creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

Ph.D. DISSERTATION

Cancelable Biometrics based on Biometric Salting

임의 흩뿌림에 기반한 가변생체인증

BY

LEE DAE-HYUN

AUGUST 2018

DEPARTMENT OF ELECTRICAL ENGINEERING AND
COMPUTER SCIENCE
COLLEGE OF ENGINEERING
SEOUL NATIONAL UNIVERSITY

Abstract

Nowadays biometrics systems for identification or authentication of a person are everywhere. These system have a number of advantages. In particular, biometrics traits cannot be lost or forgotten compared to passwords. Moreover biometric identification offers good accuracy. However, their uses raises several privacy concerns, especially in their storage. In fact, if a password is stolen, it can be replaced by a new password. This is not possible in biometrics. To overcome the security problems, biometric cryptosystems (BCS) and cancelable biometrics (CB) represent emerging technologies of biometrics template protection addressing this concerns and improving public confidence and acceptance of biometrics. BCS are designed to securely bind a digital key to a biometric or generate a digital key from a biometric offering solutions to biometric-dependent key-release and biometric template protection while CB consist of intentional, repeatable distortions of biometric signals based on transforms which provide a comparison templates in the transformed domain.

In this dissertation, a cancelable biometric scheme for iris recognition system is proposed. The first proposed CB method uses the reduced random permutation and binary salting (RRP-BS). RRP-BS consists of random permutation of binary iris template followed by the orthogonal binary salting. The random permutation perturbs the rows of iris template structure and eliminates some rows of iris template. This guarantees the non-invertibility of CB scheme even though the all of bio-security keys is stolen. Then this CB scheme also proposes an orthogonal binary salting method, where the random binary keys are generated by Gram-Schmidt orthogonalization. The orthogonality of random keys maximizes the Hamming distances among binary-salted templates. Thus, the inter classes (different users) are discriminated while the intra class (one user) is well identified. While this method has good performance and unlinkability, its non-invertibility is vulnerable to muliplicity or hill-climbing attacks.

The second proposed method uses more robust non-invertibility transform based on the first method. We use the RRP-BS as the biometric salting, and use the Hadamard product for enhancing the non-invertibility of salted data. Moreover, to overcome the shortcomings of perserving the keys of the conventional salting methods, we generate several templates for an input, and define non-coherent and coherent matching regions among these templates. We show that salting the non-coherent matching regions is less influential on the overall performance. Specifically, embedding the noise in this region does not affect the performance, while making the data difficult to be inverted to the original. For the evaluation, we use three datasets, namely CASIA V3 iris-interval, IIT Delhi iris, and ND-Iris-0405. The extensive evaluations show that the proposed algorithm yields low error rates and good intra/inter classification performances, which is better or comparable to the existing methods. Moreover, the security analysis ensures that the proposed algorithm satisfies non-invertibility and unlinkability, and is robust against several attacks as well.

주요어: biometrics, cancelable biometrics, biometric salting

학 번: 2009-20855

Contents

List of Tables

List of Figures

Chapter 1

INTRODUCTION

1.1 Biometrics

The word biometrics is defined as automated recognition of individuals based on their behavioral and biological characteristics (ISO/IEC JTC1 SC37). Physiological as well as behavioral biometric characteristics are acquired applying adequate sensors and distinctive features are extracted to form a biometric template in an enrollment process. At the time of verication or identication (identication can be handled as a sequence of verications and screenings) the system processes another biometric input which is compared against the stored template, yielding acceptance or rejection. It is generally conceded that a substitute to biometrics for positive identication in integrated security applications is non-existent. While the industry has long claimed that one of the primary benefits of biometric templates is that original biometric signals acquired to enroll a data subject cannot be reconstructed from stored templates, several approaches have proven this claim wrong. Since biometric characteristics are largely immutable, a compromise of biometric templates results in permanent loss of a subjects biometrics. Standard encryption algorithms do not support a comparison of biometric templates in encrypted domain and, thus, leave biometric templates exposed during every authen-

tication attempt (homomorphic and asymmetric encryption, which enable a biometric comparison in encrypted domain represent exceptions). Conventional cryptosystems provide numerous algorithms to secure any kind of crucial information. While user authentication is based on possession of secret keys, key management is performed introducing a second layer of authentication (e.g., passwords). As a consequence, encrypted data inherit the security of according passwords applied to release correct decrypting keys. Biometric template protection schemes which are commonly categorized as biometric cryptosystems (also referred to as helper data-based schemes) and cancelable biometrics (also referred to as feature transformation) are designed to meet two major requirements of biometric information protection (ISO/IEC FCD 24745)

Irreversibility It should be computationally hard to reconstruct the original biometric template from the stored reference data, i.e., the protected template, while it should be easy to generate the protected biometric template

Unlinkability Different versions of protected biometric templates can be generated based on the same biometric data (renewability), while protected templates should not allow cross-matching (diversity)

Cancelable biometrics (CB) consist of intentional, repeatable distortions of biometric signals based on transforms which provide a comparison of biometric templates in the transformed domain. The inversion of such transformed biometric templates must not be feasible for potential imposters. In contrast to templates protected by standard encryption algorithms, transformed templates are never decrypted since the comparison of biometric templates is performed in transformed space which is the very essence of CB. The application of transforms provides irreversibility and unlinkability of biometric templates. Cancelable biometric transforms are designed in a way that it should be computationally hard to recover the original biometric data. The intrinsic strength (individuality) of biometric characteristics should not be reduced applying transforms (constraint on FAR) while on the other hand transforms should be

tolerant to intra-class variation (constraint on FRR). In addition, correlation of several transformed templates must not reveal any information about the original biometrics (unlinkability). In case transformed biometric data are compromised, transform parameters are changed, i.e., the biometric template is updated. To prevent impostors from tracking subjects by cross-matching databases it is suggested to apply different transforms for different applications. Two main categories of CB are distinguished. (1) Non-invertible transforms: In these approaches, biometric data are transformed applying a noninvertible function. In order to provide updatable templates, parameters of the applied transforms are modified. The advantage of applying non- invertible transforms is that potential impostors are not able to reconstruct the entire biometric data even if transforms are compromised. However, applying noninvertible transforms mostly implies a loss of accuracy. Performance decrease is caused by the fact that transformed biometric templates are difficult to align (like in BCSs) in order to perform a proper comparison and, in addition, information is reduced. For several approaches these effects have been observed. (2) Biometric salting: Biometric salting usually denotes transforms of biometric templates which are selected to be invertible. Any invertible transform of biometric feature vector elements represents an approach to biometric salting even if biometric templates have been extracted in a way that it is not feasible to reconstruct the original biometric signal. As a consequence, the parameters of the transform have to be kept secret. In case user-specific transforms are applied, the parameters of the transform which can be seen as a secret seed have to be presented at each authentication. Impostors may be able to recover the original biometric template in case transform parameters are compromised, causing a potential performance decrease of the system in case underlying biometric algorithms do not provide high accuracy without secret transforms. While approaches to biometric salting may maintain the recognition performance of biometric systems non-invertible transforms provide higher security.

1.2 Outline of the Dissertation

In this dissertation, a cancelable biometric scheme for recognition system is proposed. Specifically, even though we used only iris biometric for this purpose, all biometrics can be applied if they can be represented as binary data. Chapter 2 shows the background about iris biometric systems and security problems. Chapter 3 proposes a cancelable biometric scheme using random permutation and orthogonal keys. Since the original bio-information of individual user cannot be replaced, the biometric templates should be more secure and be cancelable by some transforms. The first proposed CB method consists of random permutation of iris binary template followed by orthogonal binary salting. The random permutation perturbs the rows of iris template structure and eliminates some rows of iris template. This guarantees the non-invertibility of CB scheme even though the all of bio-security keys is stolen. Then this CB scheme also proposes an orthogonal binary salting method, where the random binary keys are generated by Gram-Schmidt orthogonalization. The orthogonality of random keys maximizes the Hamming dis- tances among binary-salted templates. Thus, the inter classes (different users) are discriminated while the intra class (one user) is well identified. But, because the tokens for CB are stored to database, there is still problem to be stolen by adver- sary. To overcome this situation, the proposed cancelable iris biometrics uses a combination method, which applies a non-invertible transform to the salted data. We use the reduced random permutation and binary salting (RRP-BS) method as the biometric salting, and use the Hadamard product for enhancing the non-invertibility of salted data. Moreover, to overcome the shortcomings of the conventional salting method, we generate several templates for an input, and define non-coherent and coherent matching regions among these templates. We show that salting the non-coherent matching regions is less influential on the overall performance. Specifically, embedding the noise in this region does not affect the performance, while making the data difficult to be inverted to the original. For the evaluation, we use three datasets, namely

CASIA V3 iris-interval, IIT Delhi iris, and ND-Iris-0405. The extensive evaluations show that the proposed algorithm yields low error rates and good intra/inter classification performances, which is better or comparable to the existing methods. Moreover, the security analysis ensures that the proposed algorithm satisfies non-invertibility and unlinkability, and is robust against several attacks as well.

Chapter 2

BACKGROUND

2.1 Iris Biometric Processing

The demand for biometric systems causes continuous proposals of new iris recognition techniques [1]. Most of traditional iris recognition systems has retained generic framework unaltered. In particular, generic iris recognition systems consist of four main stages.

- Iris image acquisition
- Image preprocessing
- Feature extraction
- Comparison

A flowchart of a generic iris recognition system is shown in Figure 2.1. With respect to image acquisition, good-quality images are necessary to provide a robust iris recognition system. Still, most current implementations of iris recognition systems require users to fully cooperate with the system. At preprocessing, the pupil and the outer boundary of the iris are detected. Subsequently, the vast majority of iris recognition algorithms unwraps the iris ring to a normalized rectangular iris texture. To complete

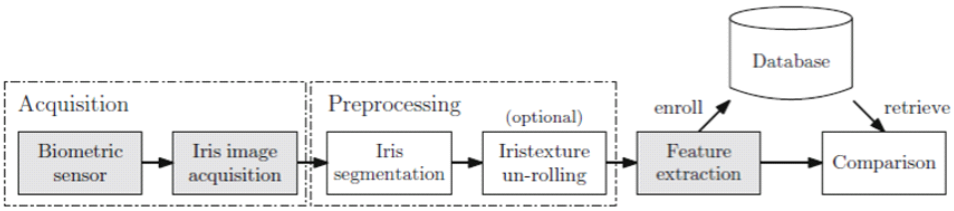

Figure 2.1: Iris biometric: the processing chain of a generic iris recognition system.

the preprocessing, the contrast of the resulting iris texture is enhanced applying histogram stretching methods. Based on the preprocessed iris texture, feature extraction is applied. As shown in figure 2.2, most iris recognition algorithms follow the approach of Daugman by extracting a binary feature vector, which is commonly referred to as iris-code. While Daugman suggests to apply 2D Gabor filters in the feature extraction stage, plenty of different methods have been proposed.Most comparison techniques apply the bit-wise XOR-operator to decide whether two iris-codes have the same biometric source (match) or not (non-match) [2]. The decision is based on a comparison score by counting the number of miss-matching bits: the (fractional) HD, the minimum number of substitutions required to change one bit-string into the other (divided by the string length), indicates the grade of dissimilarity. Small fractional HD values indicate high similarity. In order to compensate against head tilts, template alignment is achieved by applying circular shifts in both directions. The minimum HD between two iris-codes refers to an optimal alignment. Hence, the comparison of iris-codes can be performed in an efficient process, which can be parallelized easily. In contrast to other biometric systems based on different modalities requiring a more complex matching procedure, millions of comparisons can be done within one second. With respect to biometric recognition systems operating in identification mode, iris recognition algorithms are capable of handling large-scale databases. In addition, potential occlusions originating from eyelids or eyelashes are masked out during comparison by storing a bit-mask generated in the preprocessing step.

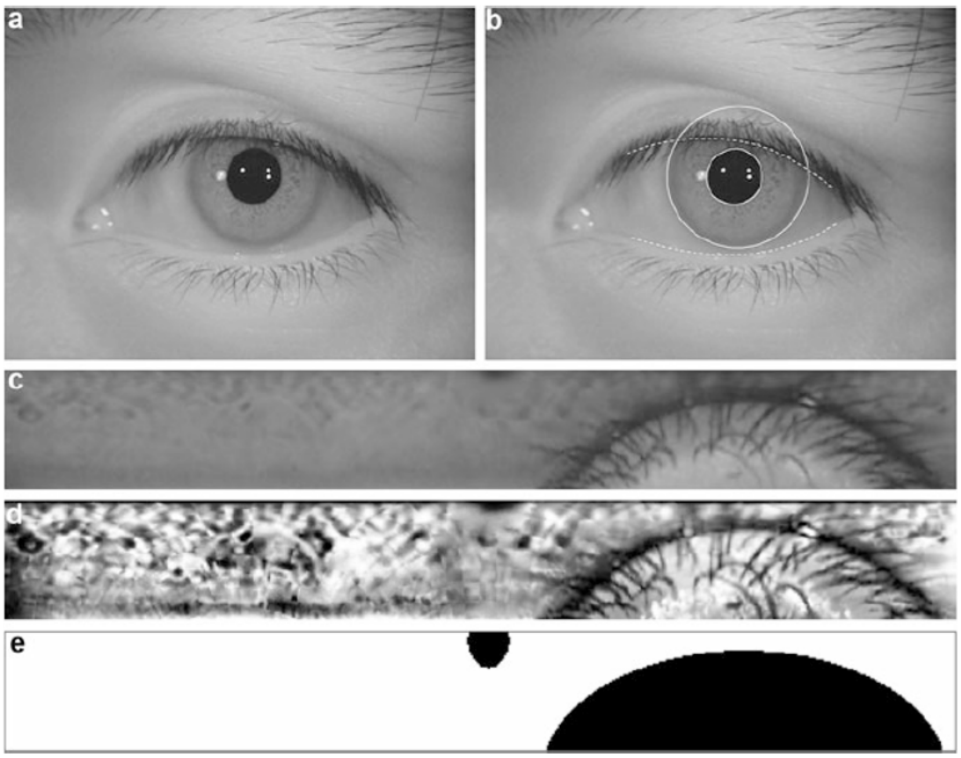

Figure 2.2: Processing steps: (a) original, (b) segmentation result, (c) iris texture before enhancement, (d) normalization result after enhancement, (e) noise mask.

2.2 Potential Attacks against Cancelable Biometrics

While in the vast majority of approaches security is put on a level with obtained recognition accuracy according to a reference system, analysis with respect to irreversibility and unlinkability is rarely done. With respect to irreversibility, the applied feature transformations have to be analyzed in detail. For instance, if block permutation of biometric data is utilized to generate cancelable templates the computational effort of reconstructing the original biometric data has to be estimated. While for some approaches analysis of irreversibility appear straightforward for others more sophisticated studies are required. In order to provide renewability of protected biometric templates, the applied feature transformations are performed based on distinct parameters. In general, protected templates differ more as more distant the respective transformation parameters are. To satisfy the property of unlinkability, different transformed templates, generated from a single biometric template applying different parameters, have to ap pear as distinct as templates of different subjects. This implies that the amount of applicable parameters is limited by the requirement of unlinkability. The major objective of attacking cancelable biometrics systems is to expose the hidden transform applied to biometric templates. Thereby substitution attack can be done by hackers. If transforms are nearly invertible then original biometric tem plates may be recovered or appoximately reconstructed. Hill climbing attacks could be performed and comparison score could be overwritten. Since most approaches to biometrics salting become highly vulnerable in case secret tokens are stolen false accept attacks could be effectively applied. If the salting process is invertible templates may be reconstructed and applied in masquer ade attacks. Approaches to biometric salting which do not comprise a key-binding step are vulnerable to overwriting final decisions. Several vulnerabilities in the origi nal concept of the BioHashing algorithm have been encountered in [3]. The main drawback of BioHashing resides in exhibiting low performance in case attackers are in possession of secret tokens.

Chapter 3

NON-INVERTIBLE CANCELABLE IRIS BIOMETRICS USING RANDOM PERMUTATION AND ORTHOGONAL KEYS

3.1 Introduction

The interest in biometrics have been increasing for security authentication systems including mobile phones. The fingerprint, face, and iris are the popular bio-information to feature the individual identity. The unique characteristics of bio-information distinguish genuine user from imposters. However it is especially important to secure the original bio-information since it is natural-born identity and cannot be replaced. Thus, the interest in cancelable biometric (CB) systems is increased recently. The cancelable biometrics means that the bio-information of each user can be replaced with another bio-templates, where the original and replaced templates should not be matched by some transforms. This dissertation focuses on the cancelable biometric algorithms for iris pattern.

Since Daugman proposed the automated iris recognition method, many algorithms of iris recognition have been developed. And the iris biometric template protection

systems have been highlighted.

Cancelable biometrics methods are aimed to satisfy the conditions. The basic structure of iris CB schemes is shown as Figure **??**. When the bio-information is entered in enrollment step, the iris codeword generator transforms it into the binary template or feature. Then, the CB key which are generated by personal identification number transforms the original codeword. The transformed bio-template should not matched to the original codeword. By changing the CB keys, the users can replace the previous stolen bio-templates with new one. The users protect their own original iris templates by transforming them with the CB keys. In authentication step, the transformed bio-template is compared with the current input template using the CB key transformation.

Various iris security system show good identification performance. Thus, this dissertation focuses on the CB scheme, and exploits the usual iris recognition algorithms. We proposes a non-invertible binary salting scheme with random permutation and orthogonal random keys, which satisfy all conditions of bio-information protection. The rows in the iris template are randomly permutated and some rows are eliminated for irreversibility. The reduced template is also changed by binary salting which uses orthogonal random keys generated by Gram-Schmidt orthogonalization. Then we inspects the optimal conditions on permutation schemes, number of skipped rows, and orthogonal basis keys. Consequently, the proposed CB scheme satisfies the irreversibility and good error rates of binary salting.

The rest of this chapter is organized as follows. Section 3.2 summarizes the related work of CB systems. In Section 3.3, the proposed CB scheme is described in detail. The random permutation and orthogonal basis keys are explained. Section 3.4 shows experimental results based on the stolen key scenario to prove the safer CB systems. Finally, this chapter is concluded in Section 3.5.

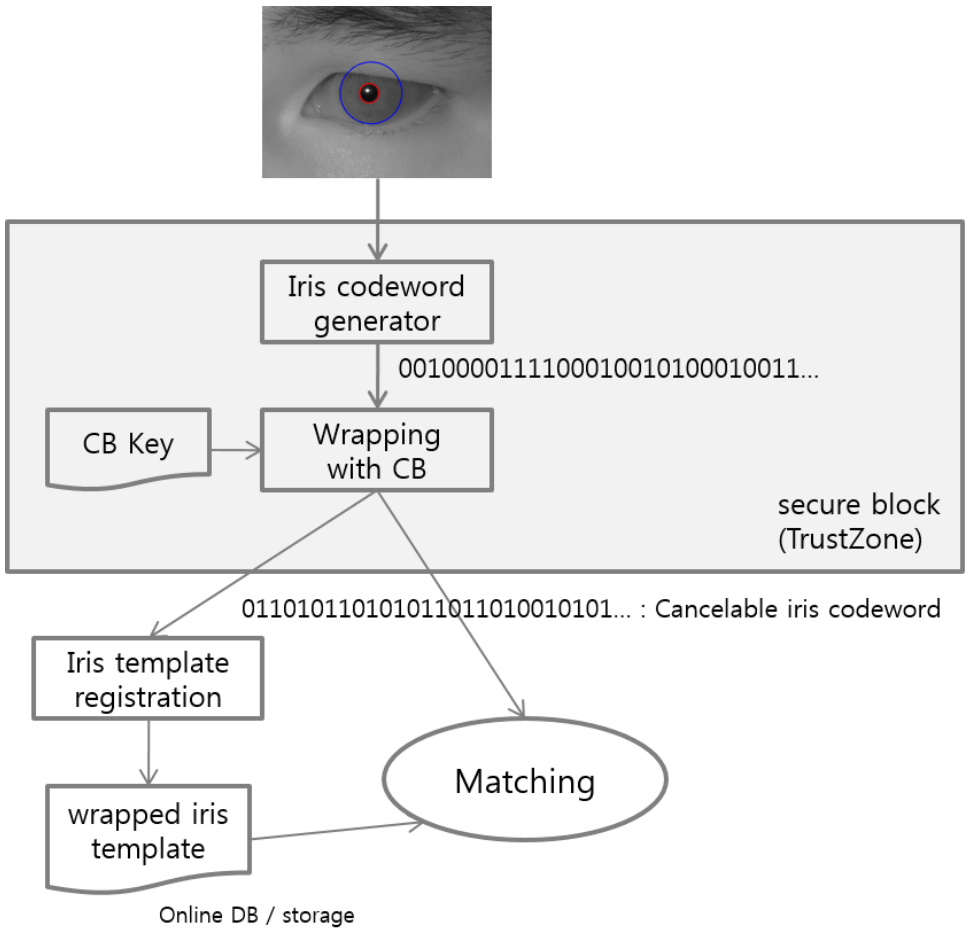

Figure 3.1: Cancelable biometric structure of iris information.

3.2 Related Works

There are two main groups of work in cancelable biometrics area, non-invertible transforms and biometric salting. The purpose of non-invertible transform methods is to make transforms not to reconstruct the original bio-templates even though the transforms are compromised. These approaches usually eliminate partial template data or they are computationally hard to get. Ratha *et al.* used fingerprint data for three non-invertible transforms such as polar, Cartesian, surface folding transforms [4]. The transforms distort an image space or permute image blocks, but these transforms lead to low discriminability between genuine and imposters if they are compromised. Zuo *et al.* proposed the method based on row shift and combinations (GRAY-COMBO, BIN-COMBO) to generate iris templates [5]. Since the partial templates are dropped for computational load, the method is sensitive to the eye boundary environment such as eyelids and eyelashes. Hmmerle-Uhl *et al.* proposed block re-mapping and image warping methods for iris biometric security [6]. Block permutation worked well in terms of non-invertible transform, but could not surpass the equal error rate (EER) of original template. These algorithms had trade-off between non-invertibility and discriminability in similar objects, and showed low performance of some measures such as EER, false acceptance rate (FAR), and false reject rate (FRR). Biometric salting means that user bio-templates are blended with auxiliary data such as random keys. Because salting algorithms use user-specific keys, the keys are easily revocable and regenerated when the keys are compromised. Jin *et al.* introduced biohashing to generate secure biocode template [7]. The orthogonal user-specific random matrix as a key is constructed by tokenized random number (TRN) and combined with features from bio templates. The random key maximizes distinctiveness among different users while minimizes the distances among the same user templates. However, the biohashing shows critically low performance when keys are stolen since the adversary can regenerate the coarse approximation of original bio-templates. Teoh *et al.* proposed multiple

random projection (MRP) onto non-invertible random subspace [21, 22]. MRP protects the original bio-templates excellently, but it exposed weak points when imposters steal the random projection keys. To mitigate the effect of some outlier such as specular reflections, eyelash and eyelids, Pillai *et al.* introduced sectored random projection (SRP), where they handled different qualities n each partial iris region [8, 9][23,24]. This method divides the iris into sectored regions and applies random projections separately to each sector followed by concatenating the transformed vectors [8]. And hash table which has permutated sector index is adopted for cancelable template [9]. When the random seed and the hash table are not compromised, the verification result is better than the random projection methods even if the random projection matrix is stolen. But if they are known to imposters, the performance is deteriorated as is the same cases with MRP. Zuo *et al.* proposed basic salting (GRAY-SALT, BIN-SALT) algorithms that blends random matrix with biocodes [5]. The salting methods show good performance in aspect of FAR and FRR, and BIN-SALT is specifically robust to stolen token scenario. But it has a disadvantage that the original biocodes can be completely reconstructed when the random keys are exposed. Savvides *et al.* proposed the idea to encrypt biometric template using random convolution kernel and minimum average correlation energy (MACE) filter [10]. They proved that the training image convolution before building MACE filter does not change the correlation result so that authentication performance preserves. But it is very vulnerable in situation with known random kernel.

More detailed and various reviews of cancelable biometrics are introduced in many literatures [11, 12, 13]. As mentioned before, this dissertation focuses on the cancelable biometric algorithms, not the recognition methods. Given the biocodes or bio templates by any recognition methods, the CB algorithms transform the original bio-information not to be invertible and not to be recovered without the user-specific keys.

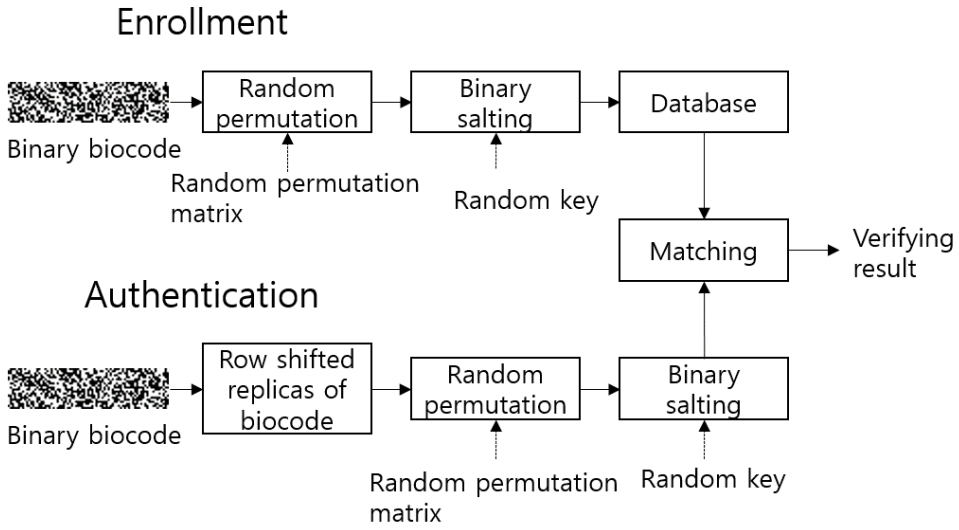

Figure 3.2: Proposed cancelable iris biometric system.

3.3 Proposed Non-invertible Binary Salting

In this section, reduced random permutation and binary salting (RRP-BS) scheme for cancelable biometrics is proposed. The proposed CB scheme considers the compromise situation, that is, all of individual information including bio-template, random permutation matrix, and random keys, is exposed to the imposters. The proposed CB scheme is shown in Figure 3.2. The original biocode or template is transformed by random permutation and random key. Furthermore, the transformed template lose some rows, thus, the proposed CB scheme satisfies the conditions of CB systems. The proposed CB method shows that the bio-templates can be replaced with new one without loss of recognition performance (EER, FAR, and FRR).

3.3.1 Binary Salting Review

Zuo introduced binary salting concept for cancelable iris biometrics [5]. Suppose that an original binary template or biocode of $m \times n$ matrix $X \in \{0,1\}^{m \times n}$ where m, n are

row and column number. X can be usually generated by Gabor filtering to unwrapped iris region and binary quantization as shown in Figure 3.2. Then the binary salting algorithm is mathematically described for one class,

$$Y = K \oplus X, \tag{3.1}$$

where K is an $m \times n$ random key matrix for binary salting with binary element, Y is the $m \times n$ transformed bio-template, and an operator $\oplus$ is the exclusive-OR. The random key K is usually obtained by binary quantizing random values from Gaussian distribution $N(0; 1)$ for each element. The binary salting is very simple method which can be used for legacy systems and have no trouble with outlier amplification [5]. Also, it fulfills three conditions of bio-information protection for cancelable biometric system described in Section [9, 14, 15]. Diversity is satisfied by using different with respect to different devices. The normalized Hamming distance (NHD) is usually used for matching in binary templates, the accuracy and reversibility can be easily proved by calculating cascaded exclusive-or operation. Note that when the random key K is compromised, the original bio-template X can be completely recovered from Y and K.

3.3.2 Random permutation

For protecting the original data, the random permutation and row elimination are introduced. Let $P \in \{0, 1\}^{r \times m}$ be a $r \times m$ permutation matrix with $r < m$ where r is a row control parameter to keep some rows and drop the others. The random permutation matrix has only one 1 in each row and there are no same rows in P. The permutation matrix perturbs the original bio-templates, which makes it difficult for imposters to recover the original biocodes. The binary salting in (3.1) is reformulated as

$$Y = K \oplus PX, \tag{3.2}$$

and the last rows in PX are eliminated. Thus, Y and K are changed to $r \times n$ matrix, respectively. The transformed template Y cannot be recovered to original data X since some rows in the original biocode are eliminated. The random keys in (3.2) should have large normalized Hamming distance (NHD) among the different keys. For the maximization of distances among the keys, this dissertation proposes the orthogonal binary keys.

3.3.3 Orthogonal random key

The orthogonal key set $\{K_1^{\perp}, K_2^{\perp}, \cdots, K_l^{\perp}\}$ g on each class can be generated by Gram- Schmidt orthogonalization process from random initial key $\{K_1, K_2, \cdots, K_l\}$. Let U_1 be a column vector which contains all elements of K_1. Then the orthonormal vector $U_l^{\perp}$ is calculated by Gram-Schmidt orthogonalization like this

$$U_l = K_l - \sum_{m=1}^{l-1} \frac{\langle K^l, U_m \rangle}{\langle U_m, U_m \rangle} U_m \tag{3.3}$$

$$U_l^{\perp} = \frac{U_l}{\|U_l\|} \tag{3.4}$$

where $\langle a, b \rangle$ denotes the inner product of vector a and b and $\| \cdot \|$ means l^2-norm function. After initial key set is transformed to orthonormal vector set $\{U_1^{\perp}, U_2^{\perp}, \cdots, U_l^{\perp}\}$ by 3.4, the orthogonal key set is obtained by

$$K_l^{\perp}(i, j) = b(U_l^{\perp}(N \cdot i + j)) \tag{3.5}$$

where $b(\cdot)$ is an element-wise quantizing function defined by

$$b(x) = \begin{cases} 0 \text{ if } x < 0 \\ 1 \text{ otherwise} \end{cases} \tag{3.6}$$

and $U_l^{\perp}(i)$ is i-th element of $U_l^{\perp}$. Since the binary random keys are generated in the vector space, the binary salting performance may be lower when the random keys are close or similar vectors. The proposed orthogonal keys maximizing the distances among themselves, by preserving the orthogonality of random keys in the vector space.

3.3.4 Cancelable Iris Biometric System

The entire system of proposed cancelable iris biometrics is shown in Fig. 3.2. In the enrollment stage, a user's eye image is captured and iris region is first extracted. Then the circular region is unwrapped to the rectangular image, and Gabor filter is applied to the unwrapped image. The initial binary biocode is generated by the usual iris recognition process. For the cancelable biometrics, the biocode is transformed by the proposed random row permutation, elimination of some rows, and binary salting with orthogonal random keys. The transformed binary template is stored to registration and authentication stage. In authentication stage, the template from query is acquired via the same process. But there is possibility not to be aligned between templates from query for the same class. To resolve the mismatch, the row-shifted templates are generated. Among the multiple distances with row-shifted templates, the minimum is chosen for the best match result. If the used random key and random permutation matrix are compromised, they are simply replaced with new ones. Note that the new key is generated through Gram-Schmidt method to keep the large distances between random keys.

3.3.5 Analysis of stolen key situations

In this subsection, the influence of stolen key situation is represented. Three cases of stolen key situation are inspected: 1) The orthogonal key $K^{\perp}$ is stolen. 2) The random permutation matrix P is stolen. 3) Both are stolen. Given the transformed templates Y_1 and Y_2, the normalized hamming distance between them becomes

$$D = \frac{1}{nr} \sum_{i=1}^{n} \sum_{j=1}^{r} (Y_1)_{ij} \oplus (Y_2)_{ij} \tag{3.7}$$

By combining 3.7 with 3.2, the Hamming distance is changed as below,

$$D = \frac{1}{nr} \sum_{i=1}^{n} \sum_{j=1}^{r} [(K_1^{\perp})_{ij} \oplus (P_1 X_1)_{ij}] \oplus [(K_2^{\perp})_{ij} \oplus (P_2 X_2)_{ij}] \tag{3.8}$$

In the first situation, two keys are same $K_1^{\perp} = K_2^{\perp}$ in (3.8) because random keys are compromised. By the associative and commutative property of exclusive OR operation, the equation (3.8) becomes as

$$D = \frac{1}{nr} \sum_{i=1}^{n} \sum_{j=1}^{r} (P_1 X_1)_{ij} \oplus (P_2 X_2)_{ij} \tag{3.9}$$

where (3.9) means that the hamming distance only depends on the random permutation. Figure 3.3 shows the correlation distribution among random permutation matrices. As shown in Figure 3.3, the distribution of random permutation matrices are closely similar to the Gaussian distribution, which means that the random permutation matrices are uncorrelated each other and their uncertainty or entropy is maximized. This property preserves the Hamming distances between templates when the random keys are stolen. In the second scenario, the permutation matrix is stolen so $P_1 = P_2 = P$ in (3.9). When PX_i is defined as X_i', the Hamming distance in (3.8) becomes

$$D = \frac{1}{nr} \sum_{i=1}^{n} \sum_{j=1}^{r} [(K_1^{\perp})_{ij} \oplus (X_1')_{ij}] \oplus [(K_2^{\perp})_{ij} \oplus (X_2')_{ij}] \tag{3.10}$$

This is the same when applying the simple binary salting to row-eliminated tem- plates, thus the performance will be similar to the conventional binary salting. In the last scenario, the random key and permutation matrix are stolen, thus $K_1^{\perp} = K_2^{\perp}$, and $P_1 = P_2$. The Hamming distance in (3.8) is changed as below,

$$D = \frac{1}{nr} \sum_{i=1}^{n} \sum_{j=1}^{r} (X_1')_{ij} \oplus (X_2')_{ij} \tag{3.11}$$

This does not apply the CB scheme except some missed rows. However, it is very difficult that the last situation occurs since the proposed CB scheme has two additional user-specific passwords, random permutation matrix and random orthogonal key. Consequently, the proposed CB scheme protects the bio-templates without loss of recognition performances.

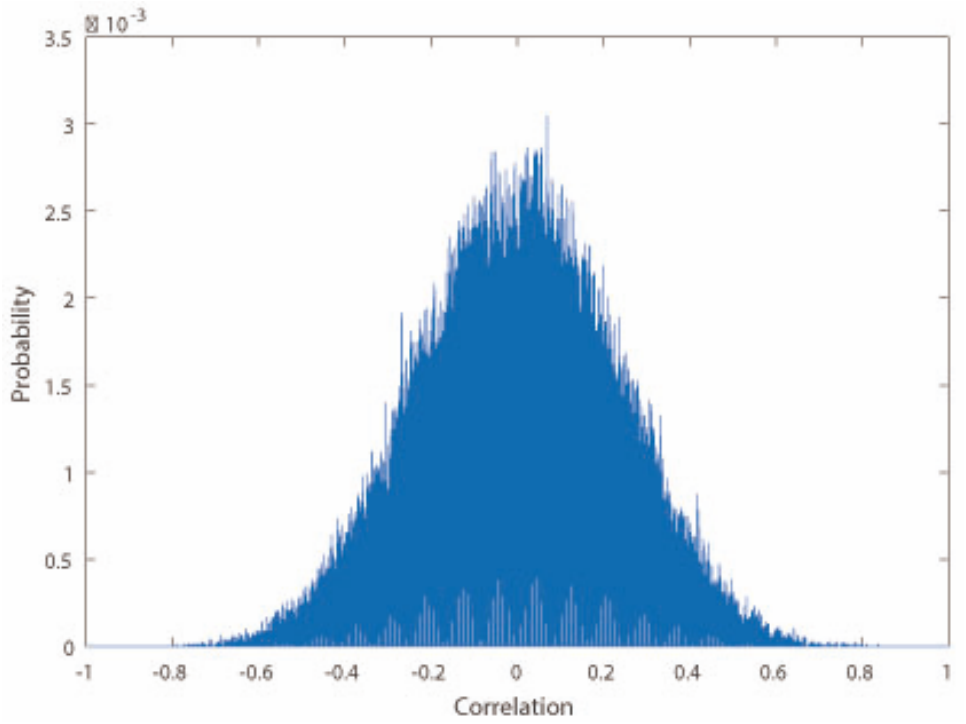

Figure 3.3: Correlation distribution among random permutation matrices.

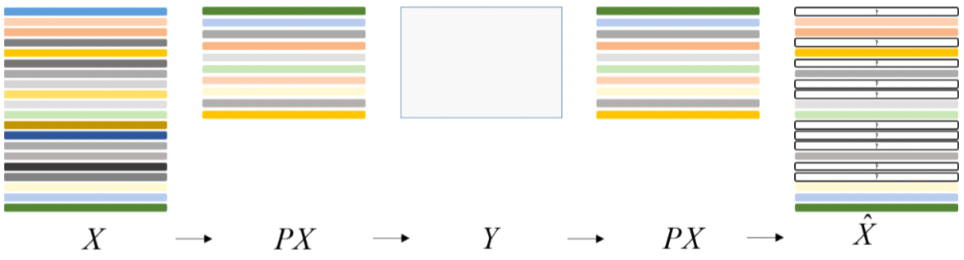

Figure 3.4: Irreversibility of random permutation and row elimination scheme.

3.4 Experiments and Discussion

For evaluation of proposed cancelable biometrics scheme, we exploited the conventional algorithm of iris recognition and a popular iris database (CASIA V3 iris-interval database which consists of 2,639 images in 396 classes of persons. The measure is the normalized hamming distance which assesses 3,471,909 comparisons for inter classes and 8932 comparisons for intra classes. The unwrapped rectangular image size from iris region is 20x240 and Gabor filtered binary biocode is 20x480. In the proposed CB scheme, 10 rows were eliminated out of 20 ones. Figure 3.5 and Figure 3.7 shows the comparison of the distribution of genuine user and imposter after applying the proposed CB algorithm on CASIA V3 database and ND-IRIS-0405 database, respectively. The intra class means the distribution of hamming distances in the same class, and the inter class does the distribution of distances among different classes. Note that the Hamming distances should be small for the intra class, but they should be large in the case of inter classes. When no key is stolen, the distance distributions of intra class are very similar for the proposed CB scheme and the original method where any CB methods are not applied. Considering the Hamming distances become usually smaller by the biosalting methods, the proposed CB scheme preserves the discriminative distances and does not influence on the iris recognition performance. Furthermore, the distances of inter classes becomes larger when the proposed CB scheme, which distinguish the different classes better. These results and distance distributions of proposed CB scheme preserve the original recognition performances without use of biosalting CB methods. And as shown in Figure 3.5 and Figure 3.7, even if the random key and random permutation matrix are stolen at the same time, the inter class distribution is almost same with that of no CB method. Figure 3.8 shows the case where the orthogonal random key is stolen and Figure 3.9 shows the case where the random permutation key is stolen. The both cases supports the proposed algorithm is good at situation where one key is stolen. The receiver operating characteristic (ROC) curve is

shown in Figure 3.6. Genuine acceptance ratio (GAR) is the ratio of correctly matched samples, and is calculated according to FRR. The higher is GAR for the same FAR value, the better is the algorithm. Comparing with some biometric salting algorithms such as BIN-SALT, biohashing (200 bits string), and MRP (200 bits string), the biohashing and MRP are the best, and BIN-SALT and the proposed algorithm also have good GAR performance. However, in the case of stolen key scenarios, the ranking of best algorithms is BIN-SALT, the proposed algorithm, MRP, and biohashing. MRP and biohashing show bad performance when the adversary uses the stolen keys. The wrong projected bio-templates fall to the incorrect classes so they are classified with different classes. If the random key of BIN-SALT is compromised, the distances of trans- formed templates are the same with that of the original templates. Notice that the proposed algorithm has low drop of GAR compared with the original method (no CB applied), which is predicted in 3.11. The more rows in the randomly permutated template are reduced, the more GAR drops, and vice versa. If one of random key or random permutation matrix is stolen, the performance of proposed algorithm is better than the other methods as shown in Figure 3.8 and 3.9. Consequently, the proposed CB scheme catches up with the biosalting algorithms in the normal situation, and is non-invertible in the stolen key situations. To see the objective performance, the equal error rate (EER) of each method on CASIA V3 database is shown in Table 3.1. When the permutation matrix and random key are not stolen, MRP is the best. However, in the stolen key scenario, BIN-SALT has the best EER and the proposed algorithm is the next by 0.7. Even though the proposed CB method is not the best in any cases, it shows uniformly good performance in the normal and stolen situations. This shows that the proposed scheme is proper in any situations in the CB platforms. The proposed CB method shows recognition performance with little differences from those of state-of-the-art algorithms, and has the invertible property in the stolen situations. Table 3.2 and 3.3 show that the EER and verification rate of each method on ND-IRIS-0405 and

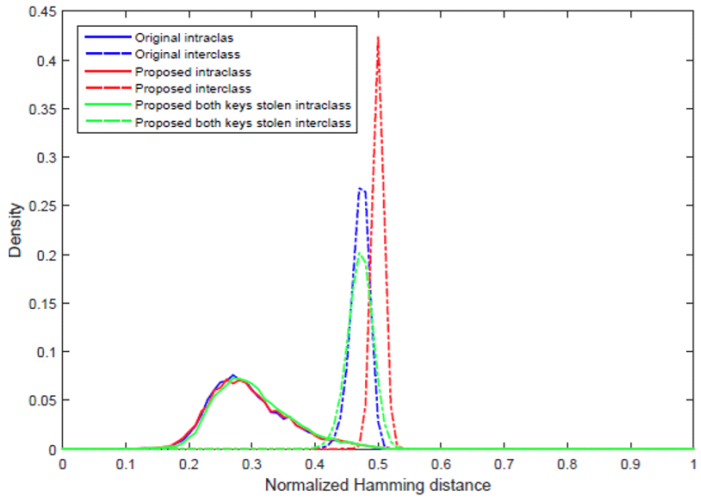

Figure 3.5: Comparison of the distribution between genuine and imposter using hamming distance.

IIT Delhi database, respectively. Their tendency is similar to previous result as shown in Table 3.1.

Finally, to assess the effect of number of eliminated rows, the performance represented by EER versus number of reduced rows is shown in Figure 3.14. Four solid graphs display the proposed scheme performed in each stolen key case, and the dashed line represents EER of original templates at 2.7 EER. There is the tendency that of EER increases as the number of eliminated rows increases. The proposed algorithm without stolen keys has best performance as well as random permutation matrix stolen scenario. Even if the random permutation matrix is compromised, the proposed method shows almost the same performance with the normal state. And the proposed algorithm guarantees the lower EER than the original method until 10 rows are reduced in the random key stolen scenario. In the both keys stolen case, 7 rows are the maximal number of eliminated rows to outperform the original method. These results show that row reduction not only makes non-invertibility but also prevents the performance from dropping seriously.

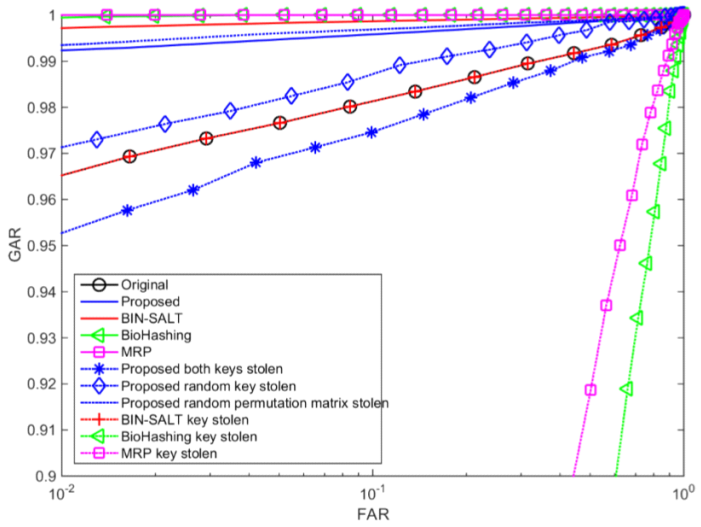

Figure 3.6: Receiver operating characteristics of cancelable biometrics methods.

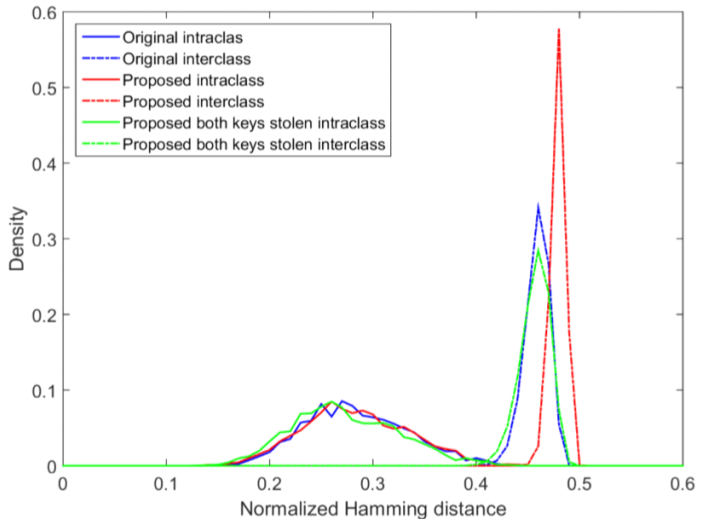

Figure 3.7: Comparison of the distribution between genuine and imposter using hamming distance with both key stolen.

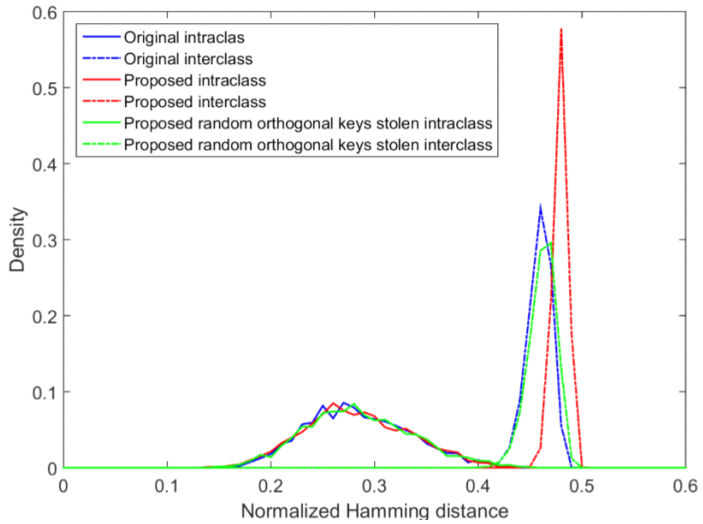

Figure 3.8: Comparison of the distribution between genuine and imposter using hamming distance with orthogonal random key stolen.

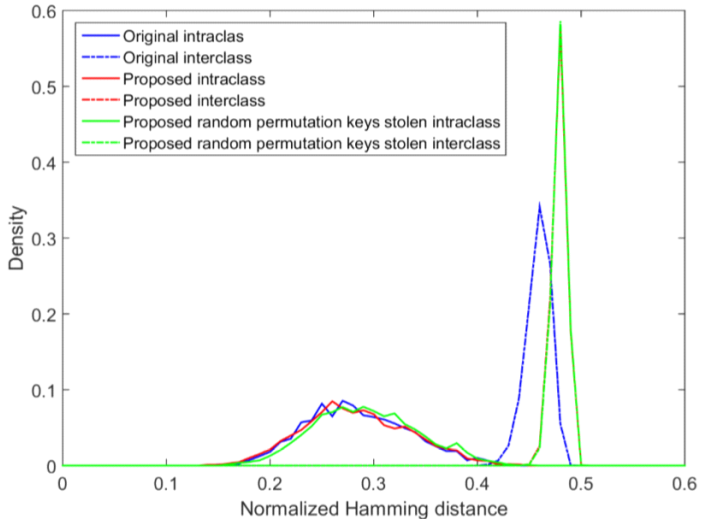

Figure 3.9: Comparison of the distribution between genuine and imposter using hamming distance with random permutation key stolen.

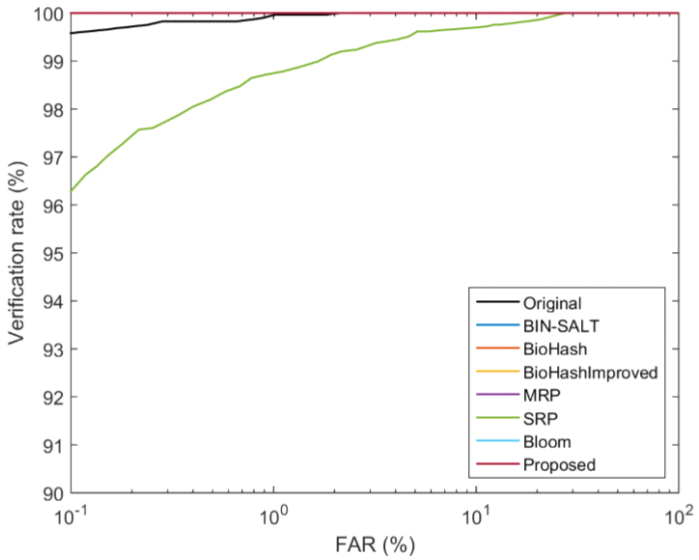

Figure 3.10: Receiver operating characteristics of cancelable biometrics methods on ND-IRIS-0405 database in normal scenario.

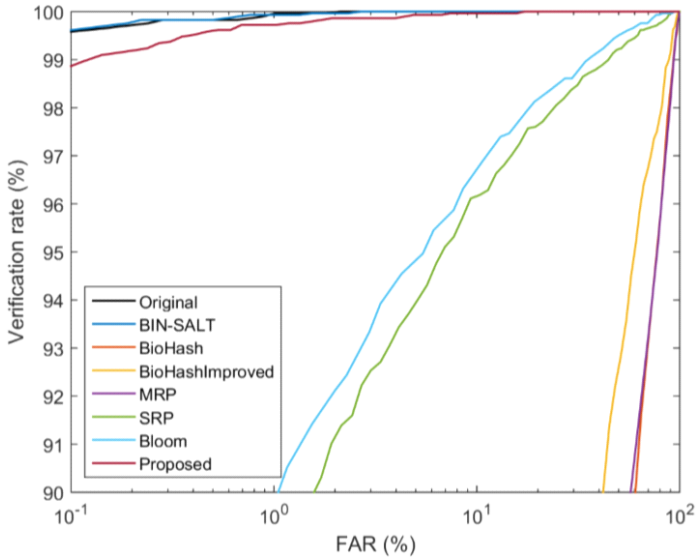

Figure 3.11: Receiver operating characteristics of cancelable biometrics methods on ND-IRIS-0405 databse in stolen key scenario.

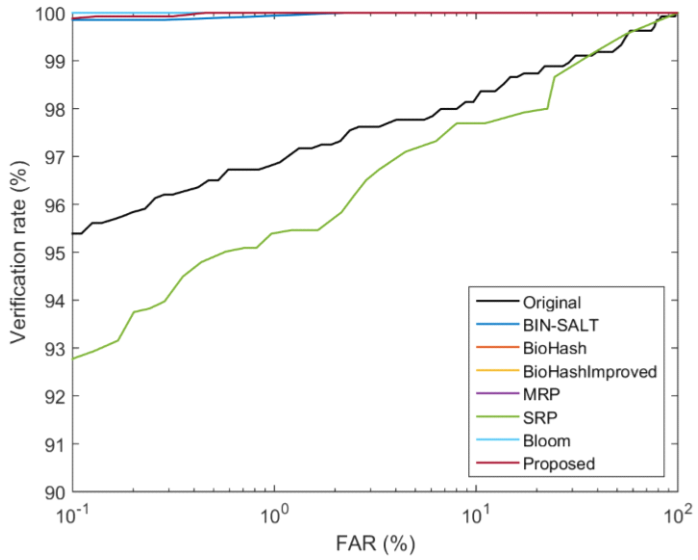

Figure 3.12: Receiver operating characteristics of cancelable biometrics methods on IIT Delhi database in normal scenario.

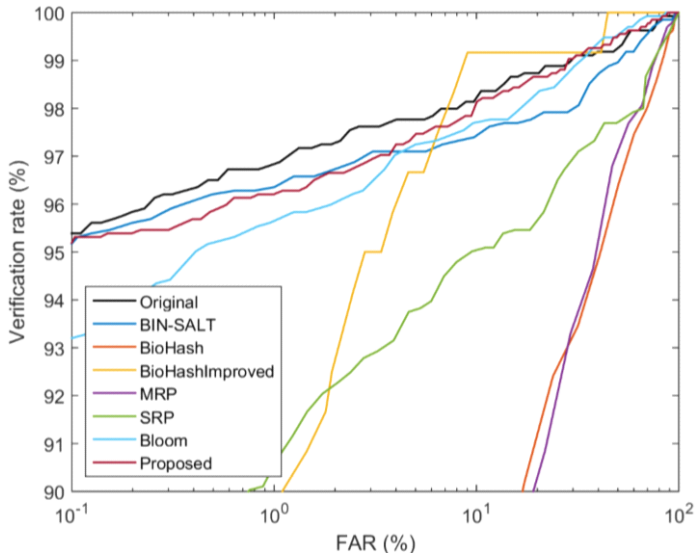

Figure 3.13: Receiver operating characteristics of cancelable biometrics methods on IIT Delhi database in stolen key scenario.

Table 3.1: EER (%) on CASIA V3 database

Method	Normal EER	Stolen Key EER
Original	2.71	N.A.
BIN-SALT	0.37	2.71
BioHashing	0.22	26.70
MRP	0.11	21.45
Proposed	0.76	3.41

Table 3.2: EER (%) and verification rate at 0.1 (%) FAR on ND-IRIS-0405 database

Method	EER		Verification rate	
	Normal	Stolen key	Normal	Stolen key
Original	0.24	N.A.	99.58	N.A.
BIN-SALT	0.00	0.21	100.00	99.62
BioHashing	0.02	26.57	100.00	11.42
BioHashing Improved	0.00	19.57	100.00	32.12
MRP	0.02	25.75	100.00	10.69
SRP	1.19	5.69	96.28	79.06
Bloom Filter	0.00	5.13	100.00	79.55
Proposed	0.00	0.44	99.97	98.02

Table 3.3: EER (%) and verification rate at 0.1 (%) FAR on IIT Delhi database

Method	EER		Verification rate	
	Normal	Stolen key	Normal	Stolen key
Original	2.44	N.A.	95.39	N.A.
BIN-SALT	0.15	2.95	99.85	95.01
BioHashing	0.00	13.90	100.00	48.33
BioHashing Improved	0.00	4.00	100.00	72.50
MRP	0.01	12.93	100.00	51.34
SRP	3.28	6.01	92.71	85.49
Bloom Filter	0.00	3.36	100.00	93.15
Proposed	0.11	3.06	99.93	95.09

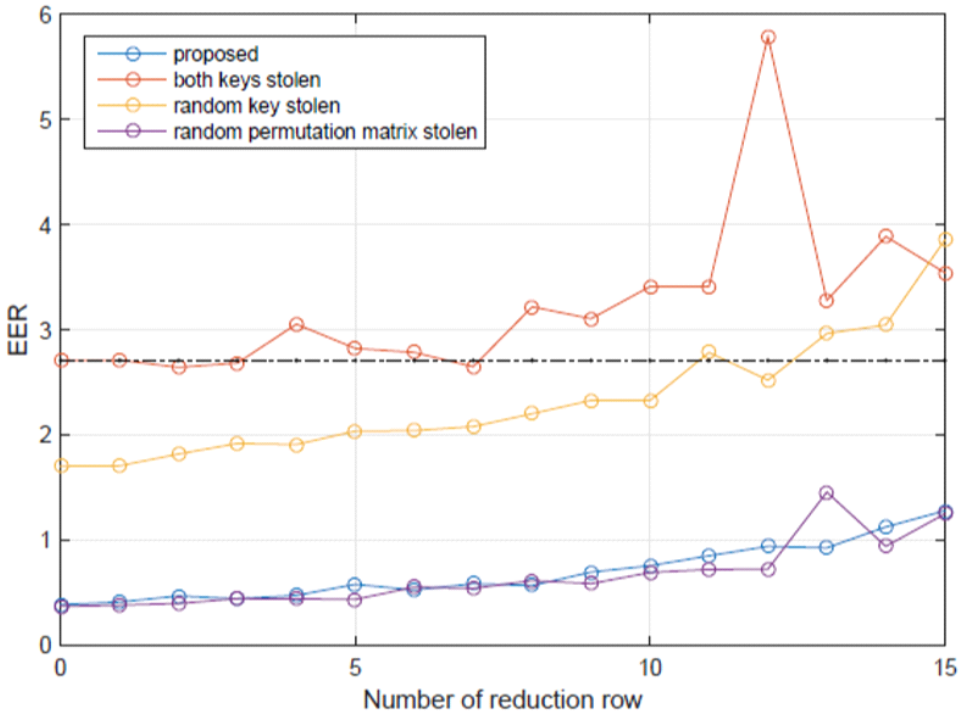

Figure 3.14: EER versus row reduction.

3.5 Conclusion

This dissertation has proposed a novel cancelable biometric scheme RRP-BS for iris recognition system. The proposed CB method consists of random permutation of iris binary template and orthogonal binary salting. The random permutation perturbs the rows of iris template structure and eliminates some rows. This guarantees the non-invertibility of bio-templates. And the relation between error rates and number of eliminated rows is inspected. This dissertation has also proposed the orthogonal binary keys for binary salting, which are generated by Gram-Schmidt orthogonalization. The orthogonality of random binary keys maximizes the Hamming distances of binary salted templates, which preserves the low error rates than the conventional binary salting methods. The proposed method has extensively evaluated the error rates and intra/inter classification to compare with other CB schemes. According to the experiments, the proposed CB scheme has shown good performance in EER, FAR, and FRR. The proposed method does not only guarantee the non-invertibility but also preserves the low error rates in the both normal and key-stolen situations. The proposed CB method is suitable for any biometric systems including mobile phones. Since the individual bio-information is not replaceable unlike the usual passwords, the cancelable biometric schemes are expected to be widely used in the biometric systems.

Chapter 4

CANCELABLE IRIS BIOMETRICS USING NOISE EMBEDDING

4.1 Introduction

The interest in biometrics is more and more increasing, and now there are many mobile phones that use biometric data for many purposes [16]. For example, the fingerprint, face, and iris patterns are the effective biometric information that help to identify and authenticate the individuals. However, if the biometric data are stolen by impostors, then it would raise many serious problems because we cannot change our biometric information. Thus it is desirable that a biometric authentication system does not keep the original data, and moreover does not use the original data for authentication. Instead, the system keeps only non-invertibly transformed or salted data, and uses these data for the recognition. When it is found that these data are stolen, then we can replace the data by using another transform or salting methods, though we need to ask the users to capture the data again. Also, it is desired that the impostors cannot recover the original information from these transformed and/or salted data. This scheme is called cancelable biometric (CB) system, which is becoming important as we use our biometric information for many purposes these days.

In this dissertation, we focus on the iris pattern which is one of the popular biometric features for identifying the individuals [17]. Specifically, Daugman has experimentally proved the effectiveness of iris recognition technology on the large data sets of various nationalities [18]. Although our iris pattern changes as we grow older [19, 20], it undergoes relatively stable changes compared to other biometric traits [21]. Also, the iris pattern can be obtained at a distance, which is an advantage as compared to other features that need contacting sensors like fingerprints [22].

A lots of algorithms have been developed, since Daugman proposed an automated iris recognition method. Specifically, the iris biometric template protection (BTP) systems have attracted attention for its efficiency [9, 14, 23], which define some important conditions that the cancelable iris biometrics (CIB) should satisfy:

- Unlinkability/Diversity: The same cancelable template should not be used in two different applications.
- Reusability/Renewability: If a template or key is compromised, it should be revoked and reproduced readily to generate a new template with a replaced key.
- Irreversibility/Non-invertibility: Complete biometric data should not be reconstructed from the current template, or the reconstruction process should be computationally infeasible.
- Accuracy/Performance: matching score between the templates should not be severely degraded even if compromise event occurs.

The basic structure of CIB schemes is shown in Figure 4.1. When an iris image is captured in the enrollment step, the iris codeword generator transforms it into a binary iris code. Then the CB key, which is generated by personal identification number (PIN), transforms the code to the protected template. In this system, the original iris image and the codeword are not stored. If the CB key is lost, the user needs to capture the image again, and replace the old template with a new one using a new key. Note

that the new template should not be correlated with the old one to satisfy the unlinkability. In the authentication step, the protected template in the database is compared with the current query transformed with the CB key. Then, it is determined by a certain measure whether the templates are the same or not.

The conventional CB approaches attempt to satisfy above stated conditions by designing a non-invertible transform and using the transformed data, or by salting the data, i.e., injecting random signals generated by user-specific keys. The principle of transform design or salting method is to keep the discriminability of templates while minimizing the possibility of recovering the original template from the transformed and/or salted data. In this dissertation, we propose a new CIB method that combines the advantages of biometric salting with non-invertible transform methods. For biometric salting, we use performance-oriented reduced random permutation and binary salting (RRP-BS) technique, which satisfies unlinkability. Also, Hadamard product and noise embedding method are introduced, which are designed to satisfy the non-invertibility. The noise embedding is applied to non-coherent matching regions obtained from some enrollment templates, so that it is robust against known threats.

The rest of this chapter is organized as follows. Section 4.2 summarizes the related works on CB systems. Section 4.3 describes some of the underlying concepts for biometric salting. In Section 4.4, the proposed method is explained. Section 4.5 presents the experimental results that compare the proposed algorithm, and security analysis is presented in section 4.6. Finally, this chapter is concluded in Section 4.7.

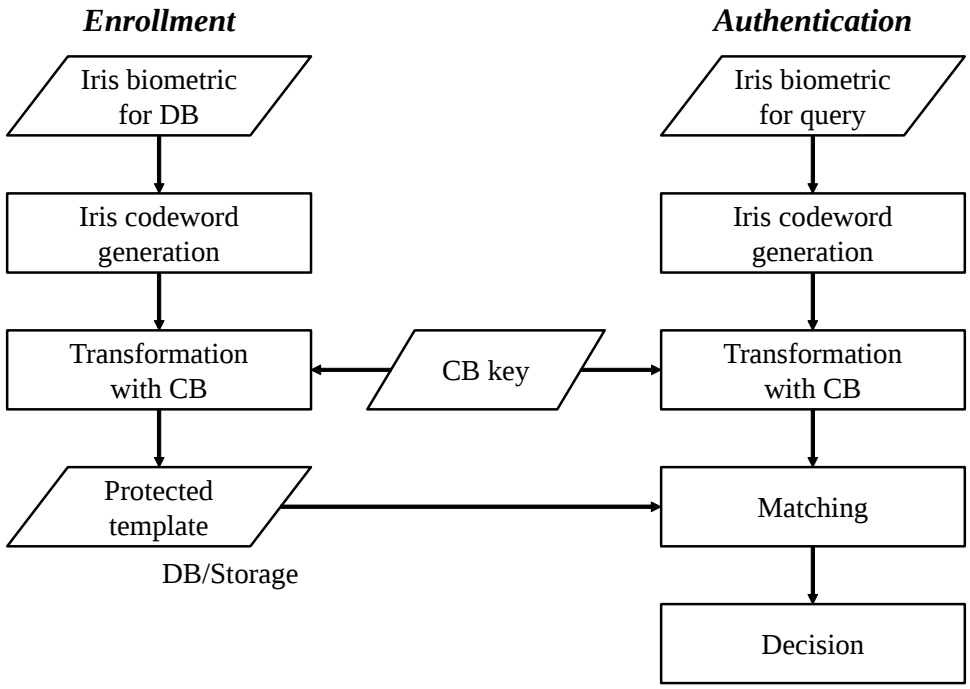

Figure 4.1: Cancelable biometric structure of iris information.

4.2 Related Works

As described above, there are two main approaches to enabling the non-invertibility. One is to apply a non-invertible transform to the original data and the other is to insert random data, i.e., biometric salting.

4.2.1 Non-Invertible Transform Approaches

The main objective of these approaches is to design a non-invertible transform that ensures that the original biometric cannot be reconstructed from the transformed data. These methods usually make the template data partially unavailable or make it computationally difficult to retrieve the original data. Since most of these algorithms are focused on the non-invertibility, the discriminating capability of the transformed template becomes lower than the original.

For some specific examples of non-invertible transform approaches, Ratha *et al.* proposed three non-invertible transforms for the cancelable fingerprint authentication such as polar, Cartesian and surface folding [4]. These transforms distort the fingerprint image or permute the image blocks for the non-invertibility, but they lead to low discriminability between the genuine and impostors if they are compromised. Zuo *et al.* proposed a method based on the row shift and combinations to generate iris templates [5]. Since the partial templates are dropped in this process for reducing the computational loads, the method is sensitive to the eye boundary environment such as eyelids and eyelashes. Hämmerle-Uhl *et al.* proposed a block re-mapping and image warping method for CIB [6], where the re-mapping process eliminates some blocks by overlapping. However, for keeping the discriminating performance similar to the original, the number of redundant blocks must be small, which may cause security problems. According to [24], 60% of blocks can be restored from the re-mapped and distorted template even if 10% blocks are left. Dwivedi *et al.* proposed a CIB scheme based on a lookup table (LUT) [25]. The LUT is created by random variables that can be 0 or

1 with the same probability, and a consistent row vector consisted of robust components indexes the LUT to create a template. However, if all parameters and database templates are stolen, it is relatively easy to deduce a consistent vector. Besides, since the vector was created in the original domain, it is possible to reconstruct the original biometric data from the stolen consistent vector. Rathgeb *et al.* introduced bloom filters to the CB systems [26]. The bloom filter is a binary vector that is initialized to zero at first. The original binary data is divided into several blocks with one bloom filter per block. The column vectors of the block are converted to the decimal number used for the index, and the value of bloom filter index position is changed to one. This method satisfies non-invertibility with acceptable performance degradation, but has the disadvantage of not meeting unlinkability [27]. In [1], a processing step called structure-preserving feature re-arrangement is proposed for compensating the unlinkability of bloom filter approach. The indexing-first-one (IFO) hashing was proposed by Lai *et al.* [28]. This algorithm is based on min-hashing which estimates how similar the two sets are. Given a binary input, the hash value of the IFO hashing is the location of the first one encountered. They used the fact that the discriminability increases for each class if the hash value is repeatedly obtained. They also introduced Hadamard product and modulo thresholding to enhance the non-invertibility. The performance of the IFO hashing is the state-of-the-art, and the non-invertibility and unlinkability are satisfactory.

4.2.2 Biometric Salting Approaches

Biometric salting means that the biometric data are blended with auxiliary data such as user specific random keys. The independence of keys ensures the discriminability and also satisfies the unlinkability. These approaches use user-specific keys which are revocable and regenerated when compromised. However, the transformations used in these algorithms are approximately invertible if the keys are known.

The main research in biometric salting is focused on biohashing and its variation. Jin *et al.* introduced biohashing to generate secure biocode template [7]. The orthogonal user-specific random matrix as a key is constructed by tokenized random number (TRN) and combined with biometric features. The random key maximizes the distinctiveness between different users while minimizing the distances among the same user templates. However, the biohashing has critical problem that the coarse approximation of original biometric data is possible with the stolen keys. Teoh *et al.* proposed multiple random projection (MRP) onto non-invertible random subspace [8, 9]. MRP protects the original biometric data excellently, but it has some weakness when the impostors steal the random projection keys. To mitigate the effect of some outliers in the image that affect the recognition performance such as specular reflections, eyelash and eyelids, Pillai *et al.* introduced a sectored random projection (SRP) method, where they handled different qualities in each partial iris region [29, 30]. This method divides the iris into sectored regions and applies random projections separately to each sector followed by concatenating the transformed vectors [29]. Also, the hash table which has permuted sector index is adopted for cancelable template [30]. The performance of this algorithm is better than that of conventional biohashing based methods. However if the processing schemes are known to impostors, the security performance is deteriorated as is the same cases with MRP. Zuo *et al.* proposed basic salting algorithms such as GRAY-SALT and BIN-SALT that blend random matrix with biocodes [5]. The salting methods show good performance, and BIN-SALT is specifically robust in the case of stolen token scenario. But it has a disadvantage that the original biocodes can be completely reconstructed when the random keys are exposed. Savvides *et al.* proposed the idea to encrypt biometric template using random convolution kernel and minimum average correlation energy (MACE) filter [10]. They proved that the training image convolution before building the MACE filter does not change the correlation so that the authentication performance is preserved. But it is vulnerable in the case that the

random kernel is known. More detailed and various reviews of CB are introduced in many literatures [11, 12, 13].

4.3 Preliminaries

In this section, we explain the details of binary salting (BS) and its extension which are exploited in our algorithm.

4.3.1 Binary Salting

Suppose that an original binary iris code of $M \times N$ matrix $X \in \{0,1\}^{M \times N}$ where M and N are respectively the number of rows and columns. The binary code X is usually generated by Gabor filtering to the unwrapped iris region followed by quantization. Then the BS algorithm is described as

$$Y = S \oplus X, \tag{4.1}$$

where S is an $M \times N$ random key matrix with binary elements, the operator $\oplus$ is the elementwise logical exclusive-OR, and Y is the transformed template. The BS is a very simple yet effective method which can be used for legacy systems and has no trouble with outlier amplification [5, 12]. Also, it fulfills three conditions of a CB system described in Section 4.1 [9, 14, 15]. Since the randomly generated keys are not correlated with each other, the diversity is satisfied *i.e.,* we can use different keys for other devices or systems. In addition, the keys can be easily replaced, satisfying the renewability condition. Because the normalized Hamming distance (NHD) is generally used for matching the binary templates, the accuracy can be easily proved and even if the key is stolen the performance is the same as that of the original. However, note that when both of random key S and the protected template Y are compromised, then the original iris code X can be completely recovered, which is a disadvantage of salting method.

4.3.2 Reduced Random Permutation

The security of BS algorithm can be enhanced by using reduced random permutation (RRP), which is referred to as RRP-BS. Let $P \in \{0, 1\}$ be an $h \times M$ permutation matrix with $h < M$ where h is a row control parameter that decides to keep some rows and to drop the others. The P has only one 1 in each row, and does not have the same rows. The RRP-BS is described as

$$Y = S \oplus PX, \tag{4.2}$$

where S now is an $h \times N$ salting matrix, and the result Y is the $h \times N$ matrix which is smaller than the original BS. This method improves the security by changing the order of rows of X and removing some of them. Specifically, only partial original information can be recovered even when the impostors stole the salting parameters.

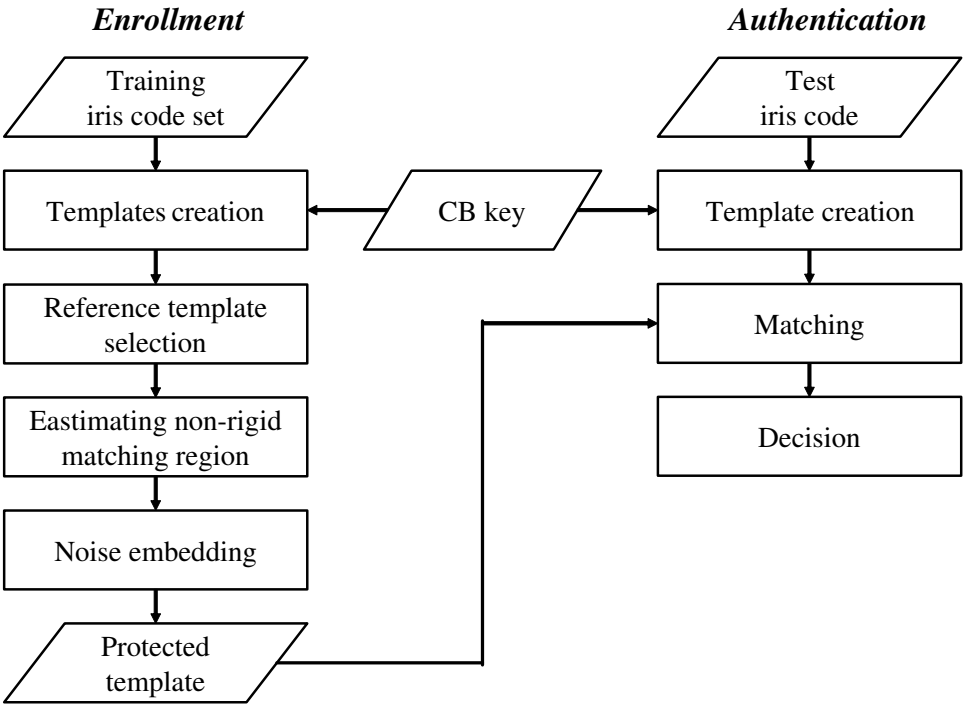

Figure 4.2: Proposed CIB system.

4.4 Proposed CIB System

The overall schematic diagram of the proposed algorithm is shown in Figure 4.2. We explain the main steps of the algorithm in this section.

4.4.1 Template Creation

The overall template creation algorithm is shown in Fig. 4.3. The authentication system takes several images (training data), and generates a set of iris codes $\{X_1, X_2, \cdots\}$ by a conventional method. Then each iris code X_i is converted to a template Z_i through the three processes: RRP-BS, Hadamard product, and decimal encoding as described in the figure. The RRP-BS is adopted for discriminability as explained in Section 4.3.2, Hadamard product is used for non-invertibility, and the decimal encoding is performed

for generating a row template and block matching of binary codes. We repeat three processes r times to vertically aggregate row templates (W_{ir}) as shown in Fig. 4.3. Since the discriminability is proportional to the size of template, larger r better ensures the discriminability. Also, we use several training iris codes to generate the non-coherent matching map, which will be explained in the following subsection.

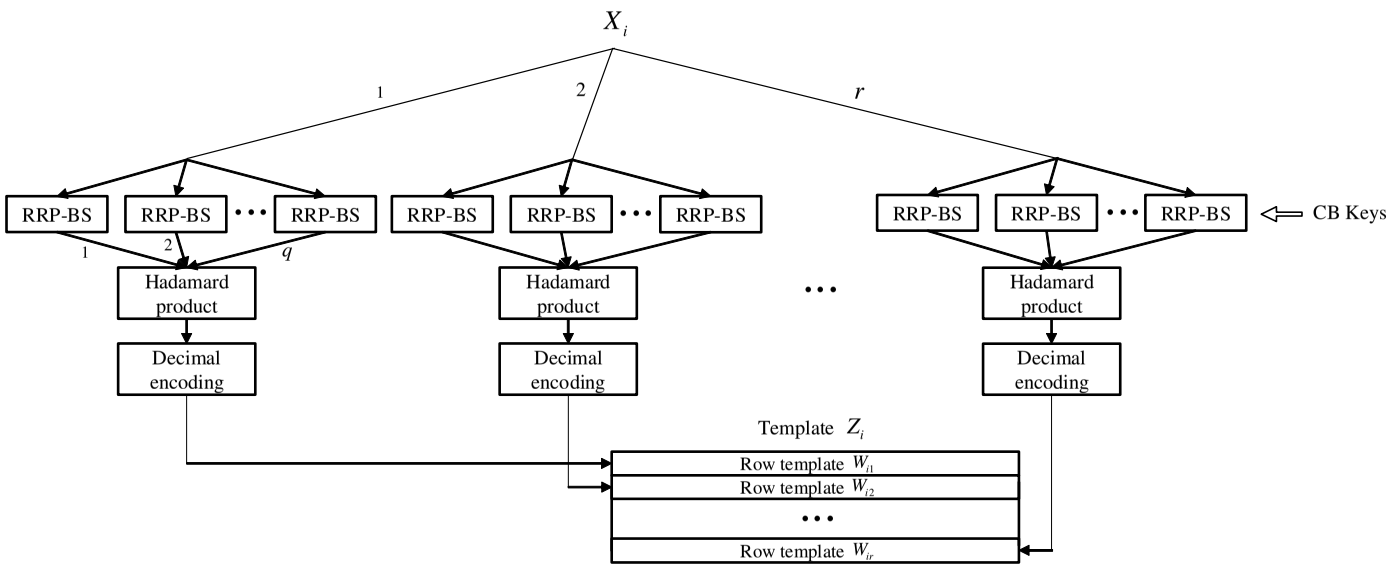

Figure 4.3: Template creation process of the proposed CIB system.

To be more precise with the first process, i.e., RRP-BS, let N_E be the number of training images per class, where the "class" here means either of left or right eye of a user. Then we have a set of binary iris codes $\{X_i,\ i = 1, ..., N_E\}$ for a class. For each X_i, we repeat the RRP-BS code generation in eq. (4.2) $r \times q$ times, i.e., we obtain the BS codes

$$Y_{ijk} = S_{ijk} \oplus P_{ijk} X_i, \tag{4.3}$$

for $j = 1, \cdots, r$, and $k = 1, \cdots, q$, where r is the height of a template and q is the order of the Hadamard product. In this process, notice that S_{ijk} and P_{ijk} act as CB keys as in eq. (4.2).

The second process is the Hadamard product of order q, which is the logical AND operation of RRP-BS codes as

$$\tilde{Y}_{ij} = \prod_{k=1}^{q} Y_{ijk}. \tag{4.4}$$

In general, each element of X_i is a binary random variable that is 0 or 1 with equal probability, and so is the element of Y_{ijk}. Applying the Hadamard product reduces the number of 1's to $hN(1/2)^q$ and thus enhances non-invertibility.

As stated above the S_{ijk} and P_{ijk} are CB keys that play important roles in BS algorithms, which need to be carefully designed. In this scheme, if the CB keys S_{ijk} and P_{ijk} are stolen, and also if the m-th row of P_{ijk} is equal to that of P_{ijl} for any pair of (k, l) with $k \neq l$, it is likely that the m-th row of Y_{ij} becomes invertible. As a result, the corresponding rows of X_i might be reconstructed with high probability. Hence, when designing P_{ijk} it is important that the same rows of $\{P_{ij1}, \cdots, P_{ijq}\}$ are different.

For generating the permutation matrices with this property, we indirectly generate a permutation sequence $D_k(n)$ that correspond to the perputation matrix P_{ijk}. Specifically, $D_k(n)$ is an integer sequence which denotes that the n-th row of P_{ijk} has 1 at the $D_k(n)$-th position and 0 in the rest. Notice that the length of $D_k(n)$ is h, and an

element $D_k(n)$ can have the value from 1 to M. Also, $D_k(n)$ should be different from that of $D_l(n)$, for $l \neq k$. For generating such D_k, we first prepare a set of integers $A = \{1, \ldots, M\}$, and define a subset $B_1 \subset A$, with h elements randomly selected from A. Then, h out of $M - h$ elements of A are again taken to make a subset B_2, and the elements of B_2 are also excluded from A. This process is repeated q times to obtain B_q. However, if the number of remaining elements becomes less than h when making the k-th subset B_k, then we put all the remaining elements of A to C and assign $\{1, \ldots, M\}$ to A again. Then we extract $h - |C|$ from $A \setminus C$ and assign it to B_k with all the elements of C. Then, the elements of the sequence D_k are just the shuffled elements of B_k, where shuffling is needed to ensure that $D_k(n) \neq D_l(n)$ for $l \neq k$. The pseudo code for generating the RRP matrix is shown in Algorithm 1. This method makes the histogram of the number of selections from 1 to M evenly distributed, and raises the information entropy by having all different values for each row of $\{P_{ij1}, \ldots, P_{ijq}\}$.

The third process is to convert the Hadamard product to a decimal number. The result of the first and second processes is Y_{ij} in eq. (4.4), which can also be expressed as

$$\tilde{Y}_{ij} = [\tilde{y}_{ij1} \cdots \tilde{y}_{ijN}] \tag{4.5}$$

where $\tilde{y}_{ijk}$ is an $h \times 1$ binary vector. The third step is to convert this binary vector into a decimal number. Specifically, we define a mapping function $f : \{0,1\}^{h \times 1} \to \mathbb{N}_{\not\vdash}$, which converts the Hadamard product result $\tilde{Y}_{ij}$ into a $1 \times N$ row vector W_{ij} with decimal elements as follows:

$$W_{ij} = [f(\tilde{y}_{ij1}) \cdots f(\tilde{y}_{ijN})]. \tag{4.6}$$

The above steps are repeated r times and we obtain a final template for X_i as follows:

$$Z_i = [W_{i1}^T \cdots W_{ir}^T]^T. \tag{4.7}$$

Algorithm 1 Generation of RRP Matrix

Input: M: template height, h: the number of rows of P_{ijk}, q: the order of Hadamard product

Initialisation : $\mathcal{A} \leftarrow \{1, \ldots, M\}$, $\mathcal{B}_k \leftarrow \emptyset, k = 1, \ldots, q$

1: **for** $k = 1$ to q **do**
2: **if** $|\mathcal{A}| \geq h$ **then**
3: $\mathcal{B}_k \leftarrow$ randomly chosen h elements from $\mathcal{A}$
4: **else**
5: $\mathcal{C} \leftarrow \mathcal{A}$
6: $\mathcal{A} \leftarrow \{1, \ldots, M\}$
7: $\mathcal{B}_k \leftarrow \mathcal{C}$ and randomly chosen $h - |\mathcal{C}|$ elements from $\mathcal{A} \setminus \mathcal{C}$
8: **end if**
9: $\mathcal{A} \leftarrow \mathcal{A} \setminus \mathcal{B}_k$
10: **end for**
11: Get a random permutation sequence D_k from each $\mathcal{B}_k$ such that $D_k(x) \neq D_l(x)$ for all $l, l \neq k$
12: Construct each permutation matrix P_{ijk} using D_k

Output: $\{P_{ij1}, \ldots, P_{ijq}\}$: a set of RRP matrix

Then, for each of the enrolled iris codes X_i, $i = 1, \cdots, N_E$, we have the protected template set $\mathcal{Z} = \{Z_1, \ldots, Z_{N_E}\}$.

4.4.2 Reference Template Selection

From the set of templates $\mathcal{Z}$ that represents a class, we find a region that all the templates have similar properties, which is called coherent region. To be precise, the templates are from several images of an eye of a person (class) which are individually different due to closure of eyelid, gaze, etc. But these also have some common regions around the pupil which are important regions for the robust iris recognition. These common regions of iris images correspond to the coherent region of the templates. For obtaining the coherent region, we first define a reference template $\tilde{Z}$ among the elements of $\mathcal{Z}$, which has the least sum of distances to other elements as

$$\hat{Z} = \underset{Z_i \in \mathcal{Z}}{\operatorname{argmin}} \sum_{Z_j \in \mathcal{Z} \setminus Z_i} dist(Z_i, Z_j) \tag{4.8}$$

where the distance $dist(Z_i, Z_j)$ is actually a dissimilarity measure defined by

$$dist(Z_i, Z_j) = 1 - \frac{\|B_{Z_i, Z_j} \wedge B_{Z_i} \wedge B_{Z_j}\|_0}{\|B_{Z_i} \wedge B_{Z_j}\|_0} \tag{4.9}$$

where B_{Z_i} is a binary matrix whose entry is 1 if Z_i is a positive or 0 otherwise, B_{Z_i, Z_j} is a binary matrix with the value of 1 if the entry of Z_i is equal to Z_j, or 0 otherwise, $\|\cdot\|_0$ is the number of non-zero entry in a matrix and $\wedge$ is the entrywise logical AND operation. The dissimilarity measure is a variation of the similarity measure used in [28] and is related to Jaccard similarity.

4.4.3 Finding Coherent and Non-Coherent Matching Region

We examine the same value among the positive values between the reference template $\tilde{Z}$ and the others Z_j. A binary map that shows whether the values are equal is called a

coherent matching map $B_{coherent}$ defined as

$$B_{\text{coherent}} = \bigvee_{Z_j \in \mathcal{Z} \setminus \hat{Z}} (B_{\hat{Z},Z_j} \wedge B_{\hat{Z}} \wedge B_{Z_j}) \tag{4.10}$$

where $\bigvee$ is the entrywise logical OR operation. Since the coherent matching region is the best matching area for the training data in the same class, we can infer that the region will also be well matched with the test data for the same class. Conversely, even if a random signal is injected into the non-coherent matching region, the score can be expected to be almost the same. The non-coherent matching map $B_{\text{non-coherent}}$ is expressed as $B_{\text{non-coherent}} = \neg B_{\text{coherent}}$ where $\neg$ is the entrywise logical negation operator.

4.4.4 Noise Embedding

Since the non-coherent matching region has quite different code values for each iris code in a class, adding an arbitrary value in this region does not greatly affect the matching result. Since the entries in Z_i are the decimal numbers converted from the h bit vector y_{ijk} in (4.5), we embed arbitrary decimal numbers with the same distribution to the non-coherent matching region. As mentioned above, since the number of 1's of Y_{ij}, which is the result of Hadamard product, is $hN(1/2)^q$, the probability of 1 per bit is $(1/2)^q$. Let G be an h bit vector whose entry g_i is a random variable with Bernoulli distribution and the probability mass function of g_i is expressed as $\Pr(g_i = 1) = (1/2)^q$ and $\Pr(g_i = 0) = 1 - (1/2)^q$. Then, the noise-embedded protection template T is defined as

$$T(m,n) = \begin{cases} f(G) & \text{if } (m,n) \in \mathcal{R}_{\text{non-coherent}} \\ Z_i(m,n) & \text{otherwise} \end{cases} \tag{4.11}$$

where $\mathcal{R}_{\text{non-coherent}}$ is the set of non-coherent matching position (m,n) such that non coherent binary map $B_{\text{non-coherent}}(m,n) = 1$ for $m = 1,\ldots,r$, $n = 1,\ldots,N$. Since T is an $r \times N$ decimal matrix and each entry uses h bits, the size of $h \times r \times N$ bits is needed

to store one template. For example, let the original iris code be an $M \times N = 20 \times 512$ matrix. If $h = 4$ and $r = 12$, then $24,576$ bits $= 24$ kbits are required, which is 2.4 times the original size. Although the final template T is larger than the original, it is reasonable to embed the noise so as to maintain good performance and to prevent inversion.

4.4.5 Modifications for Alignment

The iris matching method genrally includes successive shift matching process considering the iris mis-alignment. It means that when measuring the distance between the templates Z_i and Z_j, one of them is circularly shifted left and right by the maximum of 16 to select the smallest value among the matching scores. Using this fact, (4.8) is changed as

$$\hat{Z} = \underset{Z_i \in \mathcal{Z}}{\operatorname{argmin}} \sum_{Z_j \in \mathcal{Z} \setminus Z_i} \left[\min_{U \in H_{Z_j}} dist(Z_i, U) \right] \tag{4.12}$$

where H_{Z_j} is a set of circularly shifted templates of Z_j from left to right, and (4.10) is reformulated as

$$B_{\text{coherent}} = \bigvee_{Z_j \in \mathcal{Z} \setminus \hat{Z}} (B_{\hat{Z}, K_{\hat{Z}, Z_j}} \wedge B_{\hat{Z}} \wedge B_{K_{\hat{Z}, Z_j}}) \tag{4.13}$$

where $K_{\hat{Z}, Z_j}$ is the aligned template of Z_j based on $\hat{Z}$ so that the distance between $\hat{Z}$ and Z_j is the minimum score as follows,

$$K_{\hat{Z}, Z_j} = \underset{U \in H_{Z_j}}{\operatorname{argmin}} dist(\hat{Z}, U). \tag{4.14}$$

The proposed CIB system is summarized as Algorithm 2 .

4.4.6 Authentication

The authentication step is similar to the template creation process of the enrollment step. Given a test iris code X_t, the test template Z_t is created by (4.7), and it is com-

Algorithm 2 Enrollment Algorithm for Proposed CIB

Input: $\{X_1, \ldots, X_{N_E}\}$: a set of training templates, h: the number of rows of a RRP matrix, r: the number of iterations, q: the order of Hadamard product

Initialisation :

for $i = 1$ to N_E **do**
  for $j = 1$ to r **do**
    Generation of a set of RRP matrix $\{P_{ij1}, \ldots, P_{ijq}\}$ in Algorithm 1 and BS matrix $\{S_{ij1}, \ldots, S_{ijq}\}$
    for $k = 1$ to q **do**
      RRP-BS algorithm in (4.3)
    end for
    Calculate q-order Hadamard product in (4.4)
    Convert each binary vector to decimal number in (4.6)
  end for
end for
Find the protected template $\hat{Z}$ with having the minimum distance from the others in (4.12)
Get coherent matching map in (4.13)
Change the non-coherent matching region of the protected template $\hat{Z}$ as putting a noise in (4.11)

Output: T: an $r \times N$ protected decimal template

pared with the protected template T of the database. Since the iris rotation is considered in comparison, the minimum score is calculated by a successive shift matching process as $\text{Score}_{min} = \min_{U \in H_{Z_t}} dist(T, U)$. If the score is smaller than the criterion, it is authenticated, otherwise rejected.

4.4.7 Differences with IFO hashing

This section compares the proposed algorithm with the state-of-the-art IFO hashing. Inspired by min hashing, the IFO hashing enhances non-invertibility through Hadamard product and modulo thresholding. Also, the iteratively obtained hash values, which is called iterative hash growth (IHG), improve the accuracy performance. Our method is similar to the IFO hashing method in that it performs Hadamard product and iterative enhancement of iris code. However, the IFO hashing is based on min hashing, while our method is based on the RRP-BS. Min hashing balances the performance and security through IHG. On the other hand, the RRP-BS method is superior in terms of performance but it is supplemented by iterative template (hash) growth and noise embedding because of its security weakness. Since noise embedding increases the coherence using several samples, it provides better privacy than the IFO hashing that uses only one sample.

4.5 Experiments and Discussion

4.5.1 Experimental Databases

For the evaluation, we test our algorithm with popular iris databases such as CASIA V3 iris-interval[1], IIT Delhi iris[2][31], and ND-iris-0405 database[3][32]. Since the performance depends on the iris recognition algorithm, we experiment with the algorithm that shows the best recognition rate for each database.

CASIA V3 iris-interval database

The CASIA V3 iris database consists of 2,639 images of 320×280 pixels from 395 classes. They were captured with a close-up infrared iris camera in an indoor environment. By using the circular NIR LED array, they have very clear iris texture details and hence widely used [6],[33],[34],[28]. We also try to follow the experiment methods in the conventional works, i.e., we use 868 images from 124 classes where each class has 4 enrollment images and 3 test images [28]. We use the weighted adaptive Hough and ellipsopolar transforms of the USIT v2.1.0 program to divide the iris region into a rectangle of 512×64 size. The generated iris texture image is transformed into 512×10 size as in [26], with the bottom 14 rows removed and the 5 adjacent row pixels averaged. Then, the 1-D log Gabor filter is applied to vertically stack the real signal and the imaginary signal to generate a 512×20 iris code.

IIT Delhi iris database

This database version 1 has been acquired in Biometrics Research Laboratory in 2007 using JIRIS, JPC1000, digital CMOS camera. The resolution of these images is 320×240 pixels and all the images were acquired in the indoor environment. The database

[1] http://biometrics.idealtest.org

[2] `http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm`

[3] `https://sites.google.com/a/nd.edu/public-cvrl/data-sets`

consists of 1,200 images from 224 persons aged 14-55 years, consisting of 176 men and 48 women. So there are 5 images per class, 3 for enrollment and 2 for authentication. The iris region is divided through the Osiris program and the iris code of size 256×20 is generated by the 1-D log Gabor filter [35].

ND-iris-0405 database

This dataset was acquired in 2004-2005 at Notre Dame with LG 2200 iris image camera. It has about 65,000 iris images in a diverse and challenging environment of size 640x480 from 712 classes obtained from 356 people. We select only 15 clean samples in 80 classes to avoid environmental degradation due to eyelids, eyelashes, and specular reflections, and collect a total of 1200 samples. Among the 15 samples, 10 are used for enrollment images and 5 as authentication images. To divide and encode the iris region, the Masek algorithm was used to create a 240×20 iris code [36].

4.5.2 Scores for evaluation

In order to evaluate the performance change in various situations, four scores are measured such as genuine (GE), imposter (IM), pseudo genuine 1 (PG1), and pseudo genuine 2 (PG2). We first create the templates using different key for each class, and the GE is referred to as the score between the templates of the same class, and the IM is referred to as the score between the templates of different classes. Next, we create templates that use the same key for all classes, and the PG1 is referred to as the score between distinct classes. Finally, we refer to PG 2 as the score obtained by comparing one template with 50 templates after generating templates using 51 different keys for an iris code of each class.

GE is the benchmark for comparing three different score distributions, and we produce three performance results such as GE-IM, GE-PG1, and GE-PG2. The GE-IM refers to the performance of the algorithm in normal situations, the GE-PG1 shows

Table 4.1: EER Performance According to the Number of Rows of an RRP Matrix (h) and Hadamard Order (q) with $r = 12$.

Database	q	EER (%)						
		$h = 4$	$h = 6$	$h = 8$	$h = 10$	$h = 12$	$h = 14$	$h = 16$
CASIA V3 iris-interval	2	0.08	0.27	0.17	0.62	1.08	1.36	1.08
	3	0.48	0.27	0.27	0.27	0.81	0.27	1.08
	4	0.54	0.54	0.27	0.54	0.49	0.41	0.81
	5	0.81	1.08	0.54	0.27	0.40	0.67	0.54
IIT Delhi	2	0.66	0.89	1.56	1.12	1.56	1.41	2.14
	3	0.89	1.12	0.89	0.45	0.67	0.89	1.09
	4	2.01	1.34	1.12	1.34	1.34	0.89	1.12
	5	3.04	2.01	1.65	0.90	1.34	1.79	1.34
ND-IRIS-0405	2	0.00	0.00	0.00	0.20	0.00	0.02	0.39
	3	0.25	0.00	0.00	0.00	0.00	0.00	0.25
	4	0.25	0.02	0.01	0.04	0.00	0.05	0.00
	5	1.50	0.25	0.25	0.06	0.25	0.25	0.05

how much the performance is degraded compared to the GE-IM when a user's keys are stolen, and the GE-PG2 shows how different templates are generated in the situation when one iris is used in multiple devices using different keys. All the performances are expressed in terms of the equal error rate (EER), which means that the false accept rate (FAR) and the false reject rate (FRR) are equal.

Table 4.2: EER Performance According to the Number of Iteration (r) with some h values and $q = 3$.

Database	h	EER (%)						
		$r = 1$	$r = 4$	$r = 8$	$r = 12$	$r = 16$	$r = 20$	$r = 25$
CASIA V3	4	2.15	0.54	0.54	0.48	0.27	0.01	0.07
iris-interval	8	2.33	0.81	0.28	0.27	0.27	0.27	0.01
	12	3.23	1.08	0.54	0.81	0.27	0.54	0.27
	16	4.04	1.08	1.08	1.08	0.68	0.54	0.27
IIT Delhi	4	6.47	2.01	1.56	0.89	0.89	0.67	0.67
	8	4.69	1.79	1.34	0.89	0.67	0.89	0.45
	12	6.25	2.71	1.51	0.67	1.12	0.88	1.04
	16	6.92	2.68	1.7	1.09	0.9	1.12	0.7
ND-IRIS-	4	9.34	0.62	0.50	0.25	0.22	0.00	0.00
0405	8	3.45	0.50	0.00	0.00	0.00	0.00	0.00
	12	4.11	0.55	0.00	0.00	0.00	0.00	0.00
	16	6.15	0.65	0.25	0.25	0.00	0.00	0.00

4.5.3 Effect of parameters

In order to satisfy the conditions for the BTP system, the proposed algorithm uses three tuning parameters such as h, r and q. We fix one parameter and evaluate the performance change according to the other two parameters.

Table 4.1 shows the performance according to h and q for fixed $r = 12$. As q increases by 1, the number of valid 1's for matching is reduced by the power of $1/2$,

so we experiment with the algorithm in the range of q from 2 to 5. Since the height M of all iris codes used in this experiment is fixed at 20, h values are chosen to be less than 20. In Table 4.1, it can be seen that the EER increases with the increase of h as q approaches 2. The EER usually depends on the size of the coherent matching region, because the non-coherent matching area, where the noise is embedded, does not contribute to lowering the EER. If h increases, the number of bits to make an entry of Z_i in (4.7) increases, so that the matching performance becomes poor and the coherent matching region is reduced, resulting in the increase of EER.

On the other hand, the situation is different with large q. When q approaches 5, the EER decreases as h increases, which is opposite to the case of $q = 2$. Although the coherent matching region decreases by half when q increases by 1, the active range of entry values in Z_i decreases more quickly where the "active range" means the range of numbers that are more frequently selected from $[0, 2^h - 1]$. In the case of large q, the range of active values has a greater effect because the size of the coherent matching region is very small. For example, given $q = 2$, the entries of Z_i are appropriately distributed in the interval $[0, 15]$ when $h = 4$. However, as q is changed to 5, they usually remain at a limited number such as $0, 1, 2, 4, 8$ and the others are rarely selected. This increases the ambiguity between the classes, which results in the increase of EER. However, when q is kept to 5 and h is increased to 16, the entries of Z_i have active range of $0, 1, 2, ..., 2^{15}$. The longer the range of active values, the less the ambiguity and ERR. In summary, as h increases for a fixed r, the performance decreases when q is small, and increases when q is large. This tendency is similar for all databases.

Table 4.2 shows the EER performance for several values of h and r with the q fixed to 3. The parameter h is selected at equally spaced intervals of 4, 8, 12 and 16, and r is chosen to be 1, 4, 8, 12, 16, 20 and 25. As expected, the EER decreases with the increase of r regardless of h. It means that increasing r also increases the size of the coherent matching region to enhance the discriminability of Z_i. The EER for

ND-IRIS-0405 database converges to zero faster than the others because it is a rich database with plenty of clean images to choose from.

4.5.4 Comparison with other algorithms

In this section we compare our method with the state-of-the-art algorithms on cancelable biometrics. First, the proposed algorithm is tested with the parameters of $q = 3$, $r = 12$, and $h = 10$. We compare our method with five algorithms, such as biohashing [7], SRP [29], block remapping [6], bloom filter [1], and IFO hashing [28]. The biohashing in [7] was applied to the fingerprint, but it is compared here as it is a representative and universal algorithm in the cancelable biometrics field. The bloom filter of [1] was also applied to the face database, but we also include it for comparison because it was adopted for enhancing the unlinkability of previous iris recognition method [26]. We test the algorithms on the same environment by implementing them in MATLAB. Since there are very few comparative experiments with various databases in a common environment in the CIB field, we hope that our experiment would help to investigate the properties of the compared algorithms.

Table 4.3: Performance Comparison Between the Proposed Method and Other Algorithms in Terms of EER in Databases.

Method	EER (%)									Mean EER (%)		
	CASIA V3 iris-interval			IIT Delhi iris			ND-Iris-0405					
	GE-IM	GE-PG1	GE-PG2	GE-IM	GE-PG1	GE-PG2	GE-IM	GE-PG1	GE-PG2	GE-IM	GE-PG1	GE-PG2
Unprotected	0.54	N/A	N/A	1.86	N/A	N/A	1.28	N/A	N/A	1.23	N/A	N/A
Biohashing [7]	**0.00**	7.39	**0.00**	**0.00**	7.75	**0.00**	**0.00**	16.20	**0.00**	**0.00**	10.45	**0.00**
SRP [30]	**0.00**	0.60	**0.00**	**0.00**	3.13	**0.00**	**0.00**	5.16	**0.00**	**0.00**	2.96	**0.00**
Block Remapping [6]	0.07	1.69	1.28	0.30	5.62	2.27	1.10	12.58	4.11	0.49	6.63	2.55
Bloom Filter [1]	0.74	1.01	0.81	1.41	2.01	1.41	1.09	5.32	1.25	1.08	2.78	1.16
IFO hashing [28]	0.27	0.81	0.34	1.13	2.22	1.26	0.82	2.84	1.10	0.74	1.96	0.9
Proposed	0.27	**0.54**	0.27	0.45	**1.56**	0.45	**0.00**	**0.88**	**0.00**	0.24	**0.99**	0.24

Table 4.3 shows the EER for the above stated algorithms. As mentioned in Section 4.5.2, GE-IM means the discriminability of an algorithm in a normal situation, and GE-PG1 shows the ability to withstand the key-dependent attacks when the keys are stolen. GE-PG2 is the authentication performance of generated templates when one class is used on multiple devices with different keys and affects the unlinkability. The proposed algorithm shows good performance for all three categories in terms of EER. In GE-IM and GE-PG2, two biometric salting algorithms [7],[29] take advantage of user-specific projection and show the excellent efficiency of zero EER. In GE-PG1, however, biohashing shows poor results because it allows similar projection between classes with the stolen key. Three non-invertible transform-based algorithms [6],[1],[28] are slightly worse than salting methods on GE-IM and GE-PG2 on average, but better in GE-PG1. Among them, IFO hashing shows overall stable performance for all three cases in all datasets due to the discriminability of min-hash and repeated hash values. Our algorithm shows better performance than others in most scores because the robustness is enhanced and the accuracy is improved by composing a plurality of templates. Also, the templates are created by using repetitive hash values based on RRP-BS, which makes them coherent matching areas. This result is also demonstrated in the receiver operating characteristics (ROC) curves of all the databases as shown in Figures 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, and 4.12.

Table 4.4 shows the running times of the compared algorithms in the CASIA V3 database. The key generation process in biohashing takes much time because it needs large amount of computations in the orthogonalization process. The block remapping method in enrollment stage is very fast as the random shuffling of the duplicating blocks is done only. The bloom filter method needs the least time because of its alignment-free property during the authentication. Since the proposed algorithm uses several images when enrollment, it takes about 27.2 msec to generate the template. However, when the authentication is performed, the template is created with a single

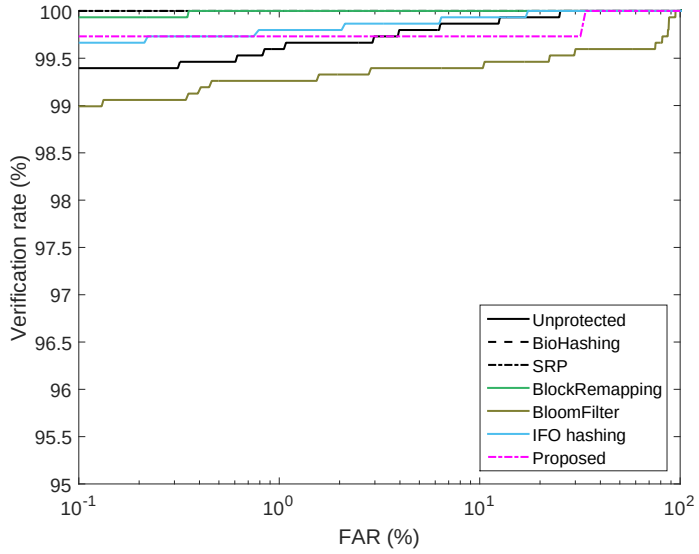

Figure 4.4: GE-IM ROC curves of the proposed system with the other algorithms for the best EER performance of CASIA V3 iris-interval database.

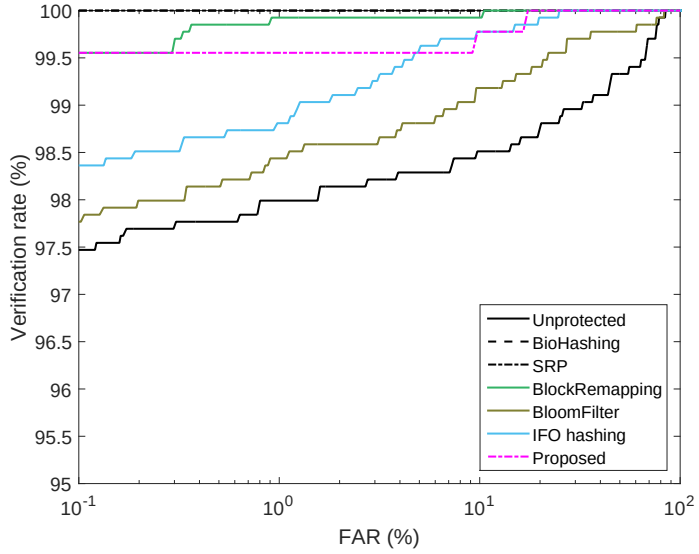

Figure 4.5: GE-IM ROC curves of the proposed system with the other algorithms for the best EER performance of IIT Delhi database.

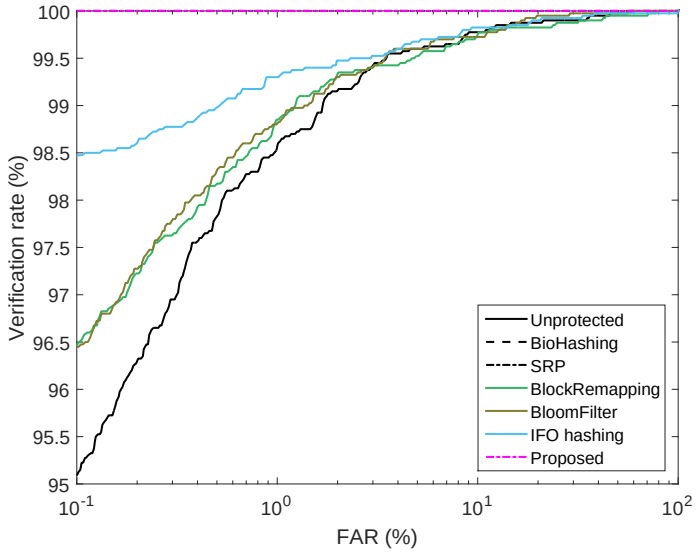

Figure 4.6: GE-IM ROC curves of the proposed system with the other algorithms for the best EER performance of ND-iris-0405 database.

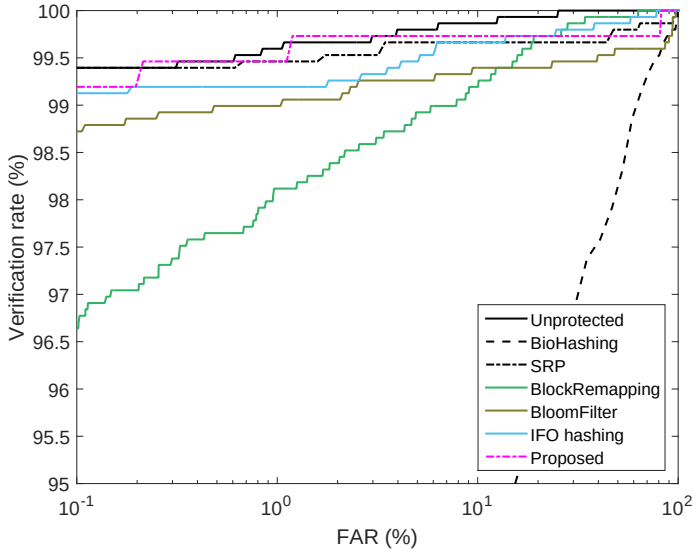

Figure 4.7: GE-PG1 ROC curves of the proposed system with the other algorithms for the best EER performance of CASIA V3 iris-interval database.

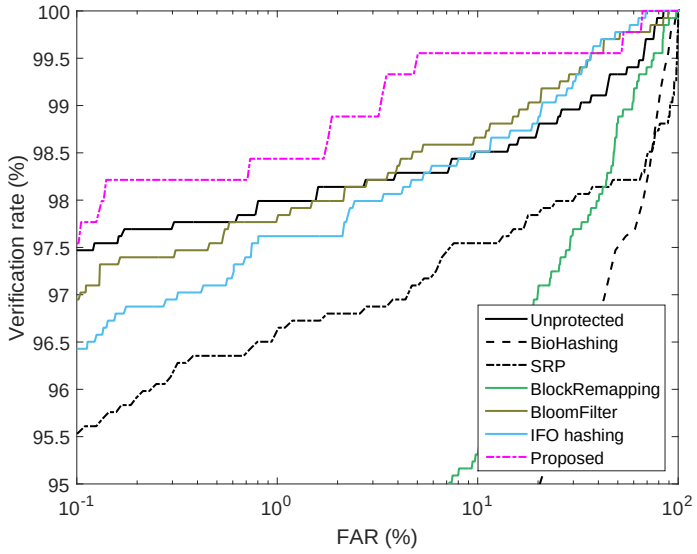

Figure 4.8: GE-PG1 ROC curves of the proposed system with the other algorithms for the best EER performance of IIT Delhi database.

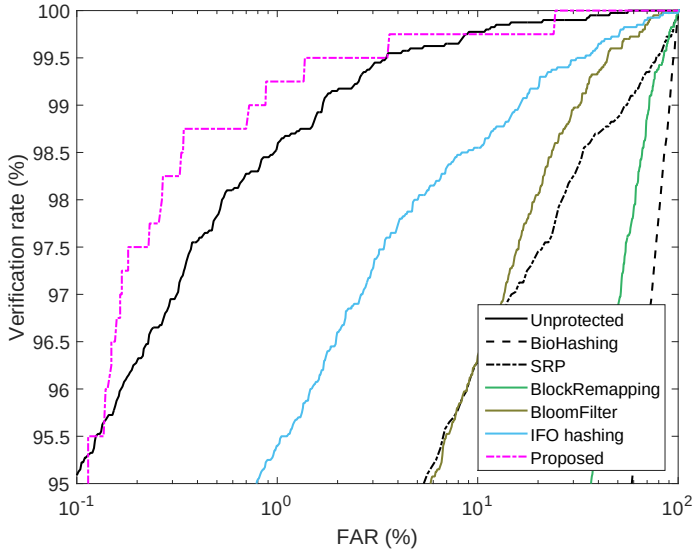

Figure 4.9: GE-PG1 ROC curves of the proposed system with the other algorithms for the best EER performance of ND-iris-0405 database.

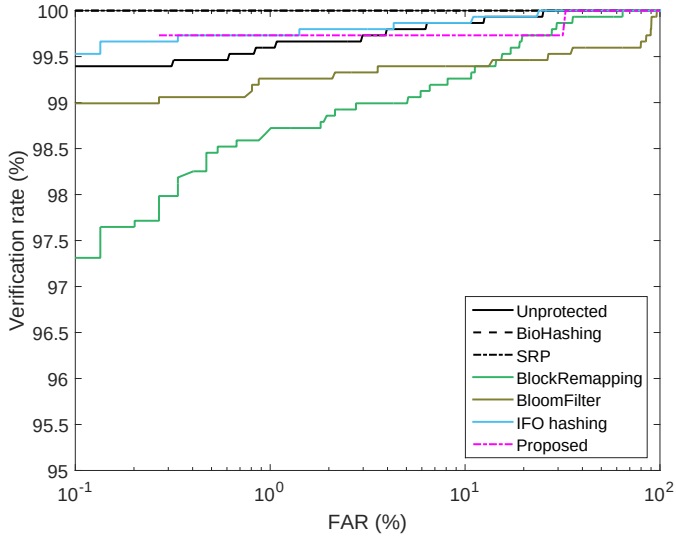

Figure 4.10: GE-PG2 ROC curves of the proposed system with the other algorithms for the best EER performance of CASIA V3 iris-interval database.

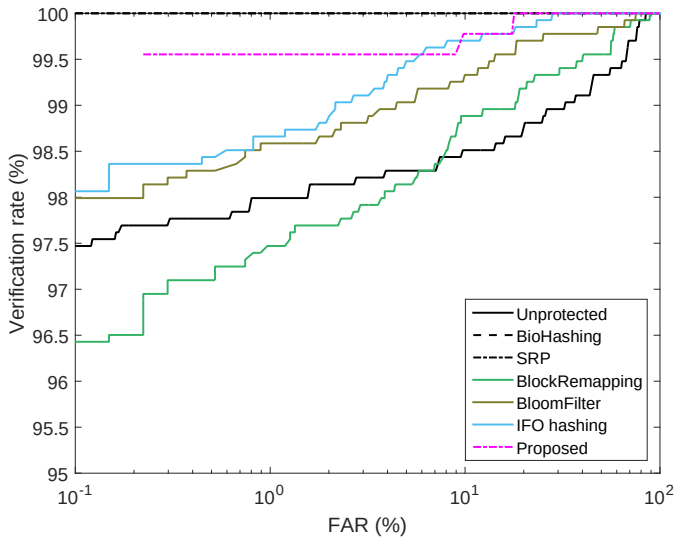

Figure 4.11: GE-PG2 ROC curves of the proposed system with the other algorithms for the best EER performance of IIT Delhi database.

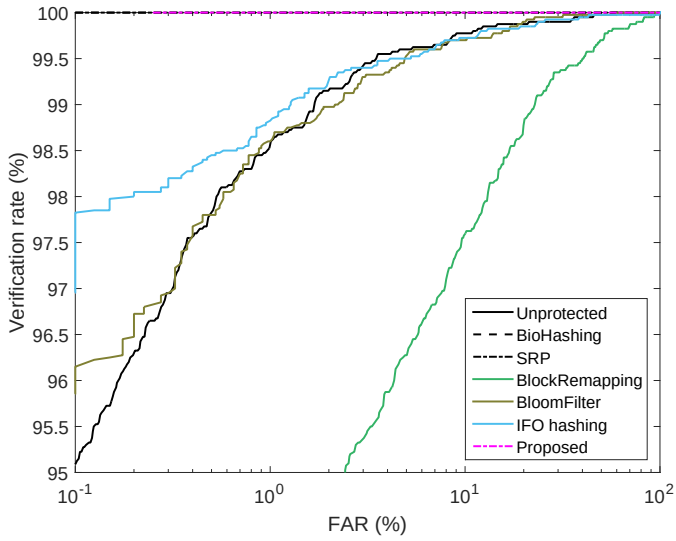

Figure 4.12: GE-PG2 ROC curves of the proposed system with the other algorithms for the best EER performance of ND-iris-0405 database.

iris code and it needs similar time to IFO hashing. The number of registered images used in Table 4.4 is four, but if the number of training images increases, the registration time may become longer. However, the execution time of the proposed algorithm is modest because a small number of registered images can achieve sufficient accuracy.

Table 4.4: Excution Time in Seconds for the Proposed System with Other Algorithms in CASIA V3 Database

Method	Enrollment time			Authentication time		
	Key(Token) generation	Template generation	Total	Key(Token) generation	Template gen. + Comparison	Total
Biohashing [7]	0.5999	0.0063	0.6062	0.5875	0.0753	0.6628
SRP [30]	0.0990	0.0018	0.1008	0.0942	0.0097	0.1039
Block Remapping [6]	0.0010	0.0007	0.0017	0.0011	0.0065	0.0076
Bloom Filter [1]	0.0013	0.0017	0.0030	0.0009	0.0017	0.0027
IFO hashing [28]	0.0049	0.0030	0.0080	0.0049	0.0444	0.0493
Proposed	0.0046	0.0272	0.0319	0.0046	0.0407	0.0453

4.5.5 Unlinkability

The unlinkability of the proposed algorithm depends on the key matrices P and S. They are generated by different pseudo random numbers for each device and have different values. We have seen that the performance of our method in terms of GE-PG2 is good enough in Section 4.5.3. It means that the iris templates among other devices have little similarity and the unlinkability is satisfied.

In this subsection, we also test whether the distribution of PG2 is ultimately ambiguous compared to that of IM. As mentioned in Section 4.5.2, the score of IM is obtained from the comparison of the other classes, and the score of PG2 is derived from the comparison within the class. Therefore, the distribution of PG2 is always statistically closer to the distribution of GE than that of IM. When the distribution of PG2 is nearly identical to that of IM, and if the adversary gets the templates of two devices derived from that class, he/she would not be able to distinguish whether they are from the same class or not. Speficically, Figure 4.13, 4.14, and 4.15 show that the distributions of PG2 and IM are almost overlapping. In other words, the proposed algorithm can create completely different templates if the keys are different.

To obtain more objective results of how similar the distribution of PG2 and IM are, we experiment with the new measure proposed in [1]. The measure estimates the unlinkability using the likelihood ratio of probability of PG2 and IM. Given a score of s, let $\mathrm{Pr}_{\mathrm{PG2}}(s)$ and $\mathrm{Pr}_{\mathrm{IM}}(s)$ be the probabilities of PG2 and IM, respectively. The likelihood ratio is given by $l(s) = \mathrm{Pr}_{\mathrm{PG2}}(s)/\mathrm{Pr}_{\mathrm{IM}}(s)$. Then the system's unlinkability estimate is defined to be in the range of $[0, 1]$ as follows

$$E_{\mathrm{u}} = \int_0^1 \left[\frac{2}{1 + e^{-(l(s)-1)}} - 1\right] \mathrm{Pr}_{\mathrm{PG2}}(s) u[l(s) - 1] ds \tag{4.15}$$

where $u[\cdot]$ is the unit step function. E_{u} means the weighted sum of the estimates with $\mathrm{Pr}_{\mathrm{PG2}}(s) \geq \mathrm{Pr}_{\mathrm{IM}}(s)$, and samller E_{u} means better unlinkability. Table 4.5 lists E_{u} for the compared algorithms, which shows that our method yields better or comparable result.

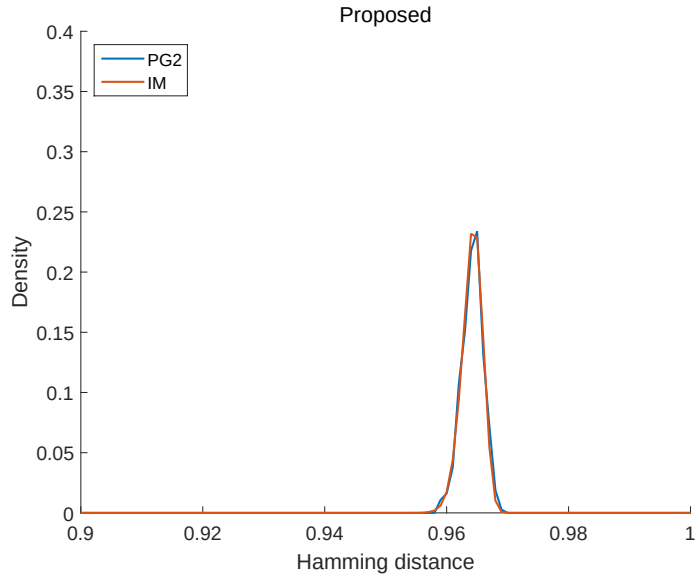

Figure 4.13: PG2 and IM distributions of the proposed algorithm for the CASIA V3 iris-interval database.

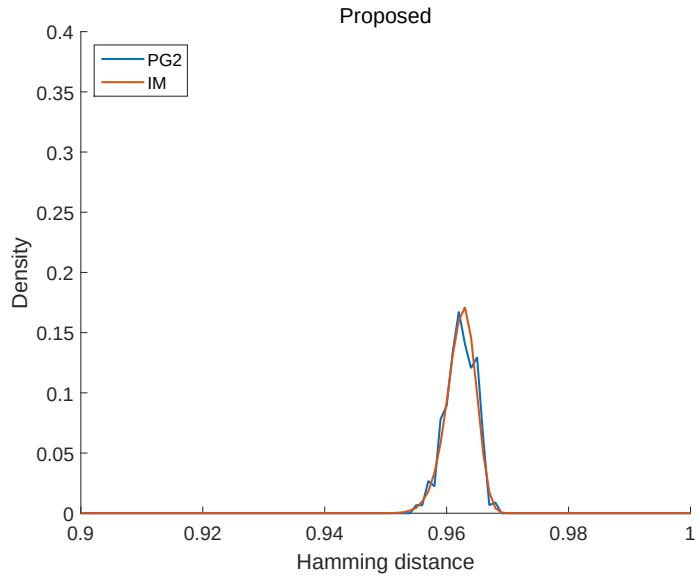

Figure 4.14: PG2 and IM distributions of the proposed algorithm for the IIT Delhi database.

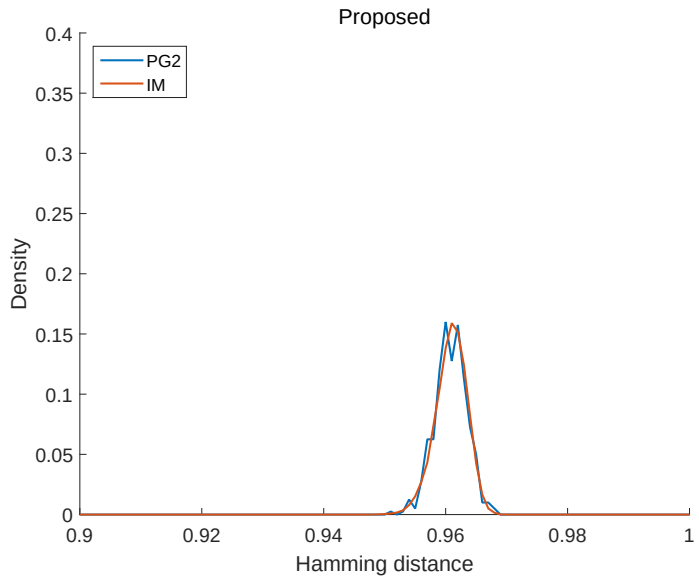

Figure 4.15: PG2 and IM distributions of the proposed algorithm for the ND-iris-0405 database.

Table 4.5: Comparison of unlinkability estimates in terms of a measure defined in [1]

Method	E_u			Mean
	CASIA V3	IIT Delhi	ND-IRIS-0405	E_u
Biohashing [7]	0.10	0.05	0.06	0.07
SRP [30]	0.14	0.19	0.10	0.14
Block Remapping [6]	0.04	0.04	0.11	0.06
Bloom Filter [1]	0.04	0.07	**0.03**	0.05
IFO hashing [28]	0.05	**0.03**	0.05	**0.04**
Proposed	**0.03**	0.04	0.04	**0.04**

4.6 Security Analysis

This section presents the security capability of the proposed algorithm. Specifically, we show that the original data can be hardly reconstructed by inverse operation.

The proposed algorithm uses Hadamard product and noise embedding method for non-invertibility in the enrollment step. Suppose an attacker has acquired all the possible parameters, key matrices, and the template T. To retrieve the original biometric, the attacker needs to fill in T with the original entries instead of noise in the non-coherent matching region $\mathcal{R}_{\text{non-coherent}}$ and perform an inverse operation of the Hadamard product. However, since neither $\mathcal{R}_{\text{non-coherent}}$ nor the binary map $B_{\text{non-coherent}}$ is stored, the attacker has no way of knowing it. If the inverse operation of Hadamard product is performed including a region with noise, it will be almost impossible to restore the original biometric because the noise region will give false estimates. For example, when $h = 10$, $q = 3$, and $r = 12$ in the CASIA database, the ratio of coherent matching region over the overall region is about 39.01% on average. Since the number of entries in the template created by the CASIA database is $12 * 240 = 2,880$, the area contains $2,880 * 0.3901 = 1,124$ entries. So the attacker needs $\binom{2,880}{1,124} \approx 10^{835}$ attempts to estimate the coherent matching region.

The goal of the Hill Climbing Attack is to continuously modify one or more biometric inputs to pass through the authentication system in order to obtain the approximate original biometric [11]. In this case, the attackers can usually only know whether the system has passed. But if the match score can be obtained, it can be planned to have the best score. Our algorithm is also robust to this attack, because we obtain the coherent matching region using several registration templates. As mentioned earlier, this domain is a key part of our algorithm's performance, and the attacker cannot know the region by any means because it is not kept in storage. That is, the hill climbing attack is infeasible because the adversary can attempt the attack only when the area is exposed. Lastly, consider the case that the attacker may have obtained the templates

from several devices with the same key [37]. The attack is also infeasible in this case, because the size of coherent matching region is usually different for each device.

4.7 Conclusion

We have proposed a new cancelable biometric (CB) scheme for the iris recognition system. The proposed algorithm adopts Hadamard product and noise embedding method based on RRP-BS. The unlinkability is statisfied by using the RRP-BS, and the Hadamard product and noise embedding enable the non-invertibility. To use the noise embedding method effectively, we defined a coherent matching region among several enrollment templates and embed the noise into the non-coherent region. The area information can not be stolen because it is not stored in the authentication system. Without precise information on the coherent regions, an attacker would have a wrong estimate even if he/she performs an inverse operation on the Hadamard product. This makes the proposed algorithm robust to brute-force, hill climbing, multiplicity or pre-image attacks. According to the experiments, the proposed CB scheme shows good performance in terms of EER. The proposed method does not only guarantee the non-invertibility but also preserves the low error rates in terms of GE-IM, GE-PG1, and GE-PG2 for three databases. The proposed CB algorithm is designed for iris data in this chapter, but it can also be applied to other biometric such as fingerprint or face by removing the alignment process specialized for the iris data.

Chapter 5

CONCLUSION

In this dissertation, the novel cancelable biometric scheme for iris recognition system was proposed. The first proposed CB method uses RRP-BS which consists of random permutation of binary iris template followed by the orthogonal binary salting. The random permutation perturbs the rows of iris template structure and eliminates some rows of iris template. This guarantees the non-invertibility of CB scheme even though the all of bio-security keys is stolen. Then this CB scheme also proposes an orthogonal binary salting method, where the random binary keys are generated by Gram-Schmidt orthogonalization. The orthogonality of random keys maximizes the Hamming distances among binary-salted templates. Thus, the inter classes are discriminated while the intra class is well identified. While this method has good performance and unlinkability, its non-invertibility is vulnerable to muliplicity or hill-climbing attacks. The second proposed method uses more robust non-invertibility transform based on the first method. We use the RRP-BS as the biometric salting, and use the Hadamard product for enhancing the non-invertibility of salted data. Moreover, to overcome the shortcomings of perserving the keys of the conventional salting methods, we generate several templates for an input, and define non-coherent and coherent matching regions among these templates. We show that salting the non-coherent matching regions is less

influential on the overall performance. Specifically, embedding the noise in this region does not affect the performance, while making the data difficult to be inverted to the original. For the evaluation, we use three datasets, namely CASIA V3 iris-interval, IIT Delhi iris, and ND-Iris-0405. The extensive evaluations show that the proposed algorithm yields low error rates and good intra/inter classification performances, which is better or comparable to the existing methods. Moreover, the security analysis ensures that the proposed algorithm satisfies non-invertibility and unlinkability, and is robust against several attacks as well.

Bibliography

[1] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, and J. Fierrez, "Unlinkable and irreversible biometric template protection based on bloom filters," *Information Sciences*, vol. 370, pp. 18–32, 2016.

[2] J. Daugman, "How iris recognition works," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 21–30, 2004.

[3] Y. Lee, Y. Chung, and K. Moon, "Inverse operation and preimage attack on biohashing," in *Computational Intelligence in Biometrics: Theory, Algorithms, and Applications, 2009. CIB 2009. IEEE Workshop on*. IEEE, 2009, pp. 92–97.

[4] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 29, no. 4, pp. 561–572, 2007.

[5] J. Zuo, N. K. Ratha, and J. H. Connell, "Cancelable iris biometric," in *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*. IEEE, 2008, pp. 1–4.

[6] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *International Conference on Information Security*. Springer, 2009, pp. 135–142.

[7] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[8] A. B. J. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37, no. 5, pp. 1096–1106, 2007.

[9] A. B. Teoh, A. Goh, and D. C. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, 2006.

[10] M. Savvides, B. V. Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, vol. 3. IEEE, 2004, pp. 922–925.

[11] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, p. 1, 2011.

[12] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015.

[13] H. Kaur and P. Khanna, "Biometric template protection using cancelable biometrics and visual cryptography techniques," *Multimedia Tools and Applications*, pp. 1–29, 2015.

[14] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[15] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, p. 113, 2008.

[16] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[17] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: A survey," *Computer vision and image understanding*, vol. 110, no. 2, pp. 281–307, 2008.

[18] J. Daugman, "Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons," *Proceedings of the IEEE*, vol. 94, no. 11, pp. 1927–1935, 2006.

[19] S. Baker, K. Bowyer, and P. Flynn, "Empirical evidence for correct iris match score degradation with increased time-lapse between gallery and probe matches," *Advances in Biometrics*, pp. 1170–1179, 2009.

[20] S. P. Fenker and K. W. Bowyer, "Experimental evidence of a template aging effect in iris biometrics," in *Applications of Computer Vision (WACV), 2011 IEEE Workshop on*. IEEE, 2011, pp. 232–239.

[21] C. Rathgeb, A. Uhl, and P. Wild, *Iris biometrics: from segmentation to template security*. Springer Science & Business Media, 2012, vol. 59.

[22] C. Fancourt, L. Bogoni, K. Hanna, Y. Guo, R. Wildes, N. Takahashi, and U. Jain, "Iris recognition at a distance," in *Audio-and Video-Based Biometric Person Authentication*. Springer, 2005, pp. 187–200.

[23] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE transactions on information forensics and security*, vol. 5, no. 1, pp. 103–117, 2010.

[24] S. Jenisch and A. Uhl, "Security analysis of a cancelable iris recognition system based on block remapping," in *Image Processing (ICIP), 2011 18th IEEE International Conference on*. IEEE, 2011, pp. 3213–3216.

[25] R. Dwivedi, S. Dey, R. Singh, and A. Prasad, "A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping," *Computers & Security*, vol. 65, pp. 373–386, 2017.

[26] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *2013 International Conference on Biometrics (ICB)*. IEEE, 2013, pp. 1–8.

[27] J. Hermans, B. Mennink, and R. Peeters, "When a bloom filter is a doom filter: security assessment of a novel iris biometric template protection system," in *Biometrics Special Interest Group (BIOSIG), 2014 International Conference of the*. IEEE, 2014, pp. 1–6.

[28] Y.-L. Lai, Z. Jin, A. B. J. Teoh, B.-M. Goi, W.-S. Yap, T.-Y. Chai, and C. Rathgeb, "Cancellable iris template generation based on indexing-first-one hashing," *Pattern Recognition*, vol. 64, pp. 105–117, 2017.

[29] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Sectored random projections for cancelable iris biometrics." in *ICASSP*, 2010, pp. 1838–1841.

[30] ——, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 9, pp. 1877–1893, 2011.

[31] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal authentication," *Pattern recognition*, vol. 43, no. 3, pp. 1016–1026, 2010.

[32] P. J. Phillips, W. T. Scruggs, A. J. O'Toole, P. J. Flynn, K. W. Bowyer, C. L. Schott, and M. Sharpe, "Frvt 2006 and ice 2006 large-scale experimental results," *IEEE transactions on pattern analysis and machine intelligence*, vol. 32, no. 5, pp. 831–846, 2010.

[33] K. Nguyen, C. Fookes, and S. Sridharan, "Fusing shrinking and expanding active contour models for robust iris segementation," in *Information Sciences Signal Processing and their Applications (ISSPA), 2010 10th International Conference on*. IEEE, 2010, pp. 185–188.

[34] H. Hofbauer, F. Alonso-Fernandez, P. Wild, J. Bigun, and A. Uhl, "A ground truth for iris segmentation," in *Pattern Recognition (ICPR), 2014 22nd International Conference on*. IEEE, 2014, pp. 527–532.

[35] N. Othman, B. Dorizzi, and S. Garcia-Salicetti, "Osiris: An open source iris recognition software," *Pattern Recognition Letters*, vol. 82, pp. 124–131, 2016.

[36] L. Masek, "Recognition of human iris patterns for biometric identification," B.S. dissertation, The School of Computer Science and Software Engineering, The University of Western Australia, Crawley WA, Perth, Australia, 2003.

[37] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Biometrics Symposium, 2007*. IEEE, 2007, pp. 1–6.

초 록

최근들어 사람의 신체 정보를 이용한 바이오메트릭 인증 시스템이 널리 사용되고 있다. 바이오메트릭 정보는 인증을 위해서 많은 장점을 가지고 있는데, 사람마다 고유하기 때문에 식별하는 정확도가 매우 높다. 그리고 패스워드 처럼 암기하고 다닐 필요없이 지니고 있는 정보이기 때문에 잃어 버리지 않으며 비접촉식이기 때문에 거부감이 덜드는 장점이 있다. 하지만 이런 장점들에 비견되는 큰 단점도 있다. 바이오메트릭은 보통 영상으로 취득되는데, 영상으로부터 추출된 정보는 쉽게 사용될 수 있는 반면, 도용도 쉽다. 바이오메트릭 정보는 개인이 함부로 바꾸기 힘든 고유한 정보이기 때문에 도용되기 쉬운 원본 데이터를 사용하는 것은 매우 위험하다. 그래서 바이오메트릭을 암호화 하려는 시도들이 있는데, 크게 두 가지로 나뉜다. 첫 번째 방법은 바이오메트릭 크립토시스템(biometric cryptosystems, BCS)으로서 암호디지털 키를 바이오메트릭에 결합하거나 또는 바이오메트릭으로부터 그 키를 생성해내는 방법이다. 이 방법은 바이오메트릭 또는 키로부터 도움 데이터를 생성하는데 이것을 생성하는 방법에 성능이 크게 좌우된다. 두 번째 방법은 가변생체(cancelable Biometrics, CB)로서 사용자에 특화된 키를 이용하여 바이오메트릭을 템플릿으로 변환시켜 키와 같이 저장한다. 만약 템플릿이나 키가 도난당하더라도 새로운 키를 가지고 쉽게 새로운 템플릿을 만들 수 있다는 장점이 있다. 새롭게 생성된 템플릿은 이전의 템플릿과 불연결성(unlinkability)을 가진다. 가변생체는 다시 불가역성을 중요시하여 불가역 변환을 이용하는 방법과 성능을 중요시하는 임의 흩뿌림(biometric salting) 방법으로 나뉜다. 불가역성과 성능은 트레이드 오프 관계

이기 때문에 두 가지의 균형을 이루기 힘들다는 단점이 있다.

본 논문에서는 임의 흩뿌림에 기반하여 가변생체를 이용한 새로운 방법이 제안된다. 첫 번째 방법은 임의의 성분이 제거된 퍼뮤테이션과 이진 흩뿌림을 이용한 방법(RRP-BS)이다. 이 방법은 이진 바이오메트릭에 임의 퍼뮤테이션 행렬을 적용하여 일부 행을 제거하고 불가역성을 만족시킨다. 그리고 이진 흩뿌림 성분을 결합하여 성능을 높힌다. 일부의 제거된 행으로 인해 바이오메트릭 키가 도난당해도 불가역성이 보장됨이 이론적으로 증명되었고, 그람 슈미트(Gram-Schmidt) 직교 방법으로 생성된 임의 흩뿌림 키로 인해 클래스 간 구별 가능성이 높아졌다. 하지만 같은 바이오메트릭으로 생성된 템플릿이 다른 키를 사용하였더라도 여러 곳에서 중복적으로 도난 당해 일부가 복원되거나, 조금씩 입력 데이터를 조작하여 원본과 비슷하게 인증이 되도록 탐색하는 힐 클라이밍 공격(hill-climbing attack)에 취약하다는 단점이 있다. 두 번째 방법은 첫 번째 방법에 기반하여 성능을 유지하며 불가역성을 강화한 알고리즘을 제안한다. 임의 흩뿌림 방법인 RRP-BS에 하다마드(Hadamard) 변환을 적용한다. 그리고 기존 임의 흩뿌림 방법이 키를 보존하여 유출 가능성이 있다는 단점이 있는데, 이를 방지하기 위해 키를 보존하지 않는 방법인 노이즈 매립 방법을 추가하였다. 이 방법은 같은 클래스의 여러 장의 바이오메트릭을 이용하여 매칭에 잘 이용되는 강인한 영역을 찾고, 그렇지 않은 영역에 매칭영역과 비슷한 확률 분포를 가지는 노이즈를 매립하여 템플릿을 만든다. 강인한 영역의 위치에 대한 정보는 저장되지 않기 때문에 불가역성이 확률적으로 보장되므로 이전 단계인 RRP-BS 의 키가 도난당하더라도 원본이 복원되거나 추측할 방법이 없다. 또한 노이즈 매립이 매칭에 잘 이용되지 않는 영역에 행해졌기 때문에 성능 저하도 덜하다. 따라서 성능을 유지 시킬 뿐 아니라 불가역성도 유지시킬 수 있는 균형 잡힌 알고리즘이며 인증 알고리즘들의 가역적인 면을 탐색하여 공격하는 대표적인 알고리즘들에 대해서도 강인하다.

주요어: 바이오메트릭, 가변생체, 임의 흩뿌림

학번: 2009-20855