Pre-image Resistant Cancelable Biometrics Scheme Using Bidirectional Memory Model

Mayada Tarek[1], Osama Ouda[2], and Taher Hamza[1]
(Corresponding author: Mayada Tarek)
Department of Computer Science, Faculty of Computer and Information Sciences, Mansoura University[1]
Department of Information Technology, Faculty of Computer and Information Sciences, Mansoura University[2]
El Gomhouria St, Mansoura, Dakahlia Governorate 35516, Egypt
(Email:mayaatarek@yahoo.com)
(Received Feb. 19, 2016; revised and accepted June 13 & July 19, 2016)

Abstract

Cancelable biometrics is a promising template protection scheme which relies on encoding the raw biometric data using non-invertible transformation function. Existing cancelable biometrics schemes ensure recoverability of compromised templates as well as users' privacy. However, these schemes cannot resist pre-image attacks. In this article, a pre-image resistant cancelable biometrics scheme is proposed, where associative memory is utilized to encode the cancelable transformation parameters with the privilege of high recognition performance. Bidirectional memory model has been suggested to memorize each user's associated key using his biometric data based on association connectors. These connector values can be safely saved in the storage along with the cancelable biometric template. The cancelable template is generated using XOR operation between the biometric data and the associated key. The simulated experiments conducted on CASIA-IrisV3-Interval dataset show that the presented resistant scheme does not affect the classification power of the raw biometric data significantly. Moreover, the resistance of the presented scheme against complete or approximate disclosure of the raw biometric template is achieved.

Keywords: Bidirectional memory model (BAM), cancelable biometrics, pre-image attacks

1 Introduction

Recently, protection schemes for biometrics data have gained a lot of interest because of the spread use of biometric data [7] instead of password or smart card for authenticating individuals [13, 15]. Ensuring the proper use of biometric data, that are saved in system storage as templates, is a key concern of any biometrics-based authentication system. Therefore, template protection schemes are needed for protecting these stored biometric templates [7, 20]. Cancelable biometrics (CB) is a promising protection scheme for biometric data designed to store a distorted version, called the cancelable template, of the raw biometric data. The cancelable template is obtained using a non-invertible transformation function and stored, instead of the genuine biometric data, in the system storage [23]. It should be computationally hard to reconstruct the genuine biometric data when cancelable templates are compromised [20].

Over the past few years, various cancelable biometric methods have been presented. Ratha et al. [24, 25] proposed a cancelable scheme for fingerprints using three different transformation named (cartesian, polar and functional). In [4], a data hiding approach is used for iris template protection. Zuo et al. [36] and Rathgeb et al. [29] suggested creating a cancelable template from iris by applying row permutation to iris code. In [17], a random key is employed to convert an on-line signature data into discrete sequences that are convolved together to create the cancelable template. In [2], a new protection scheme for signatures based on homomorphic probabilistic encryption for fixed-length templates is proposed. Savvides et al. [30] proposed a cancelable biometrics filters for face recognition where different templates could be obtained from the face images by varying a random key which acts as filter. The main challenge of these cancelable biometric schemes is the significant degradation in recognition performance achieved using the genuine (unprotected) biometric systems.

Another cancelable biometrics approach has been presented by Teoh et al. [31, 33, 34] in order to increase the recognition accuracy of cancelable biometric templates. They proposed to employ a secrete random number to project the raw biometric features into transformed templates. The scheme has been applied to different types of biometric modalities (e.g. [3, 16]). Rathgeb et al. [26, 27, 28] utilized Bloom filter to construct cancelable templates from iris codes. The scheme provides a rapid comparison among transformed templates using Bloom

filters as a non-invertible transform. Ouda et al. [21, 22] proposed a tokenless cancelable biometrics scheme for protecting iris codes. The scheme relies on mapping fixed-size groups of bits in an iris code into random bits using the concept of Boolean functions.

Although the complexity of reconstructing the genuine data from the cancelable templates in existing schemes is computationally as hard as random guessing, pre-images can be easily constructed from the stored cancelable templates which make these schemes vulnerable to some security breaches [9, 12, 14]. A pre-image attack aims to construct a non-genuine biometric data, which could be completely different from the genuine data but could generate a cancelable template similar to the cancelable template produced from the genuine biometric data [19].

Recently, Mayada et al. [32] proposed a novel cancelable biometrics scheme that can resist pre-image attacks. However, the recognition accuracy of their scheme is noticeably affected as a result.

In this paper, we propose a pre-image resistant cancelable biometric scheme that can pertain the recognition accuracy of the original biometric system. Th proposed scheme binds biometric features and their associated cancelable transformation parameter in an associative memory model. Bidirectional associative memory (BAM) is employed in order to bind each user biometric features with his transformation key through some connector information. These connectors act as an encoded representation of a user's key and its associated biometric data as well. It is safe to store these connectors on the system storage with the cancelable transformed template. The cancelable transformation in this proposed resistant scheme is a simple XOR operation between biometric template and the associated key in order to achieve high recognition performance. Since XOR is a non-invertible operation if only the result is known, the security against pre-image attacks is guaranteed because it is infeasible to extract genuine or even an approximate values for biometric data or it's associated key utilizing the compromised connectors. During authentication, the stored connectors are utilized to apply the mapping process in order to recall the associated key using input biometric data, then the cancelable template is created to be compared with the stored one.

The remainder of this article is organized as follows: the proposed resistant scheme is presented in the next section. A security analysis of the proposed scheme is given in Section 3. Experimental results are presented in Section 4, and Section 5 concludes the paper.

2 Proposed Scheme

The proposed resistant scheme focuses on producing a cancelable biometric template which withstands the pre-image attacks and also achieves high recognition performance. Most of cancelable biometric schemes suffer from the possibility of constructing an approximate biometric features, also known as a biometric template, using the stored cancelable template if system storage is compromised [20]. This paper introduces a cancelable scheme which employs the Boolean XOR operation for implementing the cancelable transformation function. Each binary biometric template is XOR-ed with an associated random binary string to construct a cancelable template. Storing this random bit-string in the system storage or on smart cards makes biometric system susceptible to different types of attacks [8, 10]. To tackle this challenge, our proposed scheme relies on hiding the user's associated bit-string (key) along with the biometric features in an encrypted form using an associative memory. If only the resulting XOR-ed template is compromised by any attacker, the XOR operation cannot be inverted (e.g. '0' can result from '1' XOR '1' or '0' XOR '0'). The associative memory binds every biometric features with its corresponding key through association connectors known as weights. These weights could be securely stored on a central storage to recall the associated key using user's biometric features in the verification stage. The steps of our proposed resistant scheme are illustrated in Figure 1.

As depicted in Figure 1, the proposed cancelable scheme is formulated of two principle processes: firstly, constructing the BAM network weights. These weights values are utilized to connect each user associated key to its biometric data. Secondly, binding biometric template with the key in order to construct the reference cancelable template; this process is accomplished using XOR binding operation. The next subsections illustrate our proposed resistant scheme in detail.

2.1 Enrollment Process

When a new user is enrolled, a reference binary-valued template is generated using all enrolled user's samples. This reference sample is computed by calculating the mean of every bit location from all samples. If this mean value is more than or equals 0.5 then this location reference set to 1 and 0 otherwise. Algorithm 1 presents the enrollment process in detail.

Instead of storing the key associated with each user in the storage or on a token, an associative memory is utilized in order to bind each key with the corresponding biometric template. During the association phase, an associative network weights are learned for each user. During the memorization phase of BAM, an input set of p associated pattern pairs is given: $\{(X_r, Y_r)|r = 1, 2, \ldots, p\}$: $X_r \in \{-1, +1\}^n$ (represent biometric template) and $Y_r \in \{-1, +1\}^n$ (represent transformation key), where bipolar representation is utilized to allow optimum patterns association [1, 35]. Out of the complete set of input patterns, only a single pattern should represent the genuine individual's biometric template binding to a genuine individual's key. Other patterns should represent non-genuine biometric templates linked to non-genuine transformation keys. In order to ensure perfect memory mapping, the other (non-genuine) patterns have to be independent from

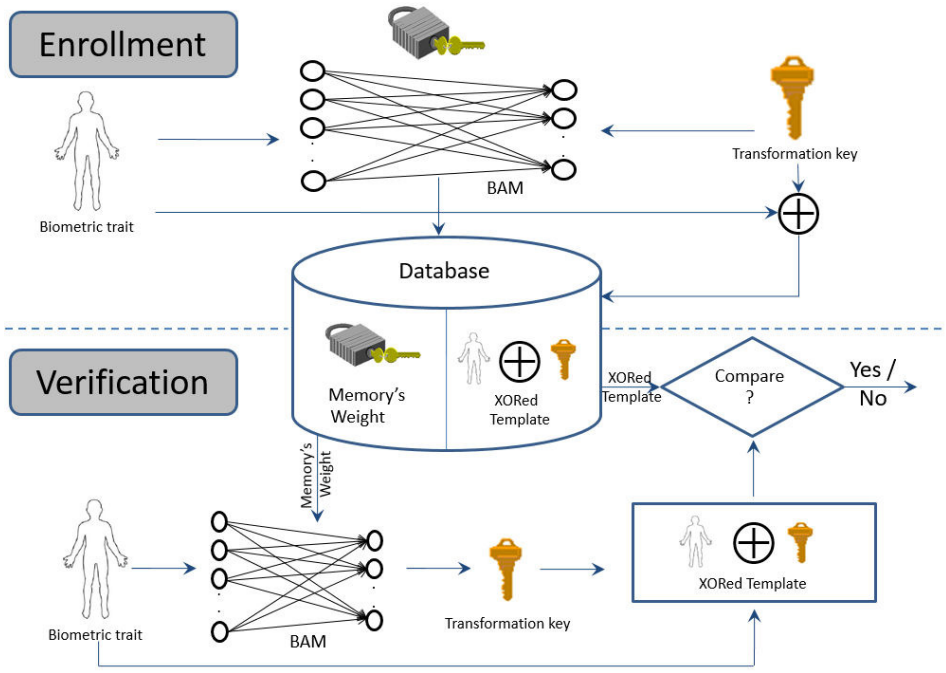

Figure 1: Overview of proposed pre-image resistant cancelable biometric scheme

the user's reference pattern. A bidirectional single layer memory network is utilized to associate two different patterns. The presented BAM model consists of an input unit of n nodes corresponding to biometric features of length n. The input layer nodes are linked to an output layer consisting of n nodes which represents a randomly constructed key of length n through W (weight matrix of size $n \times n$). The weight matrix represents an encoded representation of the cancelable transformation parameters.

In order to construct a protected non-invertible and pre-image resistant cancelable biometric template, a revocable (cancelable) transformation is needed. In our proposed method, the revocable transformation is implemented using the XOR binding operation. The proposed association model ensures that without having the biometric data, it is computationally hard to reveal any information about the genuine transformed key utilizing the stored connection weights as we will show formally in Section 3. Moreover, it is very difficult to construct an approximate version of the biometric template which can the be used to produce an approximate version of the XORed cancelable template without knowing the genuine associated key value.

2.2 Verification Process

In the verification phase, the biometric features of each user are utilized to recall his/her associated key utilizing the stored BAM weights. Due to the intra-user variations of biometric data, biometric data generated from the same individual are not the same. Fortunately, however, the presented BAM model is able to recall the stored associated key binding with the individual's biometric data [35]. Algorithm 2 illustrates the verification process in detail.

The key linked to the claimed identity is XOR-ed with the binary represented biometric data to get the cancelable template. The obtained template is matched against the stored one using the Hamming distance and the authentication process fails if the matching result exceeds a predefined threshold θ and succeeds otherwise.

3 Security Analysis

This section discusses the security properties of our proposed scheme. A secure cancelable biometrics scheme must fulfill a number of requirements; namely, diversity, revocability, non-invertability, and resistance to pre-image attacks. In the next subsections, we show how our proposed scheme can meet these requirements.

3.1 Recoverability and Diversity

The cancelable scheme is revocable if it allows generation of a new key, in case the system storage is compromised, to construct a new template for biometric data belonging to same identity. In our proposed work, the transformation random key is set in BAM network's output layer. Thus, with the possibility of constructing a new key, a new weight matrix could be generated utilizing the same individual's biometric data. Therefore, our proposed scheme satisfies the revocability property.

Algorithm 1 Proposed scheme enrollment stage

Input: A set of L training samples $\{s_1, .., s_L\}$ that belongs to the same class. P, number of associated patterns pairs (X, Y).

1: Generate binary representation templates $\{B_1, .., B_L\}$ from the training samples with n-bit length.
2: Create the reference template B_{ref} for the binary representation training templates using the fusion approach [6] computed by:

$$\phi(i) = \frac{1}{L}\sum_{l=1}^{L} B_l^i \tag{1}$$

$$B_{ref}(i) = \begin{cases} 1, & \text{if } \phi(\mathrm{i}) \geq 0.5 \\ 0, & \text{if } \phi(\mathrm{i}) < 0.5 \end{cases} \tag{2}$$

3: Convert B_{ref} into bipolar representation X_{ref}.
4: Generate random binary sequence K_{ref} with n bits length.
5: Convert K_{ref} into bipolar representation Y_{ref}.
6: Generate the cancelable template:

$$T_{ref} = B_{ref} \oplus K_{ref} \tag{3}$$

7: Generate a set of associated patterns pairs (X_j, Y_j) :
8: $J = 2$
9: **while** $j \neq P$ **do**
10: Select sample B_j from samples belong to other classes then convert it to bipolar representation X_j.
11: Generate the associated random bipolar sequence Y_j.
12: **end while**
13: Randomize the associated patterns pairs (X, Y) order.
14: Create the association BAM weights W using learning approach defined in [1]:
15: $j = 1$, $W = \phi$
16: **while** $j \neq P$ **do**
17:

$$w_j = \bar{X_j} \cdot Y_j \tag{4}$$

$$W = W + w_j \tag{5}$$

18: **end while**
19: Store W and T_{ref} in system storage.

Algorithm 2 Proposed scheme verification stage

Input: Test sample S_{test}, and user identity I.

1: Generate binary representation template B_{test} from S_{test} with n bits length.
2: Convert B_{test} into bipolar representation X_{test}.
3: Retrieve the weights matrix W from biometric system storage.
4: Recall the binary valued key associated with X_{test} as defined in [1]:

$$K = W \cdot X_{test} \tag{6}$$

$$K_{test} = \begin{cases} 1, & \text{if } \mathrm{k_i} \geq 0 \\ 0, & \text{if } \mathrm{k_i} < 0 \end{cases} \tag{7}$$

5: Compute the cancelable test template:

$$T_{test} = B_{test} \oplus K_{test} \tag{8}$$

6: Compare test and reference cancelable template for the input claimed user identity I:

$$\varepsilon = \frac{\|T_{ref} \oplus T_{test}\|}{n} \tag{9}$$

7: Decision making for I:

$$\text{Decision} = \begin{cases} \text{Accept}, & \text{if } \varepsilon \leq \theta \\ \text{Reject}, & \text{if } \varepsilon > \theta \end{cases} \tag{10}$$

The length of the BAM output layer corresponds to the key length. Hence, if it contains m nodes, it allows for generating 2^m different cancelable template using 2^m different keys for each input user. On the other hand, each individual can be enrolled in different biometric systems with different cancelable templates based on each system unique key. Thus, the property of diversity is also satisfied by our proposed scheme.

3.2 Non-invertability

In order to satisfy the non-invertability property, it should be computationally hard to decrypt the XORed template to retrieve either the genuine key or the genuine biometric data. Moreover, it should difficult to extract the key or the genuine biometric features using the stored BAM weights. The utilized XOR binding operation is non-invertible because it is very difficult to reverse the resulting XORed template without knowing either of its input parameters. The non-invertability of the publicly stored BAM weight matrix is acquired from the method used for generating those weights. As mentioned before in Section 2, the weight matrix is constructed using the approach expressed by Equations (4) and (5). This subsection analyzes the computational efforts needed by an adversary to disclose the genuine data utilizing the stored BAM weights.

$$\begin{bmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n,1} & w_{n,2} & \cdots & w_{n,n} \end{bmatrix} = \begin{bmatrix} x_{1,1}\cdot y_{1,1} & x_{1,1}\cdot y_{1,2} & \cdots & x_{1,1}\cdot y_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,n}\cdot y_{1,1} & x_{1,n}\cdot y_{1,2} & \cdots & x_{1,n}\cdot y_{1,n} \end{bmatrix} + \cdots + \begin{bmatrix} x_{p,1}\cdot y_{p,1} & x_{p,1}\cdot y_{p,2} & \cdots & x_{p,1}\cdot y_{p,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{p,n}\cdot y_{p,1} & x_{p,n}\cdot y_{p,2} & \cdots & x_{p,n}\cdot y_{p,n} \end{bmatrix} \tag{11}$$

Recall that the BAM network contains p associated vectors $\{X_r, Y_r\}$ for $r = 1, 2, \ldots, p$; and the used cancelable transform is the XOR operation, i.e., Y and X must be of equal length, where X: is the biometric template represented as vector of length n, Y: is the corresponding transformation key represented as vector of length n as illustrated below:

$$\begin{array}{cc} x_1 = [x_{1,1}, x_{1,2}, \cdots, x_{1,n}] & , \quad y_1 = [y_{1,1}, y_{1,2}, \cdots, y_{1,n}] \\ x_2 = [x_{2,1}, x_{2,2}, \cdots, x_{2,n}] & , \quad y_2 = [y_{2,1}, y_{2,2}, \cdots, y_{2,n}] \\ \vdots & \vdots \\ x_p = [x_{p,1}, x_{p,2}, \cdots, x_{p,n}] & , \quad y_p = [y_{p,1}, y_{p,2}, \cdots, y_{p,n}] \end{array}$$

The weight matrix W of size $n \times n$, computed using Equations (4) and (5), can be constructed by matrix notations as expressed in Equation (11). When an adversary has only the values of matrix W, we analyze the computational complexity needed to reconstruct the genuine transformation key Y_s or the genuine biometric template X_s using matrix W. Each single raw vector in W could be seen as a linear system of equations, e.g. the s^{th} row in W matrix which contains values: $[w_{s,1}, w_{s,2}, ..., w_{s,n}]$, could be represented by the following linear system of equations:

$$\begin{array}{c} w_{s,1} = x_{1,s}.y_{1,1} + x_{2,s}.y_{2,1} + \cdots + x_{p,s}.y_{p,1} \\ w_{s,2} = x_{1,s}.y_{1,2} + x_{2,s}.y_{2,2} + \cdots + x_{p,s}.y_{p,2} \\ \vdots \\ w_{s,n} = x_{1,s}.y_{1,n} + x_{2,s}.y_{2,n} + \cdots + x_{p,s}.y_{p,n} \end{array}$$

This linear system of equations can be represented using matrix notations as follows:

$$\begin{bmatrix} w_{s,1} \\ w_{s,2} \\ \vdots \\ w_{s,n} \end{bmatrix} = \begin{bmatrix} y_{1,1} \\ y_{1,2} \\ \vdots \\ y_{1,n} \end{bmatrix} .x_{1,s} + \begin{bmatrix} y_{2,1} \\ y_{2,2} \\ \vdots \\ y_{2,n} \end{bmatrix} .x_{2,s} + \cdots + \begin{bmatrix} y_{p,1} \\ y_{p,2} \\ \vdots \\ y_{p,n} \end{bmatrix} .x_{p,s} \tag{12}$$

Grouping the common factors yields:

$$\begin{bmatrix} w_{s,1} \\ w_{s,2} \\ \vdots \\ w_{s,n} \end{bmatrix} = \begin{bmatrix} y_{1,1} & y_{2,1} & \cdots & y_{p,1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1,n} & y_{2,n} & \cdots & y_{p,n} \end{bmatrix} \cdot \begin{bmatrix} x_{1,s} \\ x_{2,s} \\ \vdots \\ x_{p,s} \end{bmatrix} \tag{13}$$

By expanding Equation (13) for each row vector in W matrix, i.e. substituting s from 1 to n, each linear system could be expressed as follows:

$$\begin{bmatrix} w_{1,1} \\ w_{1,2} \\ \vdots \\ w_{1,n} \end{bmatrix} = \begin{bmatrix} y_{1,1} & y_{2,1} & \cdots & y_{p,1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1,n} & y_{2,n} & \cdots & y_{p,n} \end{bmatrix} \cdot \begin{bmatrix} x_{1,1} \\ x_{2,1} \\ \vdots \\ x_{p,1} \end{bmatrix} \tag{14}$$

$$\begin{bmatrix} w_{2,1} \\ w_{2,2} \\ \vdots \\ w_{2,n} \end{bmatrix} = \begin{bmatrix} y_{1,1} & y_{2,1} & \cdots & y_{p,1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1,n} & y_{2,n} & \cdots & y_{p,n} \end{bmatrix} \cdot \begin{bmatrix} x_{1,2} \\ x_{2,2} \\ \vdots \\ x_{p,2} \end{bmatrix} \tag{15}$$

$$\vdots$$

$$\begin{bmatrix} w_{n,1} \\ w_{n,2} \\ \vdots \\ w_{n,n} \end{bmatrix} = \begin{bmatrix} y_{1,1} & y_{2,1} & \cdots & y_{p,1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1,n} & y_{2,n} & \cdots & y_{p,n} \end{bmatrix} \cdot \begin{bmatrix} x_{1,n} \\ x_{2,n} \\ \vdots \\ x_{p,n} \end{bmatrix} \tag{16}$$

Mathematically, solving each linear system given only W requires guessing the matrix Y. In order to guess the values of Y, which contains $n \times p$ unknown variables, the attacker needs at most 2^{np} trails to get the correct values of Y which satisfy all linear system equations. Thus, the computational effort needed by any attacker to disclose the linear system of equations is as hard as randomly guessing all key values. Having key length equivalent to biometric template length makes it computationally infeasible to guess key values, especially when p and n are large values. Additionally, The attacker needs extra efforts to detect the genuine biometric data linked to the genuine transformation key. This is because, as mentioned before in Section 2.1, the weight matrix W not only contains the genuine user key information associate with its genuine biometric data but also contains other non-genuine keys linked to non-genuine biometric data.

3.3 Pre-image Attack Analysis

The pre-image attackers attempt to recreate sufficiently comparable biometric templates which act as the genuine one utilizing the compromised data. In our proposed work, generating biometric data from the stored data (connection weights and cancelable template) is computationally as hard as random guessing. It is unattainable to reveal any information using only the stored XORed template without knowing either the key or biometric data as proven in the previous subsection. However, the pre-image attacker can construct a non-genuine biometric features and a non-genuine transformation key which generate enough similar XORed template. Fortunately, there is no mathematical way to construct a non-genuine biometric template that is close enough to the original one from both of the stored XORed template and the connection weights. Therefore, our proposed method is robust against pre-image attack.

Since the pre-image attacker has no way to create an approximated input patterns except through ran-

Table 1: CASIA-IrisV3-Interval properties [5]

# subjects	# classes	Total number of images	Image Resolution
249	395	2683	320×282

Table 2: *Experimental parameters setting*

Masek output-code		BAM Structure		XOR- parameters	
Iris array size	40×480 bits	# input nodes	9600	Iris' size	9600
		BAM weights size	9600×9600	Key size	9600
Reference iris code size	9600 bit	# output nodes	9600	XORed Template' size	9600
		# patterns	p		

dom guessing (Brute-force), the maximum number of trials needed to construct biometric data or key to disclose biometric system's data is 2^n, (where n represents the input binary-valued biometrics template length, or equivalently, the input binary-valued transformation key length). Therefore, our proposed scheme maximizes the efforts needed for this kind of attacks, especially when n is large.

4 Experimental Results

In order to evaluate our proposed work from recognition performance perspective, several experiments were performed on the standard CASIA-IrisV3-Interval database [5]. The database is partitioned into 249 subjects; each subject has his right or left or both eye' samples. Table 1 illustrates the CASIA-IrisV3-Interval database specification in detail. In order to construct iris codes for each iris dataset image, Masek code [18] was utilized to construct the genuine binary valued iris templates.

During the BAM association phase, a reference pattern for each iris was created using the approach clarified in Section 2.1. Each class reference iris code serve as an input pattern for this BAM model to be associated with a randomly generated binary key. Other training non-genuine patterns have been experimentally determined using the metric of Hamming distance by taking iris codes belong to other classes which are far enough to the class' reference iris code. Each non-genuine iris code is associated with a randomly constructed non-genuine key. Once the training phase is complete, the learned weights were stored in the system storage. The reference iris code for each iris is XORed with its associated key to construct the final stored cancelable template. Table 2 summarizes the simulated experiments parameters' values. The output binary iris array was reshaped to be formed into reference binary code by combining each array rows one followed by another. This binary iris vector and another binary sequence (key) with the same length were utilized to compose BAM network structure with set of patterns p, where the lengths of both the stored cancelable template and the input binary iris vector are equal.

To detect the appropriate number of associated pattern pairs p which achieve high recognition performance, various experiments were executed. For each experiment, a sample of ten classes has been randomly selected from CASIA-Iris V3-Interval to testify the best number of patterns p. These experiments have been done using various number of patterns (e.g. $p = 5, p = 10, p = 30, p = 70$). Figure 2 shows the impostor and genuine matching score distributions using the metric of hamming distance from all possible comparisons. The separability between genuine and impostor distributions is measured by the decidability metrics d' [22] computed by:

$$d' = \frac{|\mu_i - \mu_g|}{\sqrt{\frac{\sigma_i^2 + \sigma_g^2}{2}}} \tag{17}$$

where μ_i and μ_g are the means and σ_i^2 and σ_g^2 are the variances of the impostor and genuine distributions, respectively. The larger decidability metrics d' value, the larger separation between impostor and genuine distributions which indicates better recognition performance. As shown in Figure 2, the obtained values of the decidability metric are 2.708, 2.56, 2.53 and 2.25 for $p = 5, p = 10, p = 30$, and $p = 70$, respectively. From security perspective, the security of our proposed scheme depends upon number of associated patterns p, i.e., the larger p value, the more efforts needed to disclose the saved cancelable template (as previously explained in Section 3). To balance both of security and recognition performance constraints for the experiment, the number of patterns is suggested to be 30.

The recognition accuracy of our proposed method is evaluated using the receiver operation characteristic (ROC) curves. Figure 3 illustrates the ROC curves of the protected iris code compared to the unprotected (genuine) codes applied on the entire CASIA-V3 iris database. The EER(%) of the genuine unprotected iris code is 1.78; the EER(%) of XORed protected iris code is 2.001, lower EER value indicates high recognition performance. As can be seen in Figure 3, our proposed scheme achieved a recognition performance comparable to the genuine unprotected system.

To compare our proposed work with other existing cancelable biometric schemes. Several cancelable schemes: Teoh [34], Rathgeb [27], Ouda [21] and Mayada [32] were selected. Table 3 illustrates this comparison form perspectives of security and performance. Moreover, the recognition accuracy comparisons are graphed using ROC curves

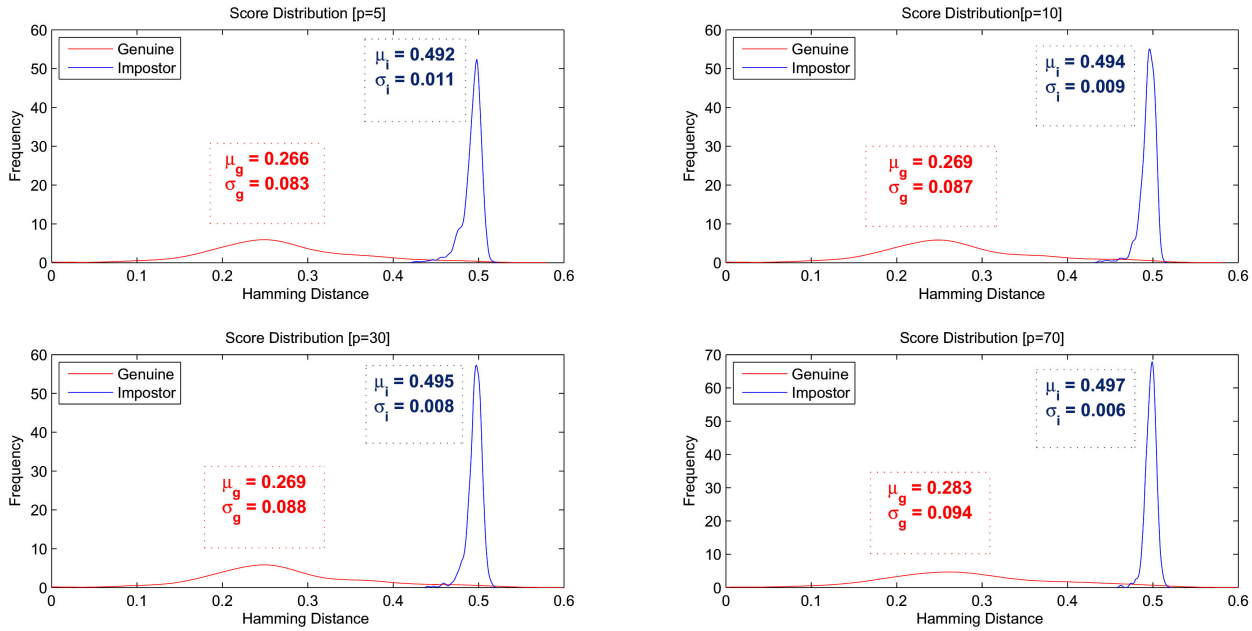

Figure 2: Impostor and genuine score distributions for different number of patterns (p)

Table 3: A comparative study analysis

Scheme	Security Strength	Pre-image attack	Performance (EER%)
Teoh [34]	Based on Token	Not protected	4.81
Rathgeb [27]	Based on secret key	Not protected	8.98
Ouda [21]	Based on public key	Not protected	5.54
Mayada [32]	Based on hidden key	Protected	3.56
Proposed	Based on hidden key	Protected	2.001

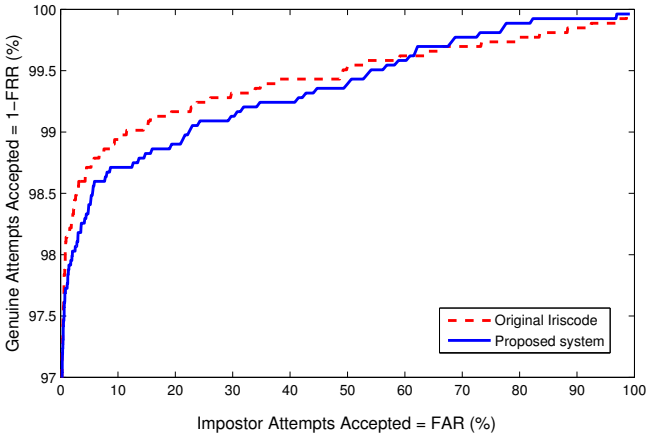

Figure 3: ROC curves of proposed and the unprotected methods

as shown in Figure 4. All experiments applied on CASIA-V3 iris database where recognition performance relies on biometric data rather than the dependency on key/token as recommended in [11].

We can infer that, our proposed work is pre-image resistant scheme with the privilege of high recognition performance.

5 Conclusions

This paper proposed a pre-image resistant cancelable biometric scheme which depends on hiding the cancelable transformation parameters in an associative memory. Bidirectional associated memory network is utilized to associate each user biometric features with his genuine transformation key to encode them in connection weights. The connection weights could be safely saved in the central storage with the XORed template between the biometric features and its associated transformation key which represent the cancelable template. The security requirements of this proposed work is guaranteed while the saved connection weights can't expose the genuine biometric data or on approximate version of it, also, transformation key is secured. Additionally, our proposed scheme does not require carrying or remembering transformation key during the verification process. Evaluation analysis in terms of revocability, diversity and non-invertability shows that our proposed scheme satisfies all these proprieties. Additionally the scheme achieves high recognition

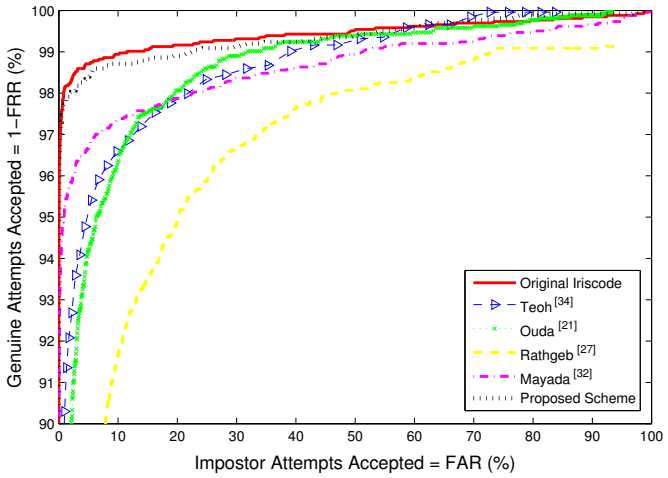

Figure 4: ROC curves of the proposed and existing cancelable biometrics schemes

accuracy when applied to CASIA-IrisV3-Interval dataset.

References

[1] M. H. Almourish, "Image recognition using bidirectional associative memory and fuzzy image enhancement," *Journal of Science and Technology*, vol. 19, no. 1, 2014.

[2] M. G. Barrero, J. Fierrez, J. Galbally, E. Maiorana, and P. Campisi, "Implementation of fixed-length template protection based on homomorphic encryption with application to signature biometrics," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, pp. 191–198, 2016.

[3] R. Belguechi, A. Hafiane, E. Cherrier, and C. Rosenberger, "Comparative study on texture features for fingerprint recognition: application to the biohashing template protection scheme," *Journal of Electronic Imaging*, vol. 25, no. 1, 2016.

[4] P. Campisi, E. Maiorana, and A. Neri, "Iris template protection," in *Encyclopedia of Biometrics*, pp. 1057–1065, 2015.

[5] CASIA, *CASIA Iris Image Database*, Sept. 2016. (`http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Iris`)

[6] A. I. Desoky, H. A. Ali, and N. B. Abdel-Hamid, "Enhancing iris recognition system performance using templates fusion," *Ain Shams Engineering Journal*, vol. 3, no. 2, pp. 133–140, 2012.

[7] N. Evans, S. Marcel, A. Ross, and A.B.J. Teoh, "Biometrics security and privacy protection," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 17–18, 2015.

[8] S. V. Gaddam and M. Lal, "Efficient cancellable biometric key generation scheme for cryptography," *International Journal of Network Security*, vol. 11, no. 2, pp. 61–69, 2010.

[9] T. Gerbet, A. Kumar, and C. Lauradoux, "The power of evil choices in bloom filters," in *45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'15)*, 22-25 June 2015.

[10] O. Kaiwartya, M. Prasad, S. Prakash, D. Samadhiya, A. H. Abdullah, and S. O. Abd Rahman, "An investigation on biometric internet security," *International Journal of Network Security*, vol. 19, no. 2, pp. 167–176, In Press, 2017.

[11] A. Kong, K. H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of biohashing and its variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359–1368, 2006.

[12] P. Lacharme, "Analysis of the iriscodes bioencoding scheme," *International Journal of Computer Science and Security*, vol. 6, no. 5, pp. 315–321, 2012.

[13] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[14] Y. Lee, Y. Chung, and K. Moon, "Inverse operation and preimage attack on biohashing," in *Proceedings of The International IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications*, pp. 1–8, Nashville, TN, 2009.

[15] C. T. Li and M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 5, pp. 2181–2188, 2010.

[16] Y. Liu, "Biohashing for human acoustic signature based on random projection," *Canadian Journal of Electrical and Computer Engineering*, vol. 38, no. 3, pp. 266–273, 2015.

[17] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to online signature recognition," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 40, no. 3, pp. 525–538, 2010.

[18] L. Masek and P. Kovesi, "Matlab source code for a biometric identification system based on iris patterns," Tech. Rep. RFC 2627, The School of Computer Science and Software Engineering, Western Australia University, 2003.

[19] A. Nagara, K. Nandakumar, and A.K. Jain, "Biometric template transformation: A security analysis," in *Proceedings of The SPIE, Electronic Imaging, Media Forensics and Security XII,* pp. 1–15, San Jose, USA, 2010.

[20] D. C. L. Ngo, A. B. J. Teoh, and J. Hu, *Biometric Security*, Cambridge Scholars Publishing, 2015.

[21] O. Ouda, N. Tsumura, and T. Nakaguchi, "A reliable tokenless cancelable biometrics scheme for protecting iriscodes," *IEICE Transaction on Information and Systems*, vol. E93-D, no. 7, pp. 1878–1888, 2010.

[22] O. Ouda, N. Tsumura, and T. Nakaguchi, "On the security of bioencoding based cancelable biometrics," *IEICE Transaction on Information and Systems*, vol. E94-D, no. 9, pp. 1768–1778, 2011.
[23] 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.
[24] 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.
[25] N. K. Ratha, J. H. Connell, R. M. Bolle, and S. Chikkerur, "Cancelable biometrics: a case study in fingerprints," in *Proceedings of The 18th International Conference on Pattern Recognition*, pp. 1–13, Hong Kong, 2006.
[26] C. Rathgeb, F. Breitinger, H. Baier, and C. Busch, "Towards bloom filter-based indexing of iris biometric data," in *IEEE International Conference on Biometrics (ICB'15)*, pp. 422-429, 2015.
[27] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier, "On the application of bloom filters to iris biometrics," *IET Journal on Biometrics*, vol. 3, no. 4, pp. 207–218, 2014.
[28] C. Rathgeb and C. Busch, "Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters," *Elsevier Computers and Security*, vol. 42, pp. 1–12, 2014.
[29] C. Rathgeb and A. Uhl, "Secure iris recognition based on local intensity variations," in *Proceedings of The International Conference on Image Analysis and Recognition*, pp. 266–275, Portugal, 2010.
[30] M. Savvides, V. kumar, and P.K. khosla, "Cancelable biometric filters for face recognition," in *Proceedings of The 17th International Conference on Pattern Recognition*, pp. 922–925, USA, 2004.
[31] M. A. Syarif, T. S. Ong, A. B. J. Teoh, and C. Tee, *Improved Biohashing Method Based on Most Intensive Histogram Block Location*, pp. 644–652, Springer, 2014.
[32] M. Tarek, O. Ouda, and T. Hamza, "Robust cancelable biometrics scheme based on neural networks," *IET Journal on Biometrics*, vol. 5, no. 3, pp. 220–228, 2016.
[33] A. B. J. Teoh and L. Y. Chong, "Secure speech template protection in speaker verification system," *Speech Communication*, vol. 52, no. 2, pp. 150–163, 2010.
[34] A. B. J. Teoh, D. C. L. Ngo, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.
[35] G. Zakar, *Artificial Neural Networks*, CreateSpace Independent Publishing Platform, 2016.
[36] J. Zuo, N. K. Ratha, and J. H. Connel, "Cancelable iris biometric," in *Proceedings of The 19th International Conference on Pattern Recognition*, pp. 1–4, NY, USA, 2008.

Biography

Mayada Tarek received her B.S. degree in 2007 and her M.S. degree in 2011, both in Department of Computer Science, Mansoura University, Egypt. She is currently pursuing here Ph.D. degree in Computer Science. Here current research interests include Pattern Recognition, Information Security, Biometrics, and Soft Computing Techniques.

Osama Ouda received his B.S. in Computer Science from Mansoura University, Egypt, in 2000, his M.S. in Computer Science from Ain-Shams University, Egypt, in 2007, and his Ph.D. in Computer and Information Sciences from Chiba University, Japan, in 2011. From November 2013 to May 2014, he was a research fellow at iPRoBe laboratory, Michigan State University, East Lansing, USA. Currently, he is an assistant professor in the Department of Information Technology, Mansoura University, Egypt. Dr. Ouda is a member of IEEE since 2011. His research interests include information security, biometrics, image processing and machine learning.

Taher Hamza received his B.S degree in 1975 and his M.S. degree in 1979, both in Department of Mathematics, Mansoura University, Egypt. Ph.D degree in 1986 from St Andrews University, Scotland, UK. His current research interests include Artificial Intelligence, Expert Systems, Biometrics, and Machine Learning.