applied sciences

MDPI

Article

Cancelable Multimodal Biometrics Based on Chaotic Maps

Sanaa Ghouzali [1,*], Ohoud Nafea [2], Abdul Wadood [2] and Muhammad Hussain [3]

[1] Department of Information Technology, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia
[2] Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia; omohammadi@taibahu.edu.sa (O.N.); aabdulwaheed@ksu.edu.sa (A.W.)
[3] Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia; mhussain@ksu.edu.sa
* Correspondence: sghouzali@ksu.edu.sa

Abstract: Biometric authentication systems raise certain concerns with regard to security, violation of privacy, and storage issues of biometric templates. This paper proposes a protection approach of biometric templates storage in a multimodal biometric system while ensuring both the cancelability of biometric templates and the efficiency of the authentication process. We propose applying a chaotic maps-based transform on the biometric features to address the cancelability issue. We used Logistic map and Torus Automorphism to generate cancelable biometric features of the face and fingerprint minutia points, respectively. Both transformed features would be concatenated and saved in the database of the system instead of the original features. In the authentication stage, the similarity scores of both transformed face and fingerprint templates are computed and fused using the weighted sum rule. The results of the experimentation, conducted using images from the ORL face and FVC2002 DB1 fingerprint databases, demonstrated the higher performance of the proposed approach achieving a genuine accept rate equal to 100%. Moreover, the obtained results confirmed the soundness of the proposed cancelable technique to satisfy the biometric systems' requirements (i.e., security, revocability, and diversity).

Keywords: multimodal biometrics; template protection; cancelable biometrics; Torus Automorphism; chaotic maps

Citation: Ghouzali, S.; Nafea, O.; Wadood, A.; Hussain. M. Cancelable Multimodal Biometrics Based on Chaotic Maps. *Appl. Sci.* **2021**, *11*, 8573. https://doi.org/10.3390/app11188573

Academic Editor: Sung Bum Pan

Received: 6 July 2021
Accepted: 10 September 2021
Published: 15 September 2021

1. Introduction

The last century witnessed tremendous development in biometric authentication systems owing to their characteristics which outperformed traditional authentication systems. A typical biometric authentication system uses a single biometric modality. However, multimodal biometric authentication overcomes the drawbacks of unimodal biometric authentication, such as accuracy, non-universality, reliability, and security (vulnerability to spoofing attacks). Information fusion of different biometric modalities comprises a means to enhance the reliability of the biometric system without restoring the system to any other mechanism or technique. Despite providing a more efficient authentication procedure than traditional systems, biometric authentication systems are also subject to several security attacks such as by-passing, repudiation, covert acquisition, collusion, coercion, and denial of service. Security specialists need to determine the appropriate mechanisms to counter these kinds of attacks. More specifically, storing biometric templates in the system database has raised concerns over their security.

To protect biometric systems from these potential hazards, it is necessary to implement efficient solutions which restrict illegal access to any information in the biometric systems. Many hardware and software solutions have been put forward to prevent the harmful actions surrounding access to biometric data in a system. A set of techniques enabling various mechanisms have been employed to deal with the technological shortcomings arising from privacy and security issues associated with biometric templates. However,

these approaches do not have an in-depth foundation that can assist in comprehending suitability and weaknesses. Henceforth, to design an ideal approach of biometric templates protection, specific requirements must be satisfied—namely security, diversity, revocability, and performance [1,2].

Existing biometric templates protection methods have been categorized by Jain et al. [2] into (1) feature transformation and (2) biometric cryptosystem. The latter can be categorized as either key-generation systems or key-binding systems. In order to facilitate the validation phase of adopting or merging cryptographic keys related to a biometric information inquiry, some publicly available data, known as helper data, concerning the biometric template should be preserved in a biometric cryptosystem.

Feature transformation techniques are classified as invertible or non-invertible. Several feature transformation techniques have been proposed such as biometric salting (a user-specific invertible transformation based on a password or key); robust hashing (a non-invertible transformation based on one-way functions); and cancelable biometrics.

The major disadvantage of using raw biometric data—if these were compromised—is that they cannot be altered or canceled. However, cancelable template schemes allow non-invertible transforms to be employed without altering the biometric template space. Thus, using transformed or altered biometric data means that a stolen datum can be canceled and new distorted features can be created. This practice is referred to as cancelable biometrics, which is by far the main challenge when designing biometric template protection schemes [3]. Using cancelable biometrics, different templates can be created as a result of changing the parameters of the transformation functions, such that no matching should exist between the original and the transformed information. In [4,5], the researchers have again clarified and analyzed this principle, which was later designed in a more general sense to designate all the biometric protection approaches that are based on a non-invertible transformation [2].

Chaotic maps were recently employed to develop biometric template protection schemes. Chaotic maps refer to the mathematical functions that reveal a chaotic behavior and create, based on initial conditions, a different sequence of numbers. These functions are highly sensitive to initial conditions, making their use very efficient in information security systems and specifically in the scrambling process. The present paper proposes using chaotic maps to develop a new hybrid cancelable multimodal biometric template protection approach that guarantees the requirements in terms of performance, security, diversity, and revocability. The main contribution of this research is combining feature transformation methods with cryptosystems by using chaotic maps, such as the Logistic map and Torus Automorphism. A chaotic map is utilized to create random chains, from which a key parameter can be introduced. Using these seemingly random chains, encrypted data are generated based on the structure of the permutation–substitution process, which is highly effective in creating confusion and diffusion characteristics. Using this approach, it should be computationally difficult for an adversary to retrieve any raw data regarding the system's genuine users in the case of the protected template being compromised. In addition, the proposed biometric system is built using in conjunction of both the fingerprint and the face of the individual, and combining matching scores of these two biometric modalities can significantly improve the reliability and the efficiency of the biometric system as two biometric sensors need to be attacked to gain illegal access. Moreover, the matching of the templates is performed in the transformed domain, which ensures that the original data are not disclosed to third parties, aiming to satisfy the revocability requirement.

The remainder of the paper is arranged as follows. In Section 2, an overview of the related work is presented. Section 3 provides details of the proposed scheme. The experimental results are analyzed and discussed in Section 4. In the last section, the conclusion and future work are drawn.

2. Overview of Related Work

In the literature, cryptography and specifically chaos-based techniques have been employed for the generation of cancelable biometric templates. An overview of recent chaos-based approaches that have been proposed to protect biometric templates is presented in this section.

A non-invertible chaotic map-based transformation for the protection of face templates was addressed in [6]. In this approach, the Logistic map metric is utilized to produce linearly independent vectors for random projection in a way that the constructed projection matrix depends on the identity of the individual to whom belongs the biometric template. The experimental results have shown the efficacy of the suggested technique to meet the requirements of biometric systems. An extension study of this approach that provided rigorous performance and security experiments and analysis using different biometric modalities was presented in [7].

In [8], the authors presented the design of an approach for the protection of biometric templates using the chaotic behavior of a Logistic map. The transform approach uses the user's secret key to mix the plain face features with a chaotic random matrix. The biometric authentication system satisfied the privacy, diversity, and revocability requirements. Furthermore, a reasonable level of performance was reached.

In [9], the authors used biohashing in combination with chaos-based permutation to improve the privacy and security of biometric templates. The extracted face features using PCA or LDA are subjected to permutation before applying the biohashing. Their approach satisfied a good level of security and achieved comparable recognition accuracy to the traditional biohashing method.

In [10], a chaos-based image cryptosystem was proposed to protect fingerprint templates. The proposed scheme design is composed of four chaotic algorithms: two 1D and two 3D chaotic maps. The advantage of the scheme is increasing the keyspace to thwart brute force attacks. The security analysis showed that the scheme satisfied the randomness characteristic of a secure cryptosystem.

In [11], the authors introduced a chaos-based encryption algorithm that merges Murillo-Escobar's scheme and the Logistic map to ensure a higher security level of fingerprint templates. In addition, the statistical security analysis was entirely highlighted to prove the efficiency of the approach in real-world applications. However, the scheme fails to satisfy the revocability of the biometric data.

Liew et al. [12] developed an encryption-based method for biometric template protection using a combination of logistic mapping and dynamic Bernoulli mapping, hence allowing to improve the reliability of the cryptographic system in terms of volatility and correlation. The analysis of experimental results demonstrated that the scheme is simple to implement and yet resistant to attacks.

Nazari et al. [13] proposed to protect face templates using a cryptosystem combining schemes of binarization transform, chaos-based feature permutation, and fuzzy commitment. The chaos-based feature permutation aimed to counter the cross-matching attacks against the fuzzy commitment scheme by generating cancelable templates, attaining better security and unlinkability features. Experimental results showed that the system gained improved discriminability, privacy, and security.

S. Rajendran et al. [14] suggested a nonlinear chaos-based cryptosystem approach to protect biometric templates stored in system databases. In their approach, a 2D Logistic Sine Map was used by joining the 2D Logistic map and 1D sine map to generate large dimension chaotic keys based on the confusion and diffusion stages of the encryption. Experimental results and analysis proved the swiftness, security, and efficiency of implementing the scheme in real-time applications.

In [15], the authors presented a cancelable biometric approach that involved using chaotic maps to generate convolution kernels that are employed to extract encrypted Gabor features from iris images. The authors also proposed an alternative of the Logistic map to

increase the domain of the keyspace, aiming to enhance privacy. Moreover, the encryption key is based on the input image.

In [16], the authors proposed an approach to incorporate fingerprint features into diverse directional DWT sub-bands of the face template. Additionally, a keystream is generated using a hyper-chaotic map to encipher the obtained watermarked image. For an extra layer of security, each user is associated with a sole key. The approach demonstrated the ability to satisfy the requirements of security and diversity.

A hybrid chaotic map-based image encryption approach was suggested in [17] to supply security to palmprint images. The presented approach was conceptualized to suit the confusion and diffusion challenges and offers a large keyspace. Security analysis showed the robustness of the scheme against both cryptanalytic and replay attacks.

However, the techniques mentioned above satisfy the biometric template protection requirements only to a certain extent. In addition, some of these approaches suffer from the time and memory required to produce cancelable features. Moreover, there is a critical issue in some of the proposed chaotic encryption approaches; in the matching process, the protected template stored in the system database was decoded, which prevents its revocability if it is compromised. Therefore, there is a need to design non-invertible chaos-based biometric template protection approaches which accomplish the matching process in the transform domain intending to satisfy the revocability requirement.

3. Proposed Approach

This paper aimed to propose a robust algorithm for the protection of multimodal biometric templates while satisfying the criteria in terms of performance, security, revocability, and diversity. The chaotic behaviors of the chaotic map and Torus Automorphism are used to cancel the biometric features of the face and fingerprint, respectively. The proposed multimodal biometric system is built using both the fingerprint and the face images of the individual, which is seen to be a comparatively efficient solution as two biometric sensors need to be attacked with the use of manufactured biometric models. The proposed approach was proven to be efficient through extensive experimentation.

3.1. Cancelable Fingerprint Features

Fingerprint recognition can be categorized as either minutia-based and pattern-based. Three basic schemes can be employed to protect the minutia points: (1) directly protecting the minutia points; (2) protecting unordered sets generated from the minutia points (e.g., the distance between a pair of minutia points); and finally (3) protecting a fixed-length feature vector generated from the minutia points. Pattern-based approaches employ a fixed-length feature vector to protect the pattern of the fingerprint [18].

In the proposed approach, we used the first category (i.e., minutia-based) to provide user authentication. However, designing a cancelable technique for an unordered set of features (i.e., minutia points) is still challenging. To overcome this issue, we suggest transforming the minutia points using Torus Automorphism, which is a type of spatial transformation that can be applied to plane region to increase chaos [19,20]. Torus Automorphism has been proven to be beneficial in the context of the encryption of images. To protect the extracted minutia points, we use the following steps:

- First, Torus Automorphism is utilized to generate a chaotic sequence using the following definition [19,20]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ N \quad (1)$$

  It uses a 2×2 matrix with fixed elements (a, b and N) to transform a point (x, y) to a new position (x', y') in a space domain or to transform a state S_t to S_{t+1}. In the context of Torus Automorphism, there is a value R that is referred to the recurrence time such that $X_0 = X_R$ [19,20]. Therefore, at time t_R, the value of a state returns to the initial value at time t_0.

The values of states in a dynamic system change over time t in accordance with the implementation of a specific rule. In a discrete domain, t refers to the number of iterations of a function f. This means that the state value at a time $t+1$ is defined in the following way [21]:

$$S_{t+1} = f(S_t) \tag{2}$$

where S_t and S_{t+1} are the states at time t and $t+1$, respectively;

- Second, the generated chaotic sequence is sorted in an ascending order and rotated using a predefined angle (e.g., $\theta = 90^\circ$) based on the following:

$$\begin{bmatrix} x'' \\ y'' \end{bmatrix} = \begin{bmatrix} x' \\ y' \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \tag{3}$$

- The final step is the shifting and scaling of the modified minutia points coordinates as the following:

$$\begin{bmatrix} x_{trsf} \\ y_{trsf} \end{bmatrix} = S_f \left(\begin{bmatrix} x_o \\ y_o \end{bmatrix} + \begin{bmatrix} x'' \\ y'' \end{bmatrix} \right) \tag{4}$$

where x_o and y_o are the original coordinate values and S_f is a predefined scaling factor. x_{trsf} and y_{trsf} are the transformed coordinate values.

The aim of using the Torus Automorphism technique was to randomly distribute the extracted fingerprint minutia points. In this way, the coordinate positions of each minutia point are transformed to a newly assigned position. The same parameter values were applied to all users in each session to preserve the inter-class and intra-class variations. In the instance that the template is disclosed, a new transformed template will be assigned in order to protect the minutia points.

3.2. Cancelable Face Features

To transform the face images, we employ a basic principle based on mathematically convolving a user-specific kernel, which is generated using a chaotic map with biometric data to establish preventative measures against a range of attacks [22]. User face images are scanned for the enrollment stage, and following this, the user-specific kernel is generated with a chaotic map. We proposed using a Logistic map to generate the user-specific kernel. The Logistic map is expressed as

$$x_{i+1} = \mu x_i (1 - x_i) \tag{5}$$

where x_0 is the initial value. $\mu \in (3.57, 4)$ is the control parameter, which is used to produce the chaotic sequence numbers, which are then used to construct the kernel. To ensure that the user-specific kernel is unique, every user will be assigned a different value x_0.

The face template is first resized to 8×8 and then convolved by the generated kernel. The convolved images are considered as being the protected templates. The convolution process is defined by

$$h = F * g \tag{6}$$

where F refers to the image, g to the kernel and the $*$ symbol refers to the convolution process, which is based on a point-wise multiplication process.

In the instance where a protected template is disclosed, a new user-specific kernel is assigned to the user through the modification of the initial value x_0. It is not possible for an attacker to construct the protected template without knowing the user-specific kernel employed in the enrollment stage. The initial value has a significant role to produce a unique kernel for each genuine user.

3.3. Combined Face-Fingerprint Cancelable Approach

During the enrollment stage, the transformed fingerprint minutia points and the transformed face features are converted into a bitstream and concatenated together in order to form one feature vector. The concatenated feature vectors are then directly saved into the system's database. The transformation parameters are stored in a system's database using a hash map. Figure 1 illustrates the overall process of the proposed scheme (the enrollment stage).

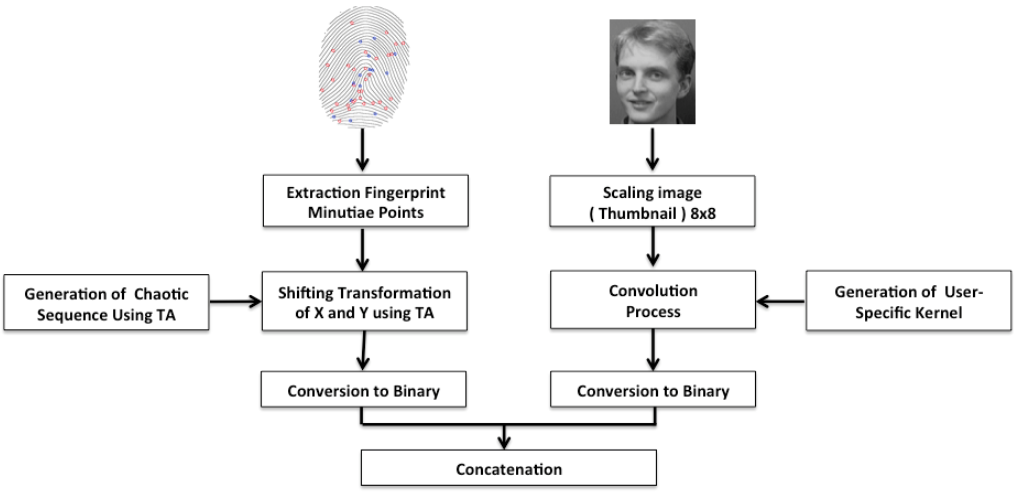

Figure 1. Proposed cancelable approach architecture (enrollment stage).

In the authentication stage, we consider the score level fusion of both biometric modalities: the fingerprint and face. The fusion of several biometric modality data represents the crux of multimodal biometrics. The fusion of biometric characteristic data can be achieved at three levels: (1) the decision level, wherein various decisions are combined; (2) the score level, wherein scores from different matching processes are combined; and (3) the feature level, wherein various biometrics features are combined. Whilst the most meaningful data are found in feature sets, incompatibilities can occur in the features from these modalities. Furthermore, data may be unimportant and/or superfluous due to the significant proportions of feature space. In addition, because data are minimal at the decision level, fusion here is somewhat inflexible. Contrarily, the score level fusion is less complex and yields better results. At this level, identifying and merging modality scores—produced using individual classifiers—is a relatively simple process [23].

Figure 2 depicts the authentication phase of the proposed approach involving the subsequent steps:

- Firstly, the system scans the query biometric features (face and fingerprint);
- Secondly, using the user key ID, the system retrieves the user parameters and the protected biometric features from the system's database;
- Thirdly, the system generates the user-specific kernel using the Logistic map and the user's initial value x_0 to transform the query face image;
- Fourthly, the Torus Automorphism parameters are recovered from the system's database to produce the transformed fingerprint features;
- Fifthly, user authentication is conducted using the score-level fusion of the similarity scores between the fingerprint and face features of the query and the database templates [24].

In this work, Euclidean distance and Cosine distance were employed to compute the similarity scores of the fingerprint and facial features, respectively. In general, a specific set of factors can ensure that the ability to recover the original biometric features is sufficiently difficult to be broken by an attacker. In the proposed approach, we use a set of parameters that controls the transformation process.

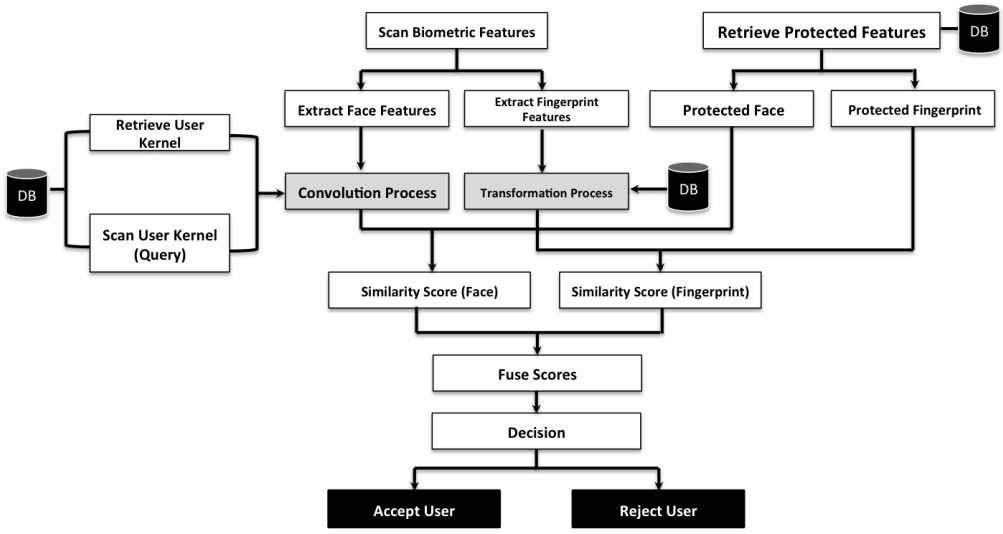

Figure 2. Proposed cancelable approach architecture (authentication stage).

4. Experimentation Results

4.1. Experiment Setting

Four hundred samples of facial templates were obtained from the Research Laboratory for the Olivetti and Oracle (*ORL*) database (https://cam-orl.co.uk/facedatabase.html, accessed on 3 January 2021), ten images each of forty subjects. Eight hundred fingerprint samples were obtained from the *FVC2002 DB1* database, eight images each from one hundred subjects [25]. The dimension of the fingerprint images utilized in the current experimentation was 374×388. The dimension of thumbnail face samples was 8×8 to balance between data discriminability and capacity. The proposed biometric protection system assigned eight pair samples of fingerprints and faces for each of the forty users.

4.2. Performance Analysis

In this experimentation, the *FVC2002* standard procedure was used to generate the legitimate (genuine) and illegitimate (impostor) scores. The impostor score was created by matching the first image of each subject with the corresponding first image of every other subject, whereas the genuine score is generated by matching each image with all the other images from the same subject. Hence, a verification system can be considered as a binary classification problem as follows. For a user (U) with a claimed identity I and a query feature set F_Q, we need to determine whether the user belongs to the genuine or impostor class. Considering the fact that F_I is the stored template assigned to the identity I, a matching score S, which compares F_Q and F_I, is computed. The verification system then provides a decision by comparing the matching score S to a pre-defined threshold ϵ. A large score indicates a good match, which means that the user is genuine. The decision rule is expressed as

$$U_{(I,F_Q)} \in \begin{cases} genuine, & if \quad S \geq \epsilon \\ impostor, & if \quad S < \epsilon \end{cases} \tag{7}$$

The recognition rate of the multimodal approach was computed using the score-level fusion of the fingerprint and face biometrics based on the weighted sum rule [26]. Moreover, 0.3 and 0.7 were acquired as weights to fingerprint and face scores, respectively. However, normalization is necessary before the fusion process because the scores generated by the diverse systems and algorithms in each constituent process are inherently dissimilar. Since matching in multimodal techniques is influenced by the normalization procedure, efficacy and resilience are the two key criteria to be considered for choosing the most appropriate method. Hence, the performance-anchored normalization (PAN) technique,

which is improved min–max normalization, was utilized in this study to fuse the scores obtained from each matching module [24].

Figure 3 illustrates the genuine and impostor matching score distribution (the term "distribution" refers to a histogram). Better discriminability between genuine and impostor users was achieved in this experiment since the corresponding distributions are well separated at a threshold equal to 0.4593—as shown in the figure.

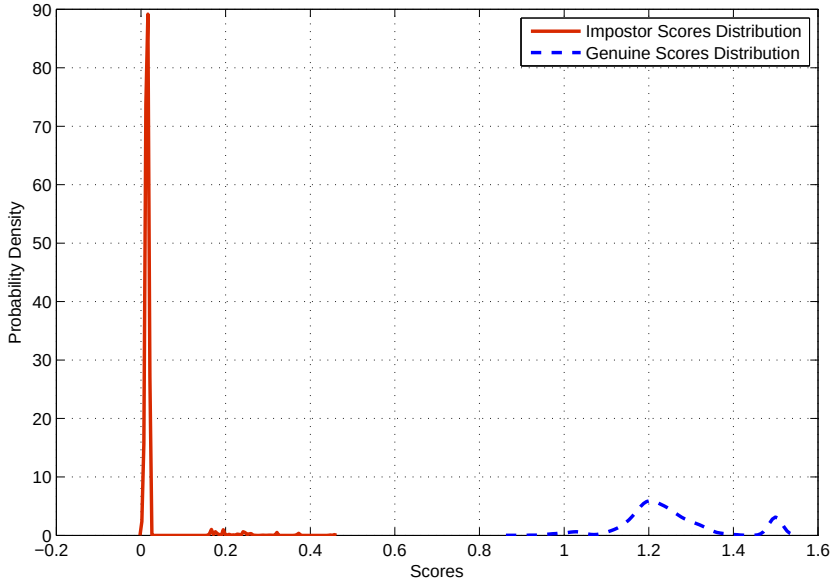

Figure 3. The matching distribution of genuine and impostor scores.

To confirm the efficacy of the proposed approach, the false acceptance rate (FAR) and the false rejection rate (FRR) were computed. FRR denotes the proportion of genuine scores that are smaller than the pre-defined threshold ϵ ($FRR = p(S < \epsilon|genuine)$), and FAR denotes the fraction of impostor scores that are larger than or equal to ϵ ($FAR = p(S \geq \epsilon|impostor)$). Figure 4 shows that the equal error rate (EER)—which is the point at which the FAR and FRR are equal—of the proposed scheme is 0% when the threshold is 0.4593.

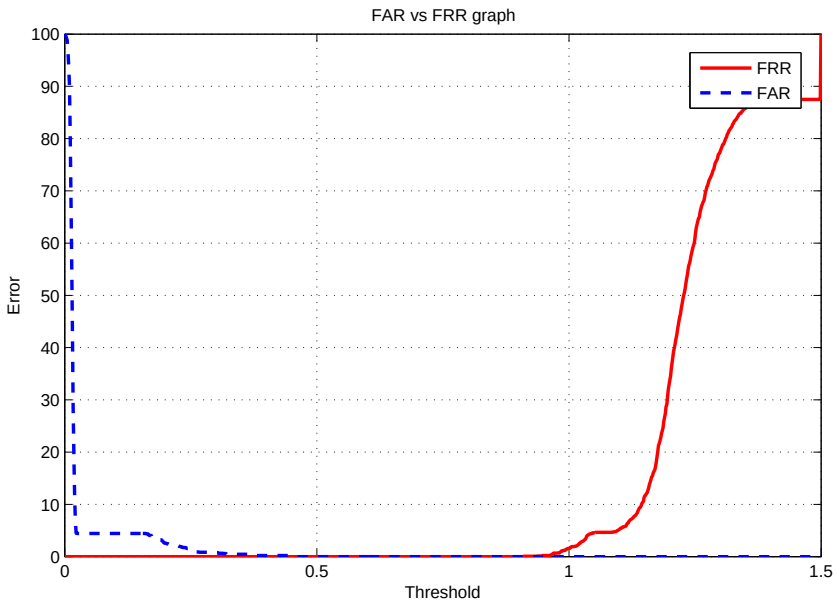

Figure 4. The EER of the proposed multimodal cancelable approach.

To validate the effectiveness of the multimodal fingerprint–face system in comparison with the unimodal face and fingerprint systems, the receiver operating curve (ROC) is shown in Figure 5. The ROC is used to relate the genuine acceptance rate (GAR) against the FAR at different threshold values. The GAR can be defined as the fraction of genuine scores that are larger than ϵ ($GAR = 1 - FRR$). As depicted in Figure 5, the GAR of the unimodal system based on the fingerprint is equal to 95.58% at an FAR of 0.05%. The corresponding GAR value of the unimodal system based on face and the proposed multimodal approach is 100%. Hence, it was concluded that the proposed approach can maintain the highest performance while encountering the major shortcoming of unimodal biometric authentication approaches.

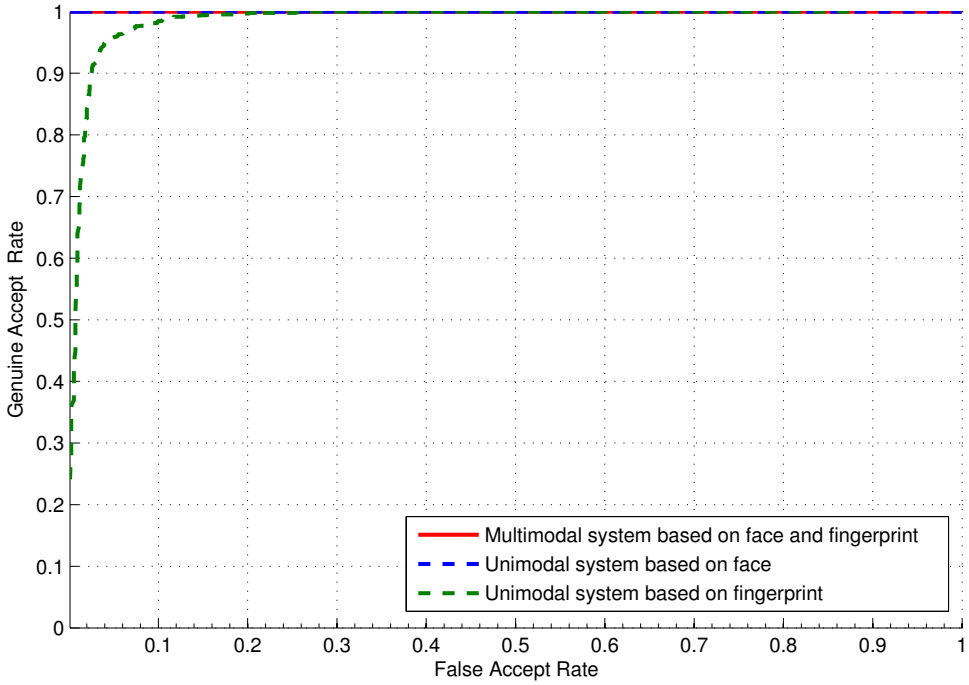

Figure 5. The ROC curve of the proposed cancelable approach.

4.3. Security Analysis

The constant parameters used in the Torus Automorphism transformation matrix and the user-specific kernel play a critical role in obtaining an appropriate level of security. Three primary concerns should be taken into consideration when developing a Torus Automorphism transformation matrix to protect the fingerprint minutia points: (1) the sensitivity to the transformation parameter values; (2) the effect on the performance recognition rate; and (3) the ability to produce multiple templates.

The keyspace provided by the proposed Torus Automorphism transformation is restricted to a value of $(R-1)N^2$. In case the parameter values utilized are $a = 9$, $b = 9$, and $N = 128$, the recurrence time R can be determined by simulation, and it is almost equal to $N - 1$ [21]. Thus, the keyspace is equal to 127×128^2, which means that it is sufficiently difficult for an adversary to formulate an estimation.

The user-specific kernel can be changed and generated using a different key (i.e., different chaotic map). Since each user has a unique kernel, it is necessary to study the effect of assigning the same kernel to all users. Figure 6 shows that in the case of using the same kernel for all users, the proposed approach achieves the same GAR as the baseline system (without protection). Hence, we conclude that the simple proposed convolution process does not deteriorate the performance accuracy under the baseline system when the kernel is stolen.

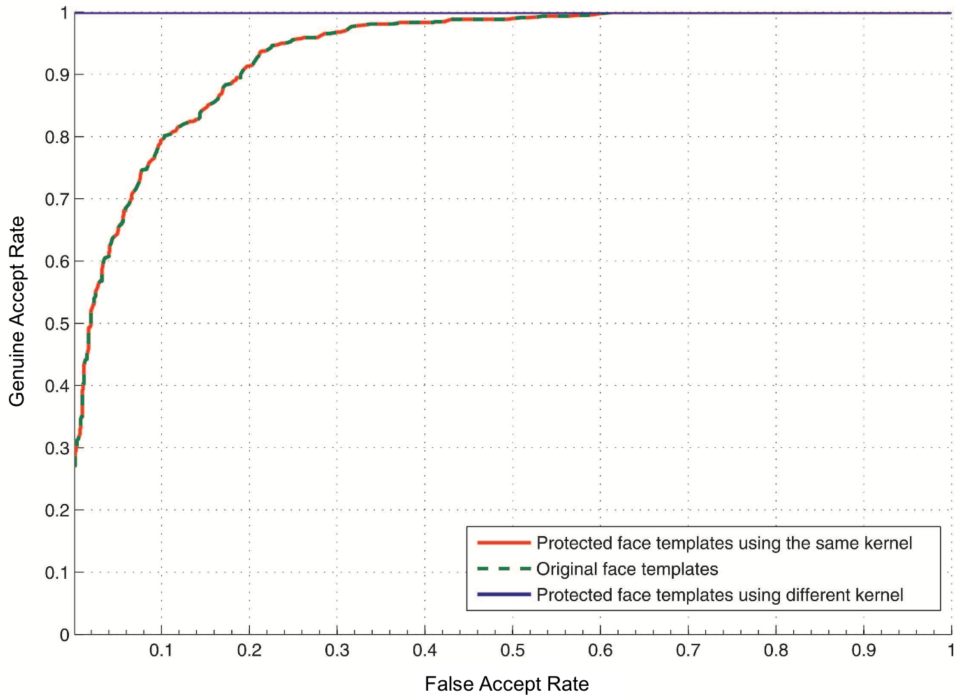

Figure 6. The ROC curve of the unimodal face system in the case of stolen-kernel.

4.4. Diversity and Revocability Analysis

To satisfy the requirements of revocability and diversity, the protected template should not match the original template, and it should be sufficiently difficult to recover the raw biometric data when the stored template is disclosed. Additionally, matching should not exist between multiple protected templates using the same features in order to avoid cross-matching between different databases. The diversity criterion is evaluated by generating various templates from a single biometric datum using diverse keys and measuring the feasibility to recover the original biometric features when using different keys to decrypt the protected templates. To implement this scenario, a new database of protected templates was generated. The proposed system efficiently denied user attempts to gain access when the key is different, categorizing the attempt as an illegal intrusion.

We also evaluated the ability to produce revocable templates for each subsystem. In the fingerprint system, we created new protected sets. The key is represented by the values of the transformation matrix (a, b, and N), the rotation angle, and the scaling factor. The proposed cancelable technique is shown to satisfy this requirement, as illustrated in the following Figures 7–10.

Figure 7 clarifies that the matching score between the original fingerprint features and the protected fingerprint features is equal to 0.1668. Figures 8 and 9 depict that the matching between templates in the same database is effective, and the transformation process does not deteriorate the recognition rate. Furthermore, it preserves the inter-class and intra-class variations. Figure 10 depicts the matching between two protected templates using different transformation parameters, which is equal to 0.1282. These results are an indication that the effectiveness of the proposed method allows the disassembling of the relation between the original and the protected templates and, additionally, between two protected templates created using different keys.

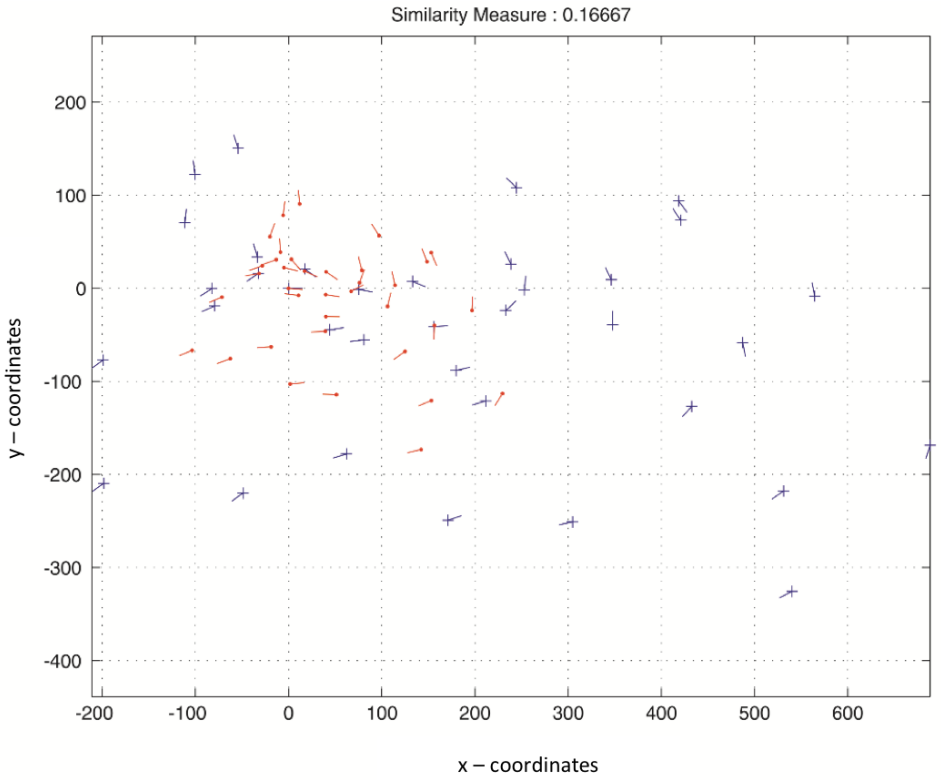

Figure 7. Matching score between original and transformed fingerprint templates.

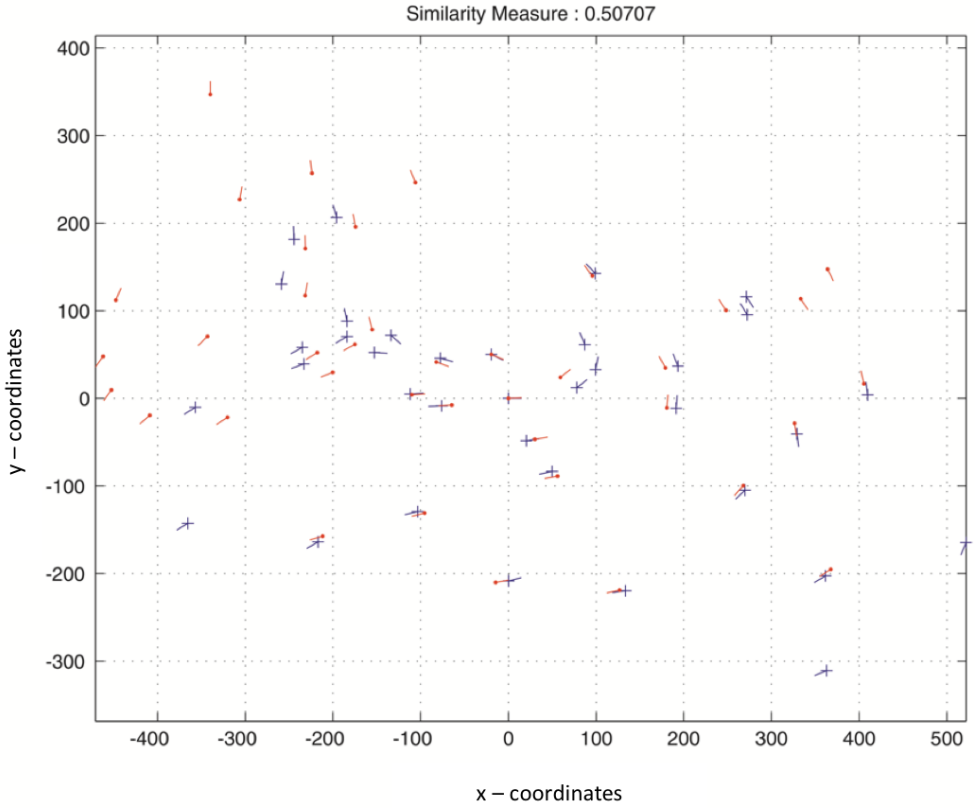

Figure 8. Matching score between two transformed fingerprint templates of the same user in the same database.

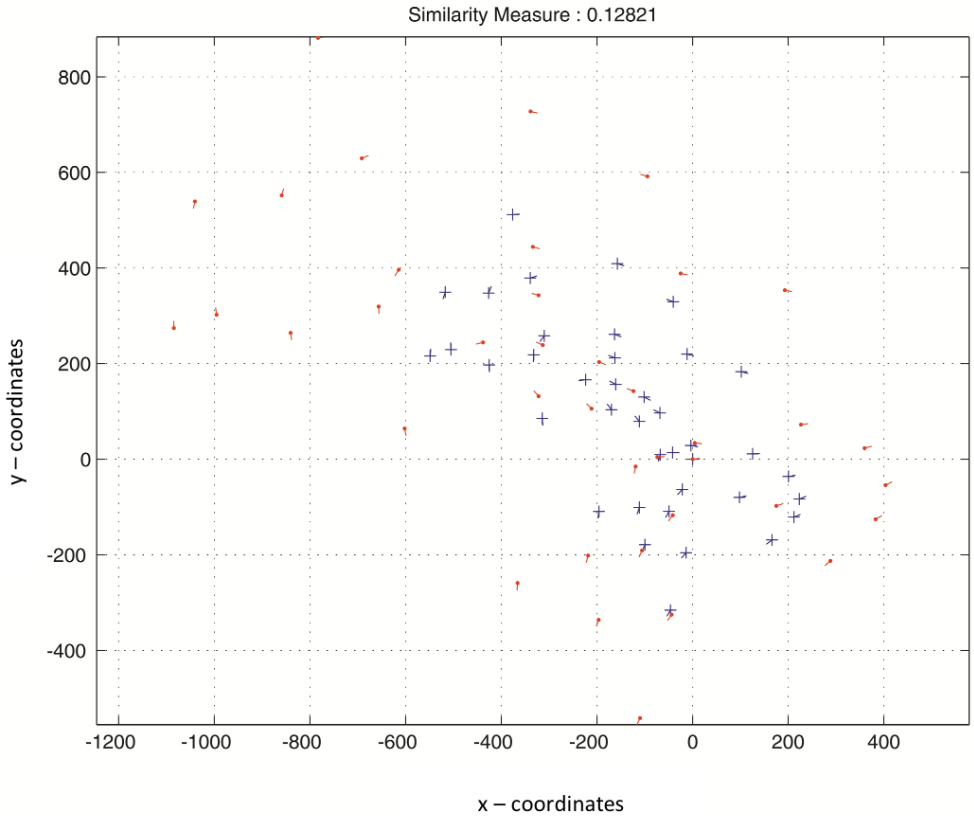

Figure 9. Matching score between two transformed fingerprint templates of the same user in two different databases.

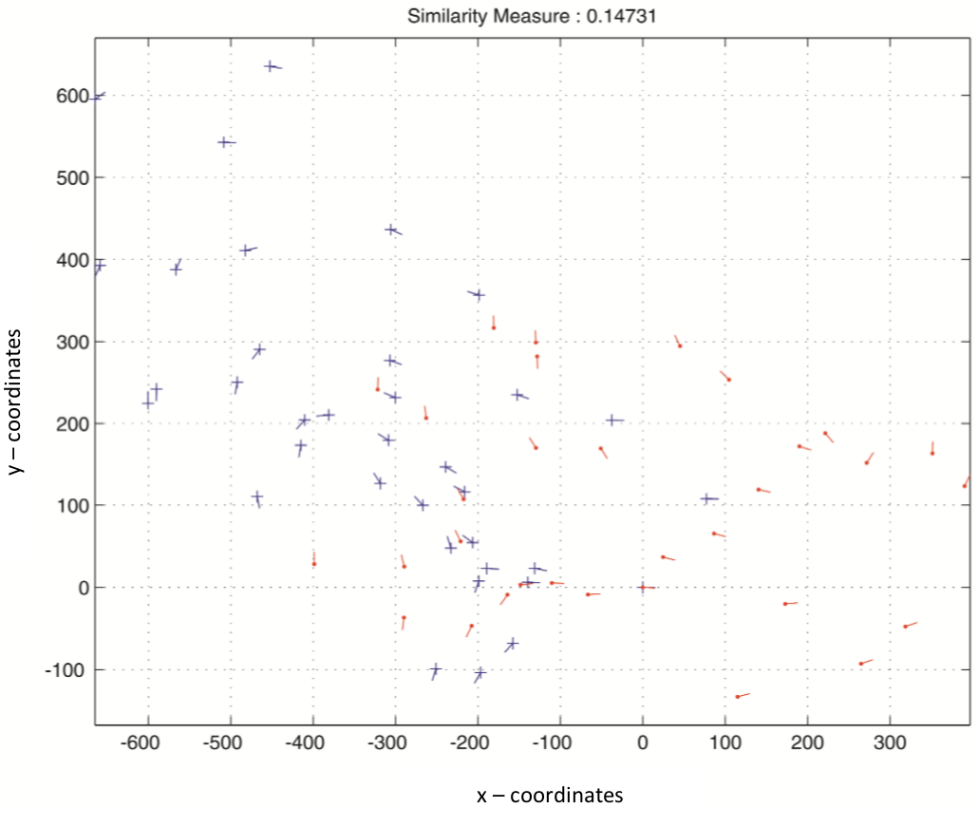

Figure 10. Matching score between two transformed fingerprint templates of two different users in the same database.

Now, to validate the revocability criterion in the proposed multimodal system, we demonstrate the pseudo-impostor distribution (illustrated in Figure 11) by creating new biometric templates of the same original biometric datum using different keys [27]. Then, the new protected templates are matched with the stored (i.e., enrolled) templates in the database. Obtaining identical EER compared to genuine/impostor authentication is an indicator of attaining good diversity and revocability. The EER is 1.77% for the pseudo-impostor distribution, which reveals a good diversity.

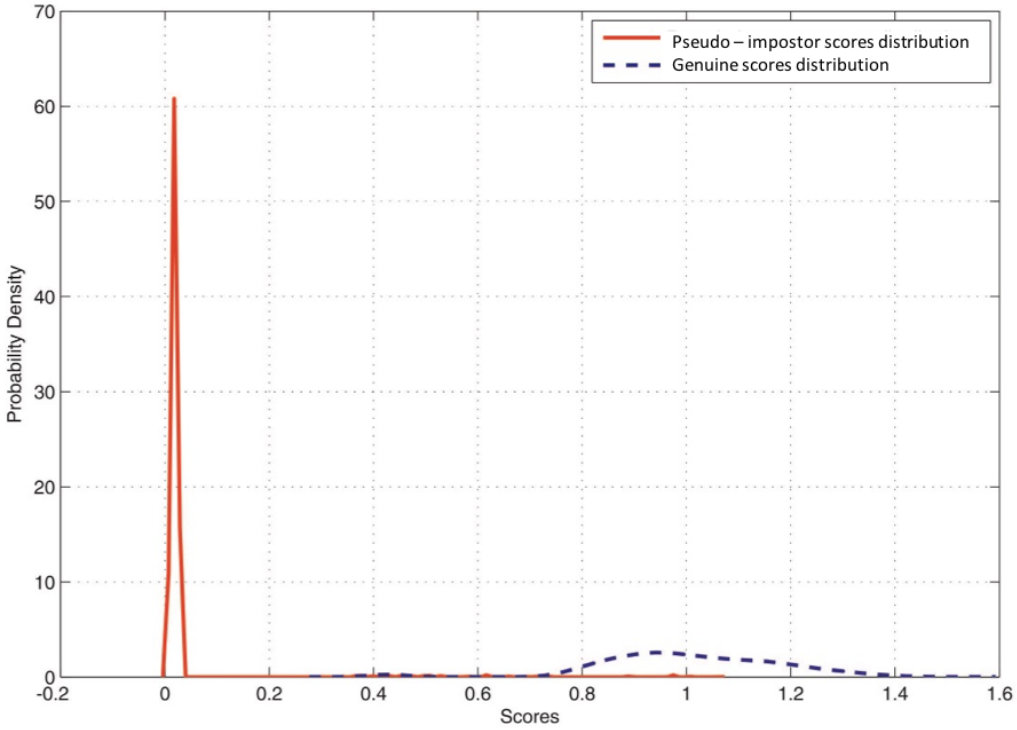

Figure 11. The matching distribution of genuine and pseudo-impostor scores.

4.5. Comparison with Previous Studies

Table 1 lists some of the related biometric template protection techniques reviewed in this paper, biometric modalities, databases, performance results, and requirements fulfillment. In our approach, we propose combining feature transformation methods with chaotic behavior to generate cancelable biometric templates. The proposed approach demonstrates an ability to satisfy the critical criteria of biometric template protection. It has been shown to achieve a minimum error rate of 0%. Moreover, the matching process is performed in the transformed domain, which ensures the cancelability of the biometric data. The main disadvantage of the proposed approach is the need to apply a preprocessing stage, including the extraction of the minutia points and the re-sizing of the face template. In addition, the performance of the proposed approach can be affected by the presence of noise and the image resolution. However, there is a need to do more experiments on other real multimodal biometric databases of fingerprint and face images to prove the effectiveness of the proposed approach.

Table 1. Comparison of the proposed approach with related works.

Schema	Biometric Modalitiy	Database	Technique	Performance	Requirements (S: Security; D: Diversity; R: Revocability)
[9]	Face	ORL	Biohashing and chaos-based cancelable biometrics	$GAR_{PCA} = 58.5\%$ $GAR_{LDA} = 67.4\%$	S
[11]	Fingerprint	—	Fingerprint template protection based on chaotic encryption	$FAR = 10^{-6}\%$ $FRR = 10^{-2}\%$	S
[13]	Face	Extended Yale B, CMU PIE, FEI	Binarization, chaos-based feature permutation, and fuzzy commitment	$GAR = 96.52\%$ $GAR = 90.7\%$ $GAR = 93.7\%$	S, R, D
[15]	Iris	CASIA-IrisV3	chaotic encryption-based cancelable IrisCodes	$EER = 1.17\%$	S, R
[16]	Fingerprint, face	FVC 2002 DB1, ORL	Multimodal approach based on watermarking and hyper-chaotic map	$EER = 3.87\%$	S, D
Proposed	Fingerprint, face	FVC2002 DB1, ORL	Chaos-based cancelable biometrics	$EER = 0\%$	S, D, R

5. Conclusions and Future Research

This paper presented a novel cancelable protection approach that ensures the security, revocability, diversity, and performance of a multimodal biometric system based on face and fingerprint templates. In this approach, we used a Logistic map and Torus Automorphism to protect the biometric features. To protect the face features, we used a Logistic map to generate a user-specific kernel. The generated kernel was convolved with the face features via a convolution process. In the proposed procedure, the original face template does not match with the protected templates. To protect the fingerprint features, we used transformation methods which include Torus Automorphism-based shifting, rotation, and scaling. The strong chaotic behavior of the Torus Automorphism resulted in the disassembling of the relationship between the original and the transformed templates. Experiments were conducted using the ORL and FVC2002 DB1 databases. However, extensive experiments are required to validate the effectiveness of the proposed approach.

With respect to the next step in this research, future work will assess the application of the proposed approach for large-scale biometric databases and for different biometric modalities. In addition, a technique to detect the image noise will be implemented to maintain a high performance rate.

Author Contributions: Conceptualization, S.G., A.W., O.N.; methodology, O.N., S.G.; validation, O.N., A.W.; writing—original draft preparation, O.N.,S.G.; writing—review and editing, S.G., O.N.,A.W.,M.H.; supervision, S.G., A.W., M.H.; funding acquisition, A.W. All authors have read and agreed to the published version of the manuscript.

Funding: This Project was funded by the National Plan for Science, Technology and Innovation (MAARIFAH), King Abdulaziz City for Science and Technology, Kingdom of Saudi Arabia, Award Number (13-INF2114-02).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: ORL and FVC2002 DB1 databases are publicly available.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Breebaart, J.; Yang, B.; Buhan-Dulman, I.; Busch, C. Biometric template protection: The need for open standards. *Priv. Data Secur. J.* **2009**, *33*, 299–304. [CrossRef]
2. Jain, A.K.; Nandakumar, K.; Nagar, A. Biometric template security. *EURASIP J. Adv. Signal Process.* **2008**, *2008*, 1–17. [CrossRef]
3. Patel, V.M.; Ratha, N.K.; Chellappa, R. Cancelable Biometrics: A review. *IEEE Signal Process. Mag.* **2015**, *32*, 54–65. [CrossRef]
4. Ratha, N.K.; Connell, J.H.; Bolle, R.M.; Chikkerur, S. Cancelable Biometrics: A Case Study in Fingerprints. In Proceedings of the 18th International Conference on Pattern Recognition, Hong Kong, China, 20–24 August 2006; pp. 370–373.
5. Ratha, N.K.; Chikkerur, S.; Connell, J.H.; Bolle, R.M. Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.* **2007**, *29*, 561–572. [CrossRef] [PubMed]
6. Moujahdi, C.; Ghouzali, S.; Mikram, M.; Rziza, M.; Bebis, G. Spiral cube for biometric template protection. In Proceedings of the International Conference on Image and Signal Processing, Agadir, Morocco, 28–30 June 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 235–244.
7. Moujahdi, C.; Bebis, G.; Ghouzali, S.; Mikram, M.; Rziza, M. Biometric Template Protection Using Spiral Cube: Performance and Security Analysis. *Int. J. Artif. Intell. Tools* **2016**, *25*, 1550027. [CrossRef]
8. Ghouzali, S.; Abdul, W. Private chaotic biometric template protection algorithm. In Proceedings of the first International Conference on Information and Image Processing (ICIIP), Melbourne, Victoria, 9–11 December 2013.
9. Nazari, S.; Moin, M.S.; Kanan, H.R. Cancelable face using Chaos permutation. In Proceedings of the Seventh International Symposium on Telecommunications (IST), Tehran, Iran, 9–11 September 2014; pp. 925–928.
10. Hsiao, H.-I.; Lee, J. Fingerprint image cryptography based on multiple chaotic systems. *Signal Process.* **2015**, *113*, 169–181. [CrossRef]
11. Murillo-Escobar, M.A.; Cruz-Hernández, C.; Abundiz-Pérez, F.; López-Gutiérrez, R.M. A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Syst. Appl.* **2015**, *42*, 8198–8211. [CrossRef]
12. Liew, C.Z.; Shaw, R.; Li, L. Protect biometric data with compound chaotic encryption. *Secur. Commun. Netw.* **2014**, *9*, 1928–1943. [CrossRef]
13. Nazari, S.; Moin, M.-S.; Kanan, H.R. Securing templates in a face recognition system using Error-Correcting Output Code and chaos theory. *Comput. Electr. Eng.* **2018**, *72*, 644–659. [CrossRef]
14. Rajendran, S.; Doraipandian, M. Biometric Template Security Triggered by Two Dimensional Logistic Sine Map. *Procedia Comput. Sci.* **2018**, *143*, 794–803. [CrossRef]
15. Soliman, R.F.; Ramadan, N.; Amin, M.; Ahmed, H.H.; El-Khamy, S.; El-Samie, F.E.A. Efficient Cancelable Iris Recognition Scheme Based on Modified Logistic Map. *Proc. Natl. Acad. Sci. India Sect. A Phys. Sci.* **2020**, *90*, 101–107. [CrossRef]
16. Abdul, W.; Nafea, O.; Ghouzali, S. Combining Watermarking and Hyper-Chaotic Map to Enhance the Security of Stored Biometric Templates. *Comput. J.* **2019**, *63*, 479–493. [CrossRef]
17. Hikal, N.A.; Eid, M.M. A new approach for palmprint image encryption based on hybrid chaotic maps. *J. King Saud Univ.-Comput. Inf. Sci.* **2020**, *32*, 870–882. [CrossRef]
18. Jain, A.K.; Nandakumar, K.; Nagar, A. Fingerprint template protection: From theory to practice. In *Security and Privacy in Biometrics*; Campisi, P., Ed.; Springer: London, UK, 2013.
19. Chang, C.C.; Hsiao, J.Y.; Chiang, C.L. An image copyright protection scheme based on torus automorphism. In Proceedings of the First International Symposium on Cyber Worlds, Tokyo, Japan, 6–8 November 2002; pp. 217–224.
20. Kakkirala, K.R.; Chalamala, S.R.; Dhillon, J. A robust image watermarking using DWT, SVD and Torus Automorphism. In Proceedings of the IEEE International Conference in Computational Intelligence and Cybernetics, Yogyakarta, Japan, 3–4 December 2013; pp. 160–163.
21. Kocarev, L.; Sterjev, M.; Amato, P. RSA encryption algorithm based on torus automorphisms. In Proceedings of the International Symposium on Circuits and Systems, Vancouver, BC, Canada, 23–26 May 2004; Volume 4, pp. 577–580.
22. Maiorana, E.; Campisi, P.; Neri, A. Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system. In Proceedings of the IEEE International Systems Conference (SysCon), Montreal, QC, Canada, 4–7 April 2011; pp. 495–500.
23. Peng, J.; El-Latif, A.A.A.; Li, Q.; Niu, X. Multimodal biometric authentication based on score level fusion of finger biometrics. *Optik-Int. J. Light Electron Opt.* **2014**, *25*, 6891–6897. [CrossRef]
24. Damer, N.; Opel, A.; Nouak, A. Performance anchored score normalization for multi-biometric fusion. In *Advances in Visual Computing*; Bebis, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2013.
25. Ross, A.; Nandakumar, K.; Jain, J. *Handbook of multibiometrics (International Series on Biometrics)*; Springer Inc.: New York, NY, USA, 2006.
26. Kittler, J.; Hatef, M.; Duin, R.P.W.; Matas, J. On combining classifiers. *IEEE Trans. Pattern Anal. Mach. Intell.* **1998**, *20*, 226–239. [CrossRef]
27. Chin, Y.J.; Ong, T.S.; Teoh, A.B.J.; Goh, K.O.M. Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. *Inf. Fusion* **2014**, *18*, 161–174. [CrossRef]