Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.027139
Article

Tech Science Press

Face Templates Encryption Technique Based on Random Projection and Deep Learning

Mayada Tarek[1,2,*]

[1]Department of Computer Science, Mansoura University, Mansoura, 35516, Egypt
[2]Department of Computer Science, Jouf University, Jouf, 2014, KSA
*Corresponding Author: Mayada Tarek. Email: mtelghaysha@ju.edu.sa
Received: 11 January 2022; Accepted: 14 March 2022

Abstract: Cancellable biometrics is the solution for the trade-off between two concepts: Biometrics for Security and Security for Biometrics. The cancelable template is stored in the authentication system's database rather than the original biometric data. In case of the database is compromised, it is easy for the template to be canceled and regenerated from the same biometric data. Recoverability of the cancelable template comes from the diversity of the cancelable transformation parameters (cancelable key). Therefore, the cancelable key must be secret to be used in the system authentication process as a second authentication factor in conjunction with the biometric data. The main contribution of this paper is to tackle the risks of stolen/lost/shared cancelable keys by using biometric trait (in different feature domains) as the only authentication factor, in addition to achieving good performance with high security. The standard Generative Adversarial Network (GAN) is proposed as an encryption tool that needs the cancelable key during the training phase, and the testing phase depends only on the biometric trait. Additionally, random projection transformation is employed to increase the proposed system's security and performance. The proposed transformation system is tested using the standard ORL face database, and the experiments are done by applying different features domains. Moreover, a security analysis for the proposed transformation system is presented.

Keywords: Cancelable biometrics (CBs); random projection; ORL face database; generative adversarial network (GAN)

1 Introduction

Each individual has a unique biometric trait that can be used to recognize his identity. Many biometric traits are used such as fingerprint, face, iris, signature, voice, palm print, gait, and keystroke which can be categorized as physical/behavioral traits [1]. Therefore, biometrics is used in the authentication process for many applications such as Airports, banks, etc. (Biometric for Security). Compared to the traditional authentication scheme which depends on passwords or tokens, biometric traits can't be stolen or forgiven or shared or lost. On the other hand, human biometrics can't be changed if his stored traits' data are stolen (Security for Biometric) [1]. To overcome this challenge, a biometrics template protection scheme

is proposed [2]. Cancelable Biometrics is one categorization of the Template Protection scheme which provides the ability to guarantee the security of the biometric data [2,3].

Cancelable biometrics achieves high biometric security and privacy by matching the biometric template in the transformed domain at the authentication process. Hence, there are two main phases in each biometric authentication system: The enrollment phase (training) and the authentication phase (testing) [1]. During the enrollment phase, the original biometric trait is captured and stored in the system database. On the other hand, in the authentication phase, the system matches this stored biometric with a live version of the same person's biometric trait (test biometric) [2]. The cancelable transformation process must satisfy the following criteria [1,2,4]:

- The original biometric data can't be revoked from the transformed one (Non- invertibility).
- It should be able to produce different transformed versions from the same original biometric data (Recoverability) by the ability to change the transformation parameters value (Diversity).
- The transformed versions must not be identical, where they can be used across multiple authentication systems without cross-matching (Unlinkability).
- The overall system performance using the transformed template must be maintained (Recognition Performance).

Various Cancelable biometrics schemes have been proposed by researchers which are categorized as Biometric Salting and Non-invertible transformation [2]. In the non-invertible transformation, the cancelable transformed template is generated by applying a one-way non-invertible transform to the original biometric data. Using changeable transformation parameters, the system recoverability is achieved [3]. However, non-invertible transform has the advantage that the original biometric never be reconstructed even if the transform is compromised, the recognition performance is degraded after transformation due to the information lost which is caused by the non-invertible transformation [5]. On the other hand, in Biometric Salting, the recognition performance is maintained, since user-specific data (password/random key) is combined with the original biometric data to generate the cancelable transformed template [2]. Although the used transformed key helps to achieve the diversity, recoverability, and unlinkability of the cancelable scheme, it causes some security issues if it is stolen [6,7].

There are many methods used to generate cancelable biometric templates such as Random Projection, Cancelable biometric filters, Biohashing, Permutation, Bio-convolving, and Bloom filters [1]. In Random Projection, the biometric features are projected into a random sub-space [8] where the distance between biometric features in the original and transformed domain is guaranteed. A cancelable iris template is generated by random projection in [9,10], where the random projection is applied separately with each iris sector and then combined to create the final cancelable template. Another cancelable iris template is based on Johnson-Lindenstrauss (JL) lemma for random projection to increase recognition performance [8]. In [11], Cancelable biometric filters are generated by convolving the biometric data with a random convolution kernel where different cancelable filters can be recovered using different convolution kernels in case of system compromising. Biohashing is an extended version of the random projection method where the cancelable template is generated from the inner product between the biometric feature and orthogonal vectors created from the random user-specific key as proposed in [12]. The Permutation process is another model used to create a cancelable template by randomly permuting the biometric features using some auxiliary data [3]. In [13], the iris texture features are shifted and the rows are combined to generate the cancelable template. Also, randomly permuted sector features are combined as proposed in [10]. In Bio-convolving method, a set of sequence cancelable template are generated from a set of sequence original biometric data [14]. Whilst, the Bloom filter process is proposed [15,16] to achieve a fast biometric query processing in which the cancelable iris template is generated using an adaptive bloom filter method.

All of the mentioned cancelable biometric methods are categorized as two-factor authentication schemes. It depends on using a cancelable key along with the biometric data in the authentication phase. Hence, this cancelable key can cause much security vulnerability in case of compromising/stolen/shared or Lost. Therefore, authentication schemes that depend only on biometric data in the authentication phase are needed.

The one-factor authentication schemes are proposed to overcome the problems of using the cancelable key in the authentication phase by using the cancelable key only in the enrollment phase [17]. The bio-encoding scheme is proposed in [18], it stores the cancelable key publicly in the system database along with the cancelable template. Other one-factor authentication schemes are proposed in [19,20], they suggested storing an encrypted cancelable key along with the cancelable template using a Hetro-Association Network model. Although those schemes are categorized as one-factor authentication systems and the cancelable key is used only in the enrollment phase, their high recognition performance depended on the value of the cancelable key rather than the biometric trait itself.

Tarek et al. [21,22] proposed one-factor cancelable authentication system that depended only on the biometric trait data in both the enrollment and authentication phases using the standard GAN model where the cancelable key is a random permuted version from the biometric feature trait. Although the proposed schemes increase the recognition performance by depending only on biometric trait, the security of the proposed system needs to be maximized.

This paper proposes a more secure version of the proposed cancelable schemes in [21,22] based on the standard GAN model. The standard GAN model is suggested here as the cancelable transformation model followed by a random projection transform process for increasing the system's security. GAN model contains pair of competitive networks in its architecture (Generator/Discriminator) network [23]. During the enrollment phase, samples from the training set are fed into the generator networks, and a random permuted version from one training sample acts as the cancelable key is fed into the discriminator network. After the training process, a transformed version from the original biometric trait is generated from the generator network. For additional security purposes, another step of transformation is needed. A random projection transformation is performed between this generator network's output and the mean computed values of all original biometric trait (Generator's input) to generate the final stored cancelable template. Additionally, the final generator's weight values are stored in the system database along with the cancelable template. On the other hand, during the authentication phase, only one live biometric sample is needed to feed into the generator network using its stored weight values to generate the transformed biometric template. Eventually, to generate the test cancelable template, a random projection transformation between the transformed biometric template (Generator's output) and the test biometric is performed. The test cancelable template is compared with the stored one.

The rest of this paper is organized as follows Section 2 discusses the main concept for the standard GAN model, and the Random Projection concept. The proposed cancelable scheme is described in Section 3. Section 4 discusses the security attack analysis for the proposed scheme. The performance results for the proposed scheme are covered in Section 5. Finally, Section 6 concludes the papers' work.

2 Related Work

In this section, the basic information about the Standard GAN model and Random Projection techniques and their roles in the cancelable biometric schemes are described.

2.1 Generative Adversarial Network

GAN is a type of deep machine learning tools which has a powerful learning framework to generate a new sample from a given distribution [24]. The GAN model is composed of a pair of networks

(Generative/Discriminator) [23]. The generative network is responsible for learning a training dataset and generating a new sample, while the discriminator's role is to distinguish between the real sample and the other sample generated from the generative network. During the GAN training process, it is a competitive process between the two networks, because the generator network tries to generate a new sample that can't be distinguished from the real one and the discriminator network tries to discover the non-real one [25]. For providing more details about how the GAN model work, the generator network, $\boldsymbol{G}$, learns the mapping from an input distribution $\boldsymbol{z}$ to a new generated distribution $\boldsymbol{y}$ with a similar look to the real sample, $\boldsymbol{G}: \boldsymbol{z} \rightarrow \boldsymbol{y}$. While the discriminator network, $\boldsymbol{D}$, tries to distinguish the generator's output sample from the real one $\boldsymbol{x}$, $\boldsymbol{D}: \boldsymbol{x} \rightarrow (0, 1)$ [24,25].

The generator's and the discriminator's network can be trained jointly in a min-max game. Where, $\boldsymbol{D}$ tries to maximize its classification ability between real and generator's output sample, while $\boldsymbol{G}$ tries to minimize the discriminator's distinguishably. The traditional back-propagation algorithm can be used in the training process for the standard GAN model using the following objective function [25]:

$$\min_{G} \max_{D} V(D, G) = E_{x \sim p_{data}(x)}[log\ D(X)] + E_{z \sim p_{data}(z)}[log\ (1 - D(G(Z))] \tag{1}$$

GAN can be used in various applications such as classification, image synthesis, semantic image editing, image super-resolution, and style transfer [23]. One of these applications applied in the biometrics field is image synthesis. Synthesizing a realistic biometric image based on a random sample such as fingerprint [25], iris [26], and face [27]. On the other hand, the GAN model can be used in the biometric template security field for generating a permuted-indexing cancellable biometric to protect the stored biometric template [28].

2.2 Random Projection

Random Projection is utilized to be used as a cancelable transformation for creating cancelable biometric template as proposed in [8,29]. Random Projection for a biometric authentication system is done by the multiplication of the biometric feature vector with a random matrix as shown in Eq. (2), where $\boldsymbol{X}$ is the biometric feature vector, $\boldsymbol{M}$ is a random matrix, and $\boldsymbol{Y}$ is the cancelable biometric template [8].

$$\boldsymbol{Y} = \boldsymbol{X}.\boldsymbol{M} \tag{2}$$

The main idea of the random projection is to guarantee that the estimated distance between the generated feature vectors after projection is larger than or equal to the estimated distance between the original biometric feature vectors [8]. Although, random projection preserves the discriminability, it is used as an invertible transformation to estimate the original biometric feature if the final cancelable template and the random matrix are comprised [12,30]. Various approaches are proposed in order to overcome this security drawback such as Random Mutlispace Quantization (RMQ) [31], Multispace Random Projections (MRP) [32], and User-dependent Multi-state Discretization (Ud-MsD) [33].

3 The Proposed Methodology

The main contribution of the proposed work is to suggest a cancelable one-factor authentication system based only on the biometric trait. However, the cancelable properties of diversity, recoverability, and unlikability are achieved using another authentication factor that can be easily changeable (cancelable key). The proposed scheme is a transformation process that is trained using a two-authentication factor and tested with only one-authentication factor. GAN is suggested to perform the transformation role by using both GAN's networks in the training phase and using only one of them in the testing phase, i.e., the generator and discriminator networks are used to train the GAN model and the final GAN output is

produced from the generator output. The training phase uses the biometric trait samples as an input to the generator network and the cancelable key as an input to the discriminator network. This cancelable key is generated by randomly permuting one biometric training sample to achieve the full dependency on the biometric trait without any other factors.

After training both networks alternatively, the generator's output is fed to a random projection process to generate the final transformed template. The random projection process uses the mean of all biometric training samples to guarantee the non-invertibility properties and the high recognition performance. Fig. 1 illustrates the proposed scheme.

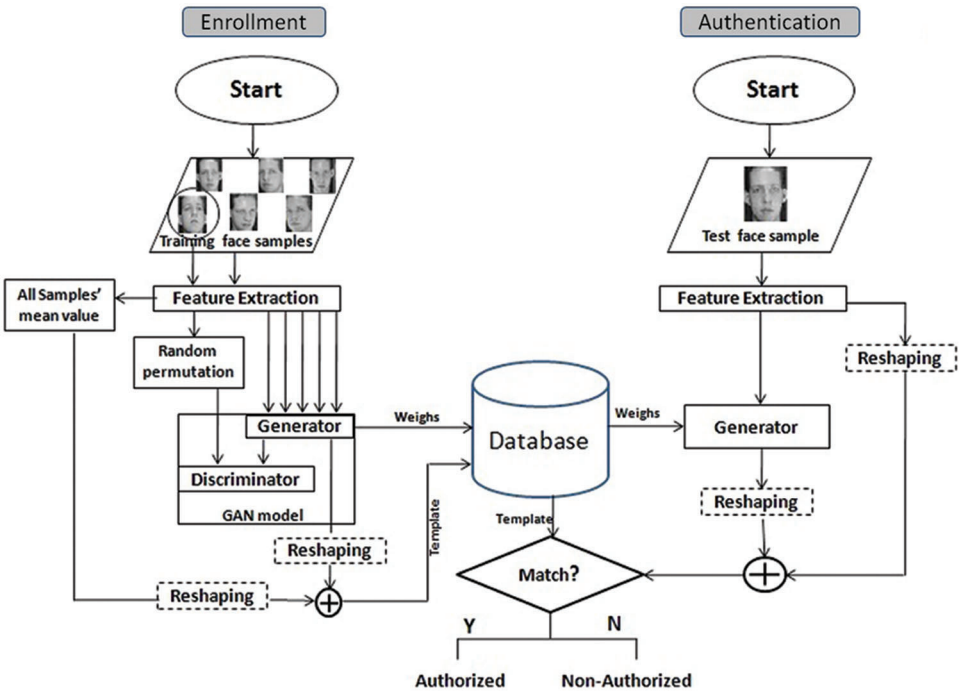

Figure 1: Flowchart of the proposed scheme

Due to the reversibility property of the GAN model [34,35], the original biometric sample can be regenerated from the transformed biometric using the stored generator's weight values. This property threatens the security of the biometric system; therefore, an additional transformation process to the transformed biometric is suggested. A random projection transformation is performed between the transformed biometric produced by the GAN model and a reference biometric template representing all the biometric samples. The reference template is computed by the average of all the input biometric trait samples values, each of size $\boldsymbol{1 \times n}$. In order to apply the projection process, the transformed GAN output and the reference template must be reshaped. The transformed template is reshaped into a matrix of size $(\boldsymbol{o \times p})$, and the reference template is reshaped into a matrix of size $(\boldsymbol{p \times o})$, where $(\boldsymbol{o \times p = n})$. Then, the projection transformation is applied between the reshaped matrices to generate a matrix of size $(\boldsymbol{p \times p})$ representing the final stored cancelable template. The enrollment process steps are illustrated in Algorithm 1.

During the authentication process, the test biometric sample is only needed to represent the personal identity. The test biometric template is generated by applying the same feature extraction method on the

input biometric trait. Then, the test template is fed into the generator network using the stored generator's weight values to produce the transformed template.

After that, the test and the transformed templates are reshaped into ($\boldsymbol{p} \times \boldsymbol{o}$) and ($\boldsymbol{o} \times \boldsymbol{p}$) matrices to apply the projection transformation process and produce the final test cancelable template. Eventually, an authentication decision is made according to the Euclidian distance between the final test cancelable template and the stored one of the claimed identity. The Authentication process steps are illustrated in Algorithm 2.

Algorithm 1: Proposed Scheme's Enrollment Phase

Input: A set of $\boldsymbol{m}$ training samples $\{S_1,\ldots, S_m\}$, $\boldsymbol{T}$: the number of training epochs for the GAN model, ***alpha***: the learning rate for the GAN model, $\boldsymbol{h_1}$: the generator network's hidden layer size, $\boldsymbol{h_2}$: the discriminator network's hidden layer size.

1: Randomly select a template $\boldsymbol{S_r} : \boldsymbol{r} \in \{\boldsymbol{1,\ldots, m}\}$.

2: Create a cancelable key $\tilde{\boldsymbol{S}}_{\boldsymbol{r}}$, a permutated version of $\boldsymbol{S_r}$

3: Create a reference template $\boldsymbol{S_{mean}}$ for each enrolled person using the input training templates using equation:

$$S_{mean}(i) = \frac{1}{m}\sum_{l=1}^{m} S_l^i \tag{3}$$

4: Create $\boldsymbol{S_{ref}}$ by reshaping vector $\boldsymbol{S_{mean}}$ into 2-D Matrix of size ($\boldsymbol{p} \times \boldsymbol{o}$) where ($\boldsymbol{p} \times \boldsymbol{o} = \boldsymbol{n}$).

5: Construct a fully connected multilayer generator network of size [$\boldsymbol{n} \times \mathbf{h}1 \times \boldsymbol{n}$].

6: Construct a fully connected multilayer discriminator network of size [$\boldsymbol{n} \times \mathbf{h}2 \times \boldsymbol{1}$].

7: Randomly initialize generator network's weight matrix, $\boldsymbol{W_g}$

8: Randomly initialize discriminator network's weight matrix, $\boldsymbol{W_d}$

9: Train the generator and the discriminator network alternatively using the back prorogation algorithm using $\{S_1,\ldots, S_m\}$ inputs for the generator network and $\tilde{\boldsymbol{S}}_{\boldsymbol{r}}$ input to the discriminator network.

10: After $\boldsymbol{T}$ epochs of training, retrieve generator network's output, $\boldsymbol{E}$.

11: Create $\boldsymbol{E_{ref}}$ by reshaping vector $\boldsymbol{E}$ into 2-D Matrix of size ($\boldsymbol{o} \times \boldsymbol{p}$) where ($\boldsymbol{o} \times \boldsymbol{p} = \boldsymbol{n}$) .

12: Generate the cancelable template, $\boldsymbol{T_{ref}}$ a ($\boldsymbol{p} \times \boldsymbol{p}$) matrix using equations:

$$T_{ref} = S_{ref} \oplus E_{ref} \text{ [where } \oplus \text{ indicates the projection operation]} \tag{4}$$

13: Store $\boldsymbol{W_g}$ and $\boldsymbol{T_{ref}}$ in the authentication system's database.

Output: Store $\boldsymbol{W_g}$ matrix of size ($n \times \boldsymbol{h_1} \times n$) and $\boldsymbol{T_{ref}}$ matrix of size ($\boldsymbol{p} \times \boldsymbol{p}$)

4 Security Analysis

This section presents an analytical study of the proposed scheme from security points of view. The study includes recoverability, diversity, un-linkability, and non-invertibility properties that must be satisfied for any cancelable biometric scheme. Moreover, a security analysis against some possible security attackers is presented.

4.1 Recoverability, Diversity, and Un-Linkability

A cancelable biometric scheme is said to be recoverable if it is easy to revoke a new cancelable template from the same biometric trait in case of the system storage is compromised. This can be easily achieved in the proposed scheme by generating a new version of the discriminator input (cancelable key).

Since the cancelable key is a random permuted version for a selected biometric sample, there are many versions of the cancelable key that could be generated from the same biometric trait. Therefore, our proposed scheme satisfies the recoverability propriety with a number of ***n!*** possible permutations to a biometric sample of size ***n***. In other words, each person has different ***n!*** cancelable templates using different ***n!*** cancelable keys. Therefore, the proposed scheme satisfies the diversity propriety across various authentication systems using the same biometric trait.

The transformation of the GAN model mainly depends on the discriminator input (real image) rather than the generator input (random noise). Since the cancelable template depends on the cancelable key value which is derived from the original biometric trait, therefore, there are different ***n!*** cancelable key across various authentication systems for the same biometric trait that are un-linkable to each other. Therefore, the proposed scheme satisfies the un-linkability propriety.

Algorithm 2: Proposed Scheme's Authentication Phase

Input: A testing sample $\boldsymbol{K_{test}}$

Database Retrieval: $\boldsymbol{W_g}$ and $\boldsymbol{T_{ref}}$ from system's database.

1: Generate $\boldsymbol{P_{test}}$ using $\boldsymbol{K_{test}}$ and the retrieved $\boldsymbol{W_g}$ by applying the following equation:

$$P_{\text{test}} = \text{K}_{\text{test}}.\ W_g \tag{5}$$

2: Create $\boldsymbol{E_{test}}$ by reshaping the vector $\boldsymbol{P_{test}}$ into 2-D Matrix of size $(\boldsymbol{o} \times \boldsymbol{p})$.

3: Create $\boldsymbol{S_{test}}$ by reshaping the vector $\boldsymbol{K_{test}}$ into 2-D Matrix of size $(\boldsymbol{p} \times \boldsymbol{o})$.

4: Generate the cancelable test template, $\boldsymbol{T_{test}}$ a $(\boldsymbol{p} \times \boldsymbol{p})$ matrix using equation:

$$\mathbf{T}_{test} = \mathbf{S}_{test} \oplus \mathbf{E}_{test} \ \text{[where} \oplus \text{indicates the projection operation]} \tag{6}$$

5: Compare the test and the reference cancelable template for the input claimed user identity $\boldsymbol{I}$ using the Euclidian distance, as follows:

$$\epsilon = \sqrt{\sum_{1<i,\ j<p} \left(\mathbf{T_{ref}}(i,\ j) - \ \mathbf{T_{test}}\ (i,\ j)\ \right)^2} \tag{7}$$

6: Decision making for $\boldsymbol{I}$:

$$\text{Decision} = \begin{cases} Non-authorized & \epsilon > \theta \\ Authorized & \epsilon \leq \theta \end{cases} \tag{8}$$

Output: Authorized/Non-authorized message.

4.2 Non-invertibility

Non-invertibility is one of the main important constraints for any cancelable scheme. A cancelable scheme is said to be non-invertible if there is no way to extract the original biometric trait from the authentication system's stored data for the same person. The stored parameters in the proposed scheme are the generator's weights values and the produced projection between the generator's output and a reference template from the input biometric trait. Firstly, as mentioned in [19] based on a mathematical

analysis study, the generator's weight values alone can't be used to recover any information about its network's input or output. Secondly, we can't recover any information about the biometric trait (the second input of the projection process) from the cancelable template (the output of the projection process) without having any information about the generator output (the first input of the projection process). Since the generator's output can't be recovered from the stored generator's weight values, and the original biometric trait can't be recovered from the cancelable template, therefore, the proposed scheme satisfies the non-invertibility propriety.

4.3 Possible Security Attacks

There are many types of attacks threat for any cancelable scheme that relies on the stored auxiliary data in the authentication system's database. The main types of these attacks are listed as follows:

4.3.1 Brute Force Attack

An attacker tries every possible solution in the solution space until he finds the biometric template that works as the original one. A cancelable scheme is said to be secured if this attack is computationally infeasible and if there is no other attack that is computationally less expensive than it. According to the proposed scheme, the maximum number of trials needed to reach the biometric template by random guessing is equal to 2^{n} for a binary biometric template of size n and it is computationally infeasible for a real-valued biometric template.

4.3.2 Known Key Attack

An attacker tries to extract the original biometric data from the stored auxiliary data using the stolen cancelable key [1]. In the proposed scheme, there are no external passwords or physical tokens that can be stolen. Also, based on the non-invertibility analysis, there is no way to recover any information about the cancelable key from the stored auxiliary data (the cancelable template and the generator's weights values). Therefore, the proposed scheme is robust against the known key attack.

4.3.3 Pre-image Attack

An attacker tries reconstructing a sufficient similar biometric trait (fake template) which is act as a real one using the stored auxiliary data [18]. This can be achieved by creating a test cancelable template similar to the stored one for any person's identity. From the previous non-invertibility study, there is no useful information that can be extracted from the stored auxiliary data. Therefore, the construction of a pre-image biometric template is computationally as hard as random guessing (the brute force attack). 2^{n} maximum number of trials is needed for a binary biometric template of size n, and it is computationally infeasible for a real-valued biometric template of the same size.

4.3.4 Correlation Attack

An attacker tries to extract the original biometric template using multi-stored auxiliary data generated from the same person's identity across multiple authentication systems. To overcome this type of attack, a cancelable template across the multiple-authentication system for the same biometric trait must be un-linkable. The un-linkability property of the proposed scheme is maintained. Various cancelable templates across multiple-authentication systems for the same biometric trait are different and un-linkable, hence each system uses a different permuted version from the biometric data (the cancelable key) and a different initialized version of the GAN networks' weight. Therefore, each authentication system generates a cancelable template using a unique cancelable key and the network's weight initialization values.

5 Experiments

This section analyzes the proposed scheme from the recognition performance point of view based on the ORL face database. These experiments were conducted on different biometric feature types to evaluate the proposed system.

5.1 Experimental Setup

The used database in the simulated experiments is AT&T (ORL) face database, which is consists of 400 images for different subjects, each person has different ten facial images varying in the facial expressions, lighting, and time taken, all images are taken in a dark homogeneous background of size 92×112 pixels and 256 gray levels per pixel [36]. Fig. 2 shows samples of four different classes in the ORL face database. The proposed system performance is analyzed using two different methods for feature extraction. The first method applies the principal component analysis (PCA) [37] to produce real-valued features, while, the second method applies an optimized Genetic algorithm transformation [38] to produce binary-valued features. Two independent experiments are applied to the proposed scheme according to each face feature type. The face feature vector is fed into the generator's and discriminator's networks. The generator's input and output layer have the same number of neurons. Tab. 1 illustrates the parameters of the experiments for both feature extraction methods. The GAN model architecture and the training parameters for each experiment are also shown. The weight values are randomly initialized for the networks in all experiments. From a security point of view, the goal is to minimize the GAN's discrimination ability to create a cancelable template that is similar to the original one, therefore, there are some parameters such as the hidden layer size, the number of training epochs, and the learning rate that are fixed to small values in all experiments.

Figure 2: Samples of AT&T (ORL) face database images

Table 1: Experimental parameters

GAN's parameters for real-valued feature		*GAN's parameters for binary face feature*	
Number of principle component	100	*Binary feature size*	200
Generator's structure	*100 × 32 × 100*	*Generator's structure*	*200 × 32 × 200*
Discriminator's structure	*100 × 32 × 1*	*Discriminator's structure*	*200 × 32 × 1*
Training epochs	50	*Training epochs*	50
Learning rate	*0.00001*	*Learning rate*	*0.00001*

5.2 Recognition Performance Evaluation

The recognition performance of the proposed scheme is evaluated using the Equal Error Rate (EER) value, and the Receiver Operation Characteristic (ROC) curve. The ROC curve is obtained by plotting the system probability of correct acceptance rate (1-FRR) against the probability of incorrect acceptance rate (FAR) across various decision threshold values. FRR (False Rejected Rate) is the proportion of falsely rejected the right biometric data as an impostor (intra-class), and FAR (False Accepted Rate) is the proportion of falsely accepted an impostor biometric data as a genuine one (inter-class). The EER value is the point where the (FAR) and (FRR) are equivalent at a certain threshold value. The EER value is inversely proportional to the system performance, where the low EER value indicated a high recognition performance [19]. During the enrollment process, several training face images are randomly selected from each class. Two types of feature (real and binary) values are extracted from these images using PCA [37] and optimizing GA [38], respectively. In each experiment, the training face features are fed into the generator's network and one of them is selected to be a randomly permuted and fed into the discriminator's network. Tabs. 2 and 3 illustrate the system accuracy in terms of EER (%) values across various reshaping sizes for the binary-valued and the real-valued feature for a face, respectively. Since, $\boldsymbol{p} \times \mathbf{o} = \mathbf{o} \times \boldsymbol{p} = \boldsymbol{n}$ where $\boldsymbol{n}$ is the face feature size with values ***200*** and ***100*** for binary-valued and real-valued face features, respectively. According to the applied projection transformation, the cancelable template size is $\boldsymbol{p} \times \boldsymbol{p}$ where $\boldsymbol{p}$ is chosen to produce the largest dimensional value to enhance both the recognition and the security performances.

Table 2: Binary-valued features experiments' performance across various projection sizes

Reference template reshaping size ($p \times o$)	Transformed template reshaping size ($o \times p$)	Cancelable template size ($p \times p$)	EER%
40 × 5	5 × 40	40 × 40	7.33%
50 × 4	4 × 50	50 × 50	7.88%
100 × 2	2 × 100	100 × 100	4.5%
200 × 1	1 × 200	200 × 200	**3.25%**

Table 3: Real-valued face features experiments' performance across various projection sizes

Reference template reshaping size ($p \times o$)	Transformed template reshaping size ($o \times p$)	Cancelable template size ($p \times p$)	EER%
20 × 5	5 × 20	20 × 20	8.75%
25 × 4	4 × 25	25 × 25	8%
50 × 2	2 × 50	50 × 50	**7.01%**
100 × 1	1 × 100	100 × 100	7.75%

It can be concluded from Tabs. 2 and 3 that the best system's evaluations are cancelable template with size [**50 × 50**] for real-valued face feature experiment, and cancelable template with size [**200 × 200**] for the binary-valued face feature experiment.

Moreover, Figs. 3 and 4 compare the experimental results (EER (%)) for the original binary-valued and the real-valued face feature system. As conducted from Fig. 3, the recognition accuracy for the cancelable template with size [**200 × 200**] for the binary face feature is closest to the original binary face feature recognition accuracy, the EER (%) values for the original unprotected system, and the proposed scheme

are 3.15, 3.25, respectively. Additionally, in Fig. 4, the recognition accuracy for the cancelable template with size [**50 × 50**] for the real-valued face feature is closest to the original real-valued face feature recognition accuracy, the EER (%) values for the original unprotected system, and the proposed scheme are 6.25, 7.01, respectively.

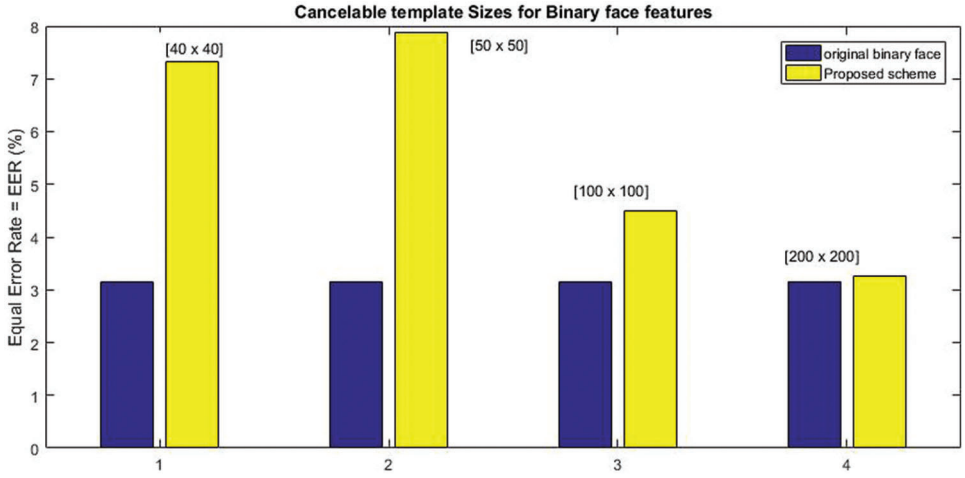

Figure 3: Original binary-valued feature *vs.* Different cancelable template size

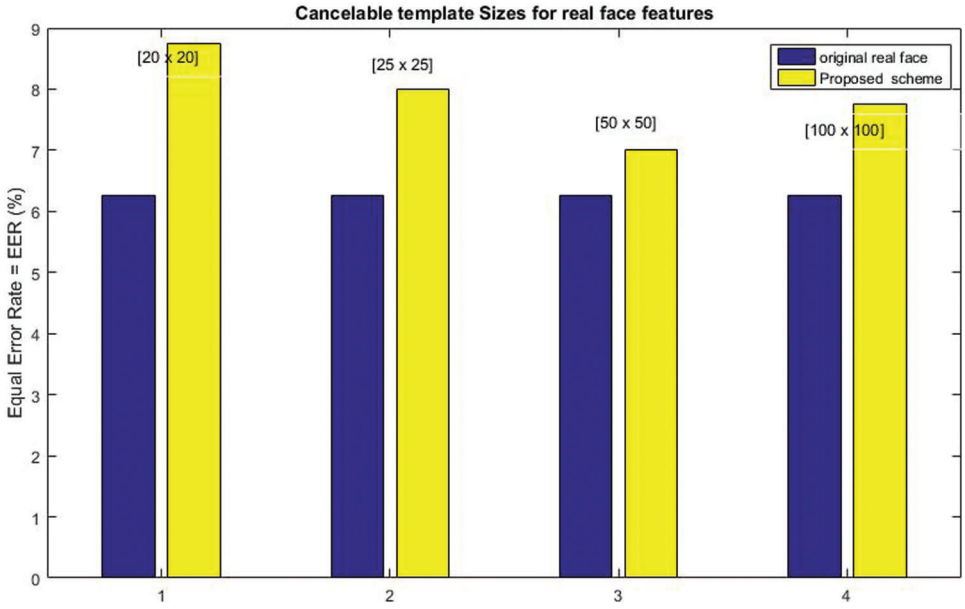

Figure 4: Original real-valued feature *vs.* Different cancelable template size

Moreover, Figs. 5 and 6 represent the receiver operation characteristic (ROC) curves for the recognition performance between the proposed scheme with the best performance compared to the original face system, for the binary-valued and the real-valued features, respectively. The two figures indicate good recognition accuracy for the proposed scheme with small and acceptable recognition degradation.

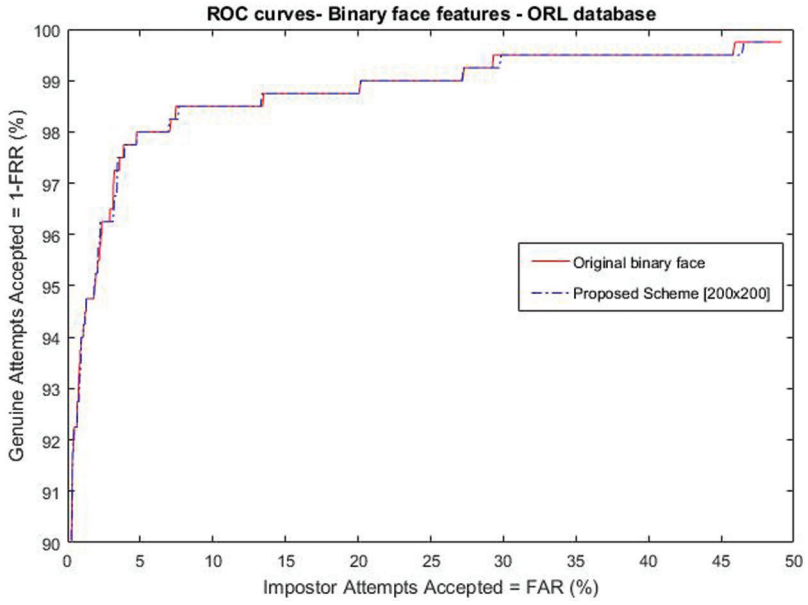

Figure 5: Roc curves for binary-valued feature

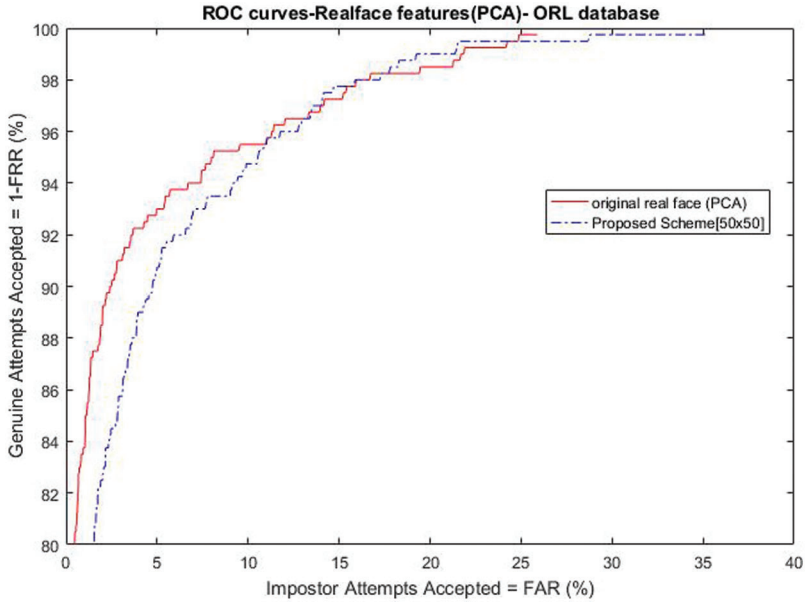

Figure 6: Roc curves for real-valued face feature

Finally, the proposed scheme is compared to the recent well-known cancelable biometric schemes such as Biohashing [12], Bloom filter [15], Bioencoding [18], Hetro Convolved [19], and CB using Random Projection [8]. Tab. 4 illustrates the differences between the applied schemes in terms of the type of the biometric feature, the cancelable key storage place, the recognition accuracy dependency, and the reliability against pre-image and correlation attacks. In summary, the proposed scheme is a robust cancelable biometric scheme for any biometric feature types with a total dependency on the biometric data rather than the cancelable key value.

Table 4: Comparative study analysis

Scheme	Feature type	Key storage	Performance dependency	Pre-image attack	Correlation attack
Biohashing [12]	binary/real	Token	cancelable key value	Unprotected	Unprotected
Bloom filter [15]	Binary	Token	cancelable key value	Unprotected	Unprotected
Bioencoding [18]	Binary	Public in DB	Public key value	Unprotected	Unprotected
Hetro_Convolved [19]	Binary	Hidden in DB	cancelable key value	Protected	Protected
CB with random projection [8]	binary	Token	Biometric data	Protected	Protected
Proposed scheme	binary/real	No key	Biometric data	Protected	Protected

6 Conclusion

This paper proposes a one-factor cancelable biometric authentication scheme that depends only on biometric data in the authentication phase. The cancelable biometrics properties such as recoverability, diversity, and unlinkability are achieved by the changeable cancelable key. The proposed scheme suggests using the cancelable key only in the enrollment phase to reduce the security threats of using this key in the authentication phase. GAN model is suggested here as a transformation function, that enables the use of the cancelable key only in the enrollment phase and authenticating using only the biometric trait. The cancelable key is derived from the biometric data to achieve good recognition performance that mainly depends on the biometric data. For more security and performance achievement, a second stage is suggested as a projection transformation between the GAN output and a reference of the biometric data. The proposed scheme achieves a high recognition performance for different biometric feature types based on the ORL face database with a highly secured performance.

Future work: The author suggests a multi-modal cancelable biometric system based on random projection and deep learning.

Funding Statement: The author received no specific funding for this study.

Conflicts of Interest: The author declares that she has no conflicts of interest to report regarding the present study.

References

[1] B. Choudhury, P. T. Greene, B. Issac, V. Raman and M. K. Haldar, "A survey on biometrics and cancelable biometrics systems," *International Journal Image Graph*, vol. 18, no. 1, pp. 1–39, 2018.

[2] A. k. Jain, K. Nandakumar and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 1, pp. 1–17, 2008.

[3] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 1, pp. 3–25, 2011.

[4] H. Kaur and P. Khanna, "PolyCodes: Generating cancelable biometric features using polynomial transformation," *Multimedia Tools and Applications*, vol. 79, pp. 20729–20752, 2020.

[5] M. Soltane, L. Messikh and A. Zaoui, "A review regarding the biometrics cryptography challenging design and strategies," *Broad Research in Artificial Intelligence and Neuroscience*, vol. 8, no. 4, pp. 42–64, 2017.

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

[7] X. Zhou and T. Kalker, "On the security of BioHashing," *Proceedings of SPIE-The International Society for Optical Engineering*, San Jose, CA, USA, pp. 7541–75410, 2010.

[8] R. F. Soliman, M. Amin and F. E. El-Samie, "A modified cancelable biometrics scheme using random projection," *Annals of Data Science*, vol. 6, no. 5, pp. 223–236, 2019.

[9] J. K. Pillai, V. M. Patel, R. Chellappa and N. K. Ratha, "Sectored random projections for cancelable iris biometrics," in *Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, Dallas, TX, USA, pp. 1838–1841, 2010.

[10] J. K. Pillai, V. M. Patel, R. Chellappa and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Transaction on Pattern Analysis and Machine Intelligence*, vol. 33, no. 9, pp. 1877–1893, 2011.

[11] M. Savvides, B. V. K. Kumar and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Proc. of the 17th Int. Conf. on Pattern Recognition*, Cambridge, UK, vol. 3, pp. 922–925, 2004.

[12] 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.

[13] J. Zuo, N. K. Ratha and J. H. Connel, "Cancelable iris biometrics," in *19th Int. Conf. on Pattern Recognition*, Tampa, FL, pp. 8–11, 2008.

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

[15] C. Rathgeb, F. Breitinger and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *Int. Conf. on Biometrics*, Madrid, Spain, pp. 1–8, 2013.

[16] C. Rathgeb, F. Breitinger, C. Busch and H. Baier, "On the application of bloom filters to iris biometrics," *IET Biometrics*, vol. 3, no. 4, pp. 207–218, 2014.

[17] O. Ouda, N. Tsumura and T. Nakaguchi, "BioEncoding: A reliable tokenless cancelable biometrics scheme for protecting iris codes," *IEICE Trans. Inf. Syst*, vol. 7, pp. 1878–1888, 2010.

[18] O. Ouda, N. Tsumura and T. Nakaguchi, "BioEncoding: Securing bioencoded iriscodes against correlation attacks," in *IEEE Int. Conf. on Communications*, Kyoto, Japan, pp. 1–5, 2011.

[19] M. Tarek, O. Ouda and T. Hamza, "Robust cancelable biometrics scheme based on neural networks," *IET Biometrics*, vol. 5, no. 3, pp. 220–228, 2016.

[20] M. Tarek, O. Ouda and T. Hamza, "Pre-image resistant cancelable biometrics scheme using bidirectional memory model," *International Journal of Network Security*, vol. 19, no. 4, pp. 498–506, 2017.

[21] M. Tarek, E. Hamouda and S. El-Metwally, "Unimodal-bio-GAN: Keyless biometric salting scheme based on generative adversarial network," *IET Biometrics*, vol. 10, no. 6, pp. 654–663, 2021.

[22] M. Tarek, E. Hamouda and A. Abouhamama, "Multi-instance cancellable biometrics schemes based on generative adversarial network," *Applied Intelligence*, vol. 52, pp. 501–513, 2022.

[23] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta *et al.,*"Generative adversarial networks: An overview," *IEEE Signal Processing Magazine*, vol. 35, pp. 53–65, 2018.

[24] I. J. Goodfellow, J. P. Abadie, M. Mirza, B. Xu, D. Warde-Farley *et al.,* "Generative adversarial nets," *Advances in Neural Information Processing Systems*, vol. 3, no. 11, pp. 2672–2680, 2014.

[25] S. Minaee and A. Abdolrashidi, "Finger-GAN: Generating realistic fingerprint images using connectivity imposed GAN," 2018. [Online]. Available: https://arxiv.org/pdf/1812.10482.pdf.

[26] S. Minaee and A. Abdolrashid, "Iris-GAN: Learning to generate realistic iris images using convolutional GAN," 2018. [Online]. Available: https://arxiv.org/pdf/1812.04822.pdf.

[27] G. Mai, K. Cao, P. C. Yuen and A. K. Jain, "On the reconstruction of face images from deep face templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 41, pp. 1188–1202, 2019.

[28] T. Murakami, R. Fujita, T. Ohki, Y. Kaga, M. Fujio *et al.,* "Cancelable permutation-based indexing for secure and efficient biometric identification," *IEEE Access*, vol. 7, pp. 45563–45582, 2019.

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

[30] A. B. J. Teoh, Y. W. Kuan and S. Lee, "Cancellable biometrics and annotation on BioHash," *Pattern Recognition*, vol. 41, no. 6, pp. 2034–2044, 2008.

[31] 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 Trans Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, 2006.

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

[33] A. B. J. Teoh, W. K. Yip and K. A. Toh, "Cancellable biometrics and user-dependent multi-state discretization in biohash," *Pattern Analysis and Applications*, vol. 13, no. 3, pp. 301–307, 2010.

[34] A. Creswell and A. A. Bharath, "Inverting the generator of a generative adversarial network," *IEEE Trans. on Neural Networks and Learning Sys*, vol. 30, pp. 1967–1974, 2018.

[35] F. Ma, U. Ayaz and S. Karaman, "Invertibility of convolutional generative networks from partial measurements," in *32nd Conf. on Neural Information Processing Systems (NeurIPS)*, Montréal, Canada, pp. 1–10, 2018.

[36] ORL face image database AT&T Laboratories. 2001. [Online]. Available: http://cam-orl.co.uk/facedatabase.html.

[37] M. Turk and A. Pentland, "Eigenfaces for recognition," *Journal of Cognitive Neurosicence*, vol. 3, no. 1, pp. 71–86, 1991.

[38] E. Hamouda, O. Ouda, X. Yuan and T. Hamza, "Optimizing discriminability of globally binarized face templates," *Arabian Journal for Science and Engineering*, vol. 41, pp. 2837–2846, 2016.