several advantages over uni-biometrics such as: better verification accuracy, larger feature space to accommodate more subjects, and higher security against spoofing. We exploit these advantages and employ multi-biometrics for obtaining high entropy keys. Additionally, the systems described in this chapter also protect the biometric templates and enhance security and privacy.

In order to have keys with higher entropy and better security, we combine the biometric information in feature domain. We propose a novel method of *Fea*ture *L*evel Fus*ion* through Wei*g*hted *E*rror *C*orre*c*tion (*FeaLingECc*). With this method, different weights can be applied to different biometric data. The shuffling scheme, which we applied earlier to the biometric data, is used in this system to randomize the error correcting codes data which helps make the system more secure. Additionally, the shuffling scheme induces revocability, template diversity, and privacy protection in the system.

Two systems are discussed: (1) a multi-unit type system, and (2) a multi-modal type system. Information from the left and right iris of a person is combined in the multi-unit type system to obtain long and high entropy crypto-bio keys. The second scheme is a multi-modal biometrics-based system in which information from iris and face is combined.

The parameters (choice of ECC and correction capacity) of the systems are first tuned on development databases and the systems are evaluated on the evaluation databases. For the two-iris tests, we used the NIST-ICE database. On this database, we obtain 147-bit keys having 147-bit entropy with 0 % FAR and 0.18 % FRR.

The multi-modal system (iris + face) is evaluated on a virtual database created by combining images from the NIST-ICE and NIST-FRGCv2 databases. We succeed to obtain 210-bit keys having 183-bit entropy at 0.91 % FRR and 0 % FAR. There is a significant improvement over uni-modal biometrics-based systems, specifically in terms of the key entropy. The key entropies for iris- and face-based uni-modal systems are 83 and 110 bits, respectively, while the entropy for the multi-iris-based system is 147 bits and for iris-face-based system, it is 183 bits.

The proposed scheme can be adapted to other biometric modalities. The feature level fusion combined with weighted error correction method allows the fusion of biometric modalities having different performances (e.g., face + iris). This opens up new directions for combining biometric information from different sources and having different dimensions.

References

1. Beveridge JR, Bolme D, Raper BA, Teixeira M (2005) The CSU face identification evaluation system. Machine Vision and Applications 16(2):128–138
2. Biosecure Tool (2007) Performance evaluation of a biometric verification system. Online. http://svnext.it-sudparis.eu/svnview2-eph/ref_syst/Tools/PerformanceEvaluation/doc/
3. Boyen X (2004) Reusable cryptographic fuzzy extractors. In: 11th ACM Conference on Computer and Communications Security (CCS)
4. Burr WE, Dodson DF, Polk WT (2006) Electronic authentication guideline. Recommendations of the National Institute of Standards and Technology
5. Cimato S, Gamassi M, Piuri V, Sassi R, Scotti F (2008) Privacy-aware biometrics: design and implementation of a multimodal verification system. In: Annual Computer Security Applications Conference (ACSAC). doi:10.1109/ACSAC.2008.13
6. Daugman J (2003) The importance of being random: statistical principles of iris recognition. Pattern Recognition 36(2):279–291
7. Dodis Y, Reyzin L, Smith A (2004) Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In: Proceedings of the Eurocrypt 2004, pp 523–540
8. Fu B, Yang SX, Li J, Hu D (2009) Multibiometric cryptosystem: model structure and performance analysis. IEEE Transactions on Information Forensics and Security 4(4):867–882
9. Hao F, Anderson R, Daugman J (2006) Combining crypto with biometrics effectively. IEEE Transactions on Computers 55(9):1081–1088
10. Jain AK, Nandakumar K, Nagar A (2008) Biometric template security. EURASIP Journal on Advances in Signal Processing 2008:579416. 17 pp. doi:10.1155/2008/579416
11. Juels A, Sudan M (2002) A fuzzy vault scheme. In: Lapidoth A, Teletar E (eds) Proc IEEE Int Symp Information Theory. IEEE Press, New York, p 408
12. Juels A, Wattenberg M (1999) A fuzzy commitment scheme. In: Proceedings of the Sixth ACM Conference on Computer and Communication Security (CCCS), pp 28–36
13. Kanade S, Camara D, Krichen E, Petrovska-Delacrétaz D, Dorizzi B (2008) Three factor scheme for biometric-based cryptographic key regeneration using iris. In: The 6th Biometrics Symposium (BSYM)
14. Kanade S, Petrovska-Delacrétaz D, Dorizzi B (2009) Cancelable iris biometrics and using error correcting codes to reduce variability in biometric data. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition
15. Kanade S, Petrovska-Delacrétaz D, Dorizzi B (2009) Multi-biometrics based cryptographic key regeneration scheme. In: IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS)
16. Kanade S, Petrovska-Delacrétaz D, Dorizzi B (2010) Obtaining cryptographic keys using feature level fusion of iris and face biometrics for secure user authentication. In: IEEE CVPR Workshop on Biometrics
17. Kelkboom E, Zhou X, Breebaart J, Veldhuis R, Busch C (2009) Multi-algorithm fusion with template protection. In: IEEE Second International Conference on Biometrics Theory, Applications and Systems

18. Kovesi P (2005) Matlab and octave functions for computer vision and image processing. Online. http://www.csse.uwa.edu.au/~pk/Research/MatlabFns/
19. Lades M, Vorbrüuggen JC, Buhmann J, Lange J, von der Malsburg C, Wüurtz RP, Konen W (1993) Distortion invariant object recognition in the dynamic link architecture. IEEE Transactions on Computers 42(3):300–311
20. Lumini A, Nanni L (2007) An improved biohashing for human authentication. Pattern Recognition 40(3):1057–1065. doi:10.1016/j.patcog.2006.05.030
21. MacWilliams FJ, Sloane NJA (1991) Theory of Error-Correcting Codes. North Holland, Amsterdam
22. Maiorana E, Campisi P, Ortega-Garcia J, Neri A (2008) Cancelable biometrics for HMM-based signature recognition. In: IEEE Conference on Biometrics: Theory, Applications and Systems (BTAS)
23. Nandakumar K (2008) Multibiometric systems: fusion strategies and template security. Phd thesis, Department of Computer Science and Engineering, Michigan State University
24. Nandakumar K, Jain AK (2008) Multibiometric template security using fuzzy vault. In: IEEE Second International Conference on Biometrics: Theory, Applications and Systems
25. National Institute of Science and Technology (NIST) (2005) Face recognition grand challenge. http://www.frvt.org/FRGC/
26. National Institute of Science and Technology (NIST) (2005) Iris challenge evaluation. http://iris.nist.gov/ice
27. Online. http://svnext.it-sudparis.eu/svnview2-eph/ref_syst/
28. Petrovska-Delacrétaz D, Chollet G, Dorizzi B (eds) (2009) Guide to Biometric Reference Systems and Performance Evaluation. Springer, Berlin
29. Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(4):561–572. doi:10.1109/TPAMI.2007.1004
30. Ross AA, Nandakumar K, Jain AK (2006) Handbook of Multibiometrics. International Series on Biometrics. Springer, Berlin
31. Stoianov A (2010) Security of error correcting code for biometric encryption (critical note). In: Eighth Annual International Conference on Privacy, Security and Trust
32. Sutcu Y, Li Q, Memon N (2007) Secure biometric templates from fingerprint-face features. In: IEEE Conference on Computer Vision and Pattern Recognition, pp 1–6. doi:10.1109/CVPR.2007.383385