axioms

MDPI

Article

Efficient Cancelable Template Generation Based on Signcryption and Bio Hash Function

Vani Rajasekar [1], Muzafer Saračević [2], Darjan Karabašević [3,*], Dragiša Stanujkić [4], Eldin Dobardžić [5] and Sathya Krishnamoorthi [1]

[1] Kongu Engineering College, Thoppupalayam, Kumaran Nagar, Perundurai 638060, Tamil Nadu, India
[2] Department of Computer Sciences, University of Novi Pazar, DimitrijaTucovića bb, 36300 Novi Pazar, Serbia
[3] Faculty of Applied Management, Economics and Finance, University Business Academy in Novi Sad, Jevrejska 24, 11000 Belgrade, Serbia
[4] Technical Faculty in Bor, University of Belgrade, VojskeJugoslavije 12, 19210 Bor, Serbia
[5] Faculty of Economics and Engineering Management, University Business Academy in Novi Sad, Cvecarska 2, 21000 Novi Sad, Serbia
* Correspondence: darjan.karabasevic@mef.edu.rs

Abstract: Cancelable biometrics is a demanding area of research in which a cancelable template conforming to a biometric is produced without degrading the efficiency. There are numerous approaches described in the literature that can be used to generate these cancelable templates. These approaches do not, however, perform well in either the qualitative or quantitative perspective. To address this challenge, a unique cancelable template generation mechanism based on signcryption and bio hash function is proposed in this paper. Signcryption is a lightweight cryptographic approach that uses hyper elliptic curve cryptography for encryption and a bio hash function for generating signatures in this proposed method. The cancelable templates are generated from iris biometrics. The hybrid grey level distancing method is used for perfect iris feature extraction for the CASIA and IITD datasets. The proposed approach is compared against the existing state-of-the-art cancelable techniques. The resulting analysis reveals that the proposed method is efficient in terms of accuracy of 98.86%, with lower EER of 0.1%. The average minimum TPR and TNR of the proposed method is about 99.81%.

Keywords: cancelable templates; biometrics; signcryption; bio hash function; security

MSC: 68T01

Citation: Rajasekar, V.; Saračević, M.; Karabašević, D.; Stanujkić, D.; Dobardžić, E.; Krishnamoorthi, S. Efficient Cancelable Template Generation Based on Signcryption and Bio Hash Function. *Axioms* **2022**, *11*, 684. https://doi.org/10.3390/axioms11120684

Academic Editor: Faith-Michael E. Uzoka

Received: 26 October 2022
Accepted: 28 November 2022
Published: 29 November 2022

1. Introduction

Biometric recognition is developing quickly due to the introduction of low-cost, high-accuracy computing technologies and the growing need for security. Biometrics are based on a person's physiological and behavioral characteristics. The majority of real-time applications, including military applications, surveillance, cognitive intelligence, forensics, banking apps, e-governance, and financing applications can use these qualities to uniquely recognize the individual [1]. Iris recognition has been shown to offer the highest level of statistical security and accuracy among the various biometric techniques, including hand geometry, facial detection, fingerprint recognition, palm print recognition, and iris recognition. The first step in the iris identification method is iris pre-processing. Biometric technologies are vulnerable to privacy issues. The biometric templates that are stored in a database can be taken by an attacker. The ability to reuse the acquired iris templates in other apps has been demonstrated. Exposure of biometric information could pose serious risks to the user's confidentiality and protection. The risk connected to the breach of biometric data necessitates the storage of biometric data in a protected format. The recognition of biometric templates is a crucial and computationally demanding process, so the security component

should not impair biometric effectiveness. Better recognition performance and secure one-to-many correlations are required for identification. Simple biometric encrypting techniques encrypt biometric features at the transmitter and decrypt them at the receiver to enable decrypted biometric authentication or verification. Unfortunately, because decrypted biometrics could be taken, this technique opens the door to hacker scenarios. The idea of cancelable biometrics, in contrast, relies on authentication or verification using fingerprints that have been altered or encrypted. Cross-matching is prevented by current trends in cancelable biometrics, since cancelable templates can be prepared for each application. To solve the issue of cross-matching among biometric collections, many methods for creating cancelable biometric information were developed. These techniques use fingerprint images to produce a variety of cancelable templates. In essence, a user can issue a unique transformation key as required to use biometric identification.

1.1. Problem Statement

Typically, during the enrollment phase, the biometric information of the enrolled users is maintained on the database server in its unsecured, plain form. The biometric data may be compromised even if the information is encrypted, since encryption requires decoding during the authentication process. Biometric databases have been the target of a significant number of hacking attempts in recent years. One of the effective approaches being developed to deal with this problem is cancelable biometrics. The non-invertible modification of the template is the most intriguing cancelable template technique. The masking of a biometric trait, picture, or signal is the primary goal of cancelable biometrics. To provide more security in application databases, this masking can also be widened to include the encryption of templates [2,3]. Although biometric-based authentication solutions have shown great promise in preventing security breaches and network intrusions, there are still certain difficulties. Since the wide range of biometric data is maintained as digital online entities, there is a substantial security and identity threat if the data are stolen by enemies.

Privacy can be easily violated if biometric templates are made available to attackers. One of the key issues is that once the original biometric data has been compromised, it cannot be changed or updated. Every biometric template in the cancelable biometric method is saved in the database in a distorted version rather than the original template. This method can thwart an attack on a stored biometric templates. Renewability is a desirable characteristic that refers to the creation of unique cancelable templates for various applications to prevent repeatedly utilizing the same cancelable templates. To give a better level of secrecy, non-invertibility entails creating a secure, cancelable biometric template that must be non-invertible.

1.2. Related Studies

In cancelable biometrics, the raw biometric pattern rather than the biometric image is changed or deformed before being saved in the database [4]. As can be seen, the templates acquired following this change are completely worthless when compared to the original biometric. Instead of the original biometric characteristics, these altered or useless templates are kept in the database. The cancelable templates need to have four key qualities: (i) diversity, (ii) non-invertibility, (ii) revocability, and (iv) performance. Diversity is defined as the idea that each created cancelable biometric template should be unique, or that no two people should be assigned the same cancelable biometric template. A cancelable biometric system is one in which the user's biometric information is encrypted using format-preserving encrypted communications before it is matched to Bloom filter-based patterns. Encryption of the template maintains the format and durability of the biometric data. The original biometric data are encrypted without adding any extra bit mistakes. The matching Bloom filter-based template is subsequently assigned to the encrypted biometric information. Non-invertible signifies that these cancelable biometric templates cannot be used to create original biometric characteristics. According to the

concept of revocable property, if a person's cancelable biometric template is lost, stolen, or otherwise compromised, a new cancelable template should be given to them without jeopardizing their original biometric identity [5]. Cancelable biometric systems should perform similarly to standard biometric systems in terms of effectiveness. Simply put, it indicates that the recognition rate should not change.

1.3. Contributions

A list of contributions of the proposed approach is shown below.

- A novel cancelable template generation method is proposed based on signcryption with hyperelliptic curve cryptography.
- The optimal features are extracted using the HGLD (hybrid grey level distance) feature extraction technique.
- The bio hash function is used to convert the cancelable features to bio hash vectors.
- Original biometric templates are converted into cancelable templates with signcryption and bio hash functions.
- The efficiency of the proposed method is compared with the state-of-the-art existing approaches.

2. Materials and Methods

In this section, an overview of cancelable template generation techniques that are aligned with the proposed methodology is presented. Cancelable biometric templates can successfully stop privacy violations and offer the original templates substantial protection. Simplified templates, on the other hand, would dramatically degrade authentication efficiency to accommodate resource-constrained IoT devices. Additionally, because available cancelable biometric templates are often fixed in length, it is challenging to implement them in a variety of memory-constrained IoT devices. They provide a unique, length-flexible, compact, cancelable biometric template to solve these problems for resource-constrained IoT applications that require privacy-preserving authentication systems. Significant investigation into deep learning-based biometric authentication methods in the post-COVID-19 era has revealed a necessity to safeguard them. Additionally, biometric data is essentially unchangeable; as a result, if it is compromised, it is lost for good. The security and privacy issues with deep network-generated biometric templates are addressed by Singh et al. [6]. They suggest using revocable biometric authentication. The system creates biometric templates using a lightweight convolutional neural network (CNN) with a few-shot enrollment. A unique cancelable biometric template-generating technique based on the Chinese remainder theorem and random randomization is proposed by Manisha et al. [7].

The original biometric and cover photos, as well as a hidden image, are used to create a cancelable biometric template in the proposed method. While maintaining the intensity values, random permutation offers visual protection against the original biometric. To ensure that the intensity levels are kept a secret from any intruder, the output of the random permutation step is transformed using the Chinese remainder theorem. A randomized walk-based approach for cancelable template creation is proposed by Pandey et al. [8]. The suggested method is unusual in that it uses fingerprint data to create a secure, unique cancelable template. Additionally, the suggested technique is resistant to a variety of security assaults. It also makes sure that the created cancelable templates are generated at random. Asthana et al. [9] introduce a unique method called the Random Area & Perimeter Method (RAPM), in which a biometric feature of a person is converted into random values that are saved as cancelable biometric templates. The suggested method interpolates feature points from the original biometrics with a user-selected random point to compute the area and circumference of the Bézier curve. The calculated area and perimeter have pseudo-random characteristics. A secure biometric system based on the idea of location sensitive hashing is introduced by Sadhya et al. [1]. In this study, we developed cancelable iris code features known as locality sampled code (LSC), which concurrently offer reliable system performance and excellent security assurances. The work of Siddhad et al. [10] processes characteristics that were retrieved using Log–Gabor filters following the suggested max–

min threshold. To construct a cancelable template, the resulting binary features are randomly projected onto a key matrix. Using publicly available databases of various physical and behavioral biometrics, the approach was thoroughly examined [11,12]. Performance compared to many current approaches showed a notable improvement. Several papers [13–16] present efficient cancelable multi-biometric recognition systems based on deep learning and bio hashing, an efficient lightweight cryptographic scheme of sign encryption based on a hyperelliptic curve, and ECG biometrics based on a combination of deep transfer learning with DNA and protected biometric identification with multiple finger vein.

The remainder of the paper is organized as follows: Section 3 describes the proposed methodology explaining signcryption, iris preprocessing, the bio hash function, and cancelable template generation. Section 4 describes the results and includes a discussion. Section 5 summarizes the conclusions and future possibilities concerning the proposed approach.

3. Proposed Methodology

3.1. Signcryption

In the cryptographic approach, signcryption is defined as a fundamental public key paradigm that involves the process of both a digital signature and encryption. The traditional authentication method is signature then encryption, which digitally signs a message and is then followed by encryption technology. Researchers have identified two major drawbacks that occur in the traditional approach: low efficiency and higher computational cost.

Signcryption is an emerging lightweight cryptographic paradigm that integrates encryption and digital signature in a single logical step. The signcryption can effectively decrease the computational cost and communication overhead [17–19]. This is a hybrid cancelable template generation scheme that generates a secure cancelable template based on signcryption. The signcryption scheme used encompasses HECC and bio hash functions. The flow of the proposed approach is given in the Figure 1. The iris image of the user is pre-processed with localization, segmentation, normalization, and HGLD feature extraction. The pre-processed iris image is signcrypted using HEC signcryption, and the final cancelable template is stored in the database. In the verification stage, the same procedure is computed, and the cancelable template is compared with the one stored in the database.

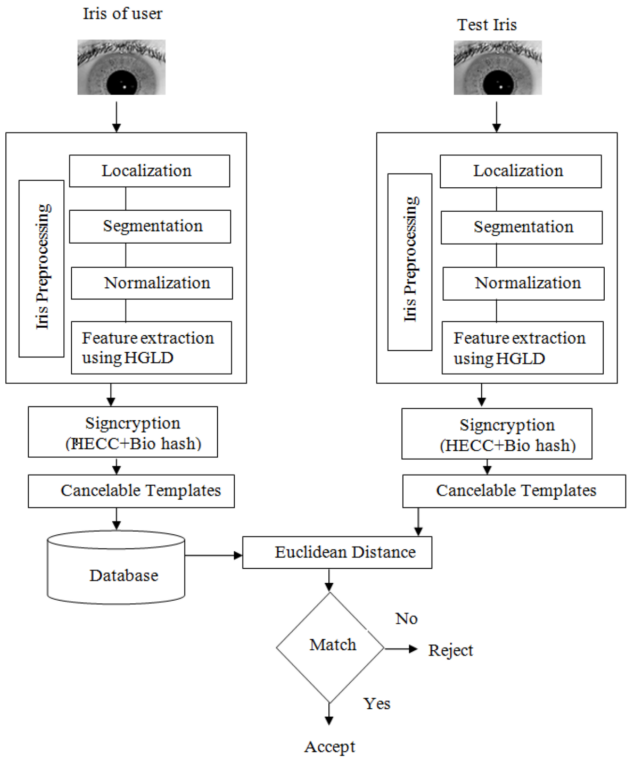

Figure 1. The flow of the proposed approach.

3.2. Iris Pre-Processing

Preprocessing is defined as a procedure that removes noise in an iris image acquired using an optical camera or other devices [20]. To perform iris segmentation for perfect iris recognition, the noise from the captured iris image has to be removed due to acquisition and blurring. The steps involved in preprocessing are: (a) iris localization, (b) iris normalization, (c) iris segmentation, and (d) feature extraction using HGLD.

3.2.1. Iris Localization

Recognition of the iris boundary both internally and externally is necessary for localization. The pupils and iris sclera must be distinguished without making any mistakes. The coarse-to-fine approach of localization is used in the present investigation. The cutoff point of an image in a few dark areas makes up the coarse stage. The suggested method, as shown in Equation (1), employs a three-level cutoff system based on histogram analytics. The proposed approach is significantly more suitable for a variety of intensity circumstances thanks to the offered threshold mechanism.

$$Threshold = \begin{cases} 120 : \sum_{i=155}^{260} h_i < 0.80RC \\ 60 : \sum_{i=0}^{i=100} h_i < 0.35RC \\ 90 : Otherwise \end{cases} \quad (1)$$

where h_i indicates the histogram based on the pixel intensity *i*. *RC* represent the number of rows and columns in the iris image, respectively.

3.2.2. Iris Segmentation

When an iris image is segmented, the pupil and limbic borders are automatically recognized. This method uses Hough transform for iris segmentation. The first step is to identify the initial derivative of pixels in the iris image. The second step is to calculate the edge point by the threshold. The general Hough equation is given in Equations (2)–(4).

$$h(r, x_c, y_c) = \sum_{i=1}^{n} h(r, x_c, y_c, x_i, y_j) \quad (2)$$

where

$$h(r, x_c, y_c, x_i, y_j) = \begin{cases} 1, \ if \ g(r, x_c, y_c, x_i, y_j) \\ 0, \ Otherwise \end{cases} \quad (3)$$

$$g(r, x_c, y_c, x_i, y_j) = (x_i - x_c)^2 + (y_i - y_c)^2 - r^2 \quad (4)$$

where $(x_i, y_i) = 1$ to n is the entire boundary point of iris image. Among these, for each boundary point (x_i, y_i), if there exists $g(r, x_c, y_c, x_i, y_i)$ identified by the parameter $g(r, x_c, y_c)$, then that point might pass through the given boundary (x_i, y_i). Consequently, if the circle moving through has the most boundary points, the Hough transform is quite able to constitute the circumference parameter to be measured, referring to the highest value.

3.2.3. Iris Normalization

Iris normalization is the following phase of iris segmentation. It results in an iris region with a consistent dimension. Daugman's rubber sheet model is the iris normalization technique that is most frequently employed. Every iris area must be translated to a pair of Cartesian coordinates (s, θ), where s represents the range [0, 1] and specifies an angle $[0, 2\pi]$. The following Equations (5)–(7) outline how to remap iris samples from Cartesian to polar coordinates.

$$i(u(s, \theta), v(s, \theta)) \rightarrow i(s, \theta) \quad (5)$$

$$u(s,\theta) = (i-s)u_p(\theta) + su_i(\theta) \tag{6}$$

$$v(s,\theta) = (i-s)v_p(\theta) + sv_i(\theta) \tag{7}$$

where *i(u, v)* represents the iris location, *(u, v)* denotes the Cartesian coordinates, *(s, θ)* denotes the polar coordinates, (u_p, v_p) means the pupil boundaries, and (u_i, v_i) refers to the iris boundaries.

3.2.4. Iris Feature Extraction

The feature extraction mechanism used in the proposed approach is HGLD. The HGLD technique is used for the extraction of perfect features. The grey level gap is defined in various directions by the HGLD matrix and expressed as a set of the contiguous intensities of the very same grey level. Let the total number of pixels for the iris image *I(x, y)* be *n* and the total number of grey levels in the iris be denoted by *g*. Let *r* be the pixel's longest run and the HGLD matrix be of size *(g, r).* Each element *E(i, j | θ)* specifies the total number of runs with the length *j* and *I* grey levels in the direction *θ*. From this matrix, seven features are extracted: short run highlight (SRH), long run highlight (LRH), non-uniformity in grey level (NGL), non-uniformity in run length (NRL), total run percentage (TRP), low grey level run highlight (LGLRH), and high gray level run highlight (HGLRH). These features are specified in Equations (8)–(14).

$$SRH = \sum_{i=1}^{g}\sum_{j=1}^{r}\frac{E(i,j|\theta)}{j^2} \Big/ \sum_{i=1}^{g}\sum_{j=1}^{r}\frac{E(i,j|\theta)}{1} \tag{8}$$

$$LRH = \sum_{i=1}^{g}\sum_{j=1}^{r} j^2 \times E(i,j|\theta) \Big/ \sum_{j=1}^{r} E(i,j|\theta) \tag{9}$$

$$NGL = \sum_{i=1}^{g}\left(\sum_{j=1}^{r} E(i,j|\theta)\right)^2 \Big/ \sum_{i=1}^{g}\sum_{j=1}^{r} E(i,j|\theta) \tag{10}$$

$$NRL = \sum_{j=1}^{r}\left(\sum_{i=1}^{g} E(i,j|\theta)\right)^2 \Big/ \sum_{i=1}^{g}\sum_{j=1}^{r} E(i,j|\theta) \tag{11}$$

$$TRP = \frac{1}{n}\sum_{i=1}^{g}\sum_{j=1}^{r} E(i,j|\theta) \tag{12}$$

$$LGLRH = \sum_{i=1}^{g}\sum_{j=1}^{r}\frac{E(i,j|\theta)}{i^2} \Big/ \sum_{i=1}^{g}\sum_{j=1}^{r}\frac{E(i,j|\theta)}{1} \tag{13}$$

$$HGLRH = \sum_{i=1}^{g}\sum_{j=1}^{r} i^2 \times E(i,j|\theta) \Big/ \sum_{i=1}^{g}\sum_{j=1}^{r} E(i,j|\theta) \tag{14}$$

3.3. Signcryption for Generating Secure Cancelable Templates

The proposed approach uses the signcryption technique to generate a secure cancelable template. In this, the signcryption process involves HECC combined with a bio hash function.

The primary step in signcryption is the bio hash function, and its flow is given in Figure 2. The random vector is generated from the cancelable template of dimension $m \times n$. The orthonormal projection matrix is the inner product, with the feature extracted from the HGLD feature extraction. The final $m \times 1$ vector is the bio hash vector.

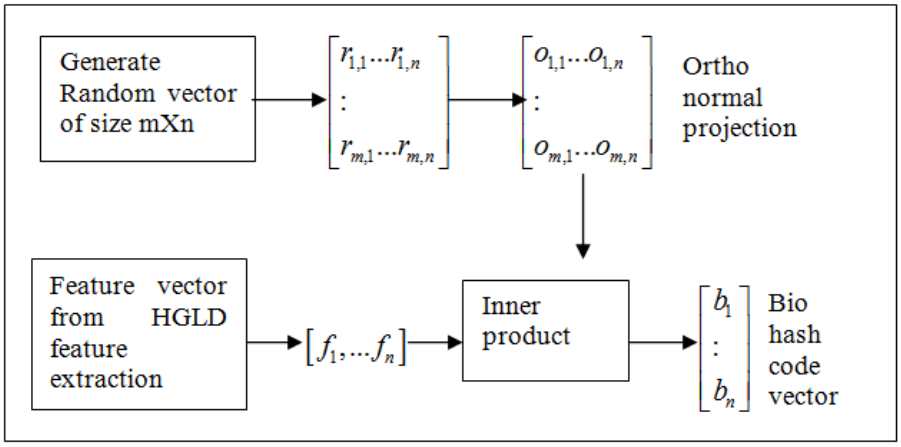

Figure 2. Bio hash function.

3.3.1. Bio Hashing

Bio hashing is defined as biometric salting in which a random number is combined with biometric features. Initially, the supplementary data are used to generate the random matrix, which is unique to every user. The column of this matrix is normalized using Gram–Schmidt Orthonormalization (GSON). From the literature, it has been identified that the GSON is the optimal normalization technique compared to median normalization, min–max normalization and Z-score normalization. The GSON is applied to the biometric feature vector obtained using HGLD feature extraction. The original biometric feature vector (r) is transformed by distributing it along the vectors of the orthonormalized random matrix in the interval $[-1, 1]$. Let S be the vector space and $r_1, r_2, \ldots, r_n$ be the basis feature vector for S. The orthogonal function for the bio hash is calculated using Equations (15)–(17).

$$S_1 = r_1 \tag{15}$$

$$S_2 = r_2 - \frac{r_2 \cdot S_1}{S_1 \cdot S_1} S_1 \tag{16}$$

$$S_n = r_n - \frac{r_n \cdot S_{n-1}}{S_{n-1} \cdot S_{n-1}} S_{n-1} \tag{17}$$

where $S_1, S_2, \ldots, S_n$ are the orthogonal basis for S. The transformed template is known as the message digest or the bio hash code. For diverse applications, each user may have as many bio hash codes as possible tokens. From the literature, bio hashing has been observed to achieve lower ERR for modalities that enhance the performance of biometric recognition significantly [21–23]. If the bio hash codes are stored in a database, this may lead to an adversary attack, since it is invertible. To make the hash code more secure, it is combined with the cryptographic technique in signcryption. In this, the hash code is converted into a non-invertible cancelable template also called an electronic digest. The generation of a bio hash code is given in Algorithm 1.

Algorithm 1: Generation of Bio Hash Code through the Bio Hash Function

Input: Feature vector from HGLD and random matrix
Output: Bio hash code
Process:
Step 1: Generate a random matrix of size $m \times n$
Step 2: Normalize the random matrix using GSON Orthonormal projection
Step 3: Perform inner product GSON matrix and HGLD feature vector
Step 4: The output matrix is bio hash code $[b_1, b_2, \ldots b_n]$

3.3.2. Signcryption for the Generation of Secure Cancelable Templates

The structure of signcryption for generating cancelable templates is shown in Figure 3. The bio hash code generated from the previous step is given as the input to the HECC approach to generate a secure cancelable template. As the bio hash codes are invertible, they are easily susceptible to malicious attacks by an adversary if they are directly stored in the database. The solution for this problem is to convert an invertible bio hash code into a non-invertible transformed template. The bio hash code is converted to divisors as given in Algorithm 2.

Algorithm 2: Bio Hash Code Converted into Divisors

Input: Bio hash code
Output: $d = (X^2 + A^*X + B, C^*X + D) \bmod p$
Process:
Step 1: Convert bio hash code into a set of two points: *p1(a1,b1)* and *p2(a2,b2)*
Step 2: Compute the following $A = (-a_1, -a_2) \bmod p$ and $B = (a_1{}^*a_2) \bmod p$
Step 3: Compute $C^*a_1 + D = b_1$ and $C^*a_2 + D = b_2$
Step 4: Return the divisor as $d = (X^2 + A^*X + B, C^*X + D) \bmod p$

After the divisor is obtained from the bio hash code, the remaining procedure followed is similar to that of the previous approach.

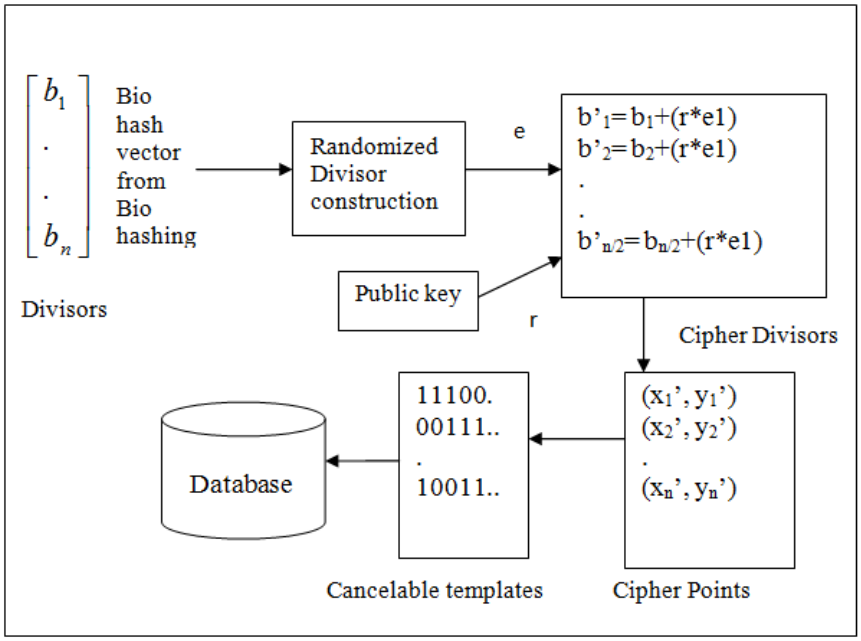

Figure 3. Signcryption for the generation of secure cancelable templates.

4. Results and Discussion

The experiment was run on a computer with an Intel Core i5 processor and 6 GB of RAM with Anaconda Python simulator. Two standard state-of-the-art datasets CASIA version 4.0 and IITD were used in this experimental analysis. The following metrics were used to determine the feasibility of the proposed approach based on the terminology stated above: false acceptance rate (FAR), false rejection rate (FRR), true positive rate (TPR) [24–26], true negative rate (TNR), equal error rate (EER), and accuracy.

- *FAR:* It indicates the likelihood that a system would mistakenly accept an unregistered or unauthorized user.

$$FAR = \frac{FP}{TN + FP} \tag{18}$$

- *FRR:* It indicates the likelihood that a system may mistakenly reject an unregistered or unauthorized user.

$$FRR = \frac{FN}{TP + FN} \tag{19}$$

- *TPR*: It indicates the likelihood that a system will approve the user who has registered in an authentication process. Recall, also known as sensitivity, is the proportion of true positives acquired among the real positives.

$$TPR = \frac{TP}{TP + FN} \tag{20}$$

- *TNR:* It indicates the likelihood that a system will reject an unauthorized user. Specificity is another name for it.

$$TNR = \frac{TN}{TN + FP} \tag{21}$$

- *EER:* It represents the rate at which FAR and FRR are equivalent.
- *Accuracy:* The frequency with which the authorized users are given access determines how many tries they make.

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{22}$$

4.1. Performance Analysis

Various iris data from CASIA and IITD were taken into consideration for the experimental investigation to determine the viability of the proposed methodology. The parameters to be considered for the evaluation of the proposed method were FAR, FRR, TPR, TNR, and F-Score [27,28]. The parameters when implemented on the CASIA dataset are shown in Table 1.

Table 1. Performance evaluation of cancelable approaches (HGLD, signcryption) on the CASIA iris dataset.

No. of Iris Samples	TP	FN	FP	TN	FAR (%)	FRR (%)	TPR (%)	TNR (%)	F-Score
100	100	0	0	100	0	0	100	100	100
300	300	0	0	300	0	0	100	100	100
500	500	0	0	500	0	0	100	100	100
800	799	1	0	800	0	0.13	99.88	100	99.94
1000	999	1	1	999	0.1	0.1	99.9	99.9	99.9
1300	1298	2	1	1299	0.08	0.15	99.85	99.92	99.88
1500	1498	2	2	1498	0.13	0.13	99.87	99.87	99.87
1800	1797	3	2	1798	0.11	0.17	99.83	99.89	99.86
2100	2097	3	3	2097	0.14	0.14	99.86	99.86	99.86

The 2100 iris samples were taken from CASIA dataset and analyzed with the proposed cancelable approach. The maximum TPR and TNR achieved with this dataset was 100%. The maximum FAR and FRR was 0.14%, which is much lower compared to two previously proposed cancelable schemes. The average minimum TPR and TNR was about 99.64%. The accuracy of the proposed approach was 99.86% for the CASIA V4 iris dataset. The maximum F-Score was 100% and minimum F-Score was 99.86%. The same parameters when implemented with the IITD iris dataset are shown in Table 2.

Table 2. Performance evaluation of cancelable approaches (HGLD, signcryption) on the IITD Iris dataset.

No. of Iris Samples	TP	FN	FP	TN	FAR (%)	FRR (%)	TPR (%)	TNR (%)	F-Score
100	100	0	0	100	0	0	100	100	100
300	300	0	0	300	0	0	100	100	100
500	500	0	0	500	0	0	100	100	100
800	799	1	0	800	0	0.13	99.88	100	99.94
1000	999	1	1	999	0.1	0.1	99.9	99.9	99.9
1300	1298	2	1	1299	0.08	0.15	99.85	99.92	99.88
1500	1497	3	2	1498	0.13	0.2	99.8	99.87	99.83
1800	1797	3	2	1798	0.11	0.17	99.83	99.89	99.86
2100	2096	4	4	2096	0.19	0.19	99.81	99.81	99.81

The same number of iris samples was taken from the IITD iris dataset and analyzed with the proposed cancelable approach. The maximum TPR and TNR achieved with this dataset was 100%, and it is same for around 500 iris samples. The graphical representation of FAR and FRR of the CASIA dataset is shown in Figure 4. The maximum FAR and FRR was 0.19%. The average minimum TPR and TNR was about 99.81%, which is a bit lower when implemented on the CASIA iris dataset. The maximum F-Score was 100% and minimum F-Score was 99.81%.

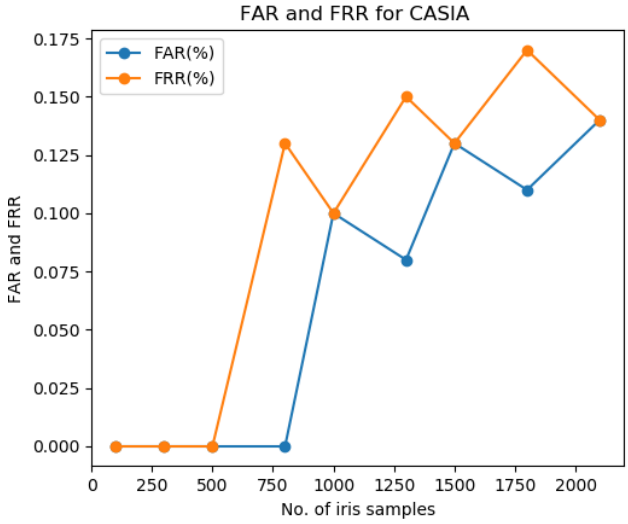

Figure 4. Plot of FAR, FRR in CASIA iris dataset.

In both datasets, the x-axis was plotted with the number of iris samples and the y-axis was plotted with FAR and FRR percentages. The plot of FAR and FRR for number of iris samples in the IITD iris dataset is shown in Figure 5. The minimum FAR and FRR was 0% for 500 iris samples in the CASIA and IITD iris datasets. The accuracy of the CASIA iris dataset was 99.77%. The proposed method provides a lower EER of 0.27%, whereas the EER of the cancelable (RP, DRPE) approach was 0.46%. The average FAR of the scheme was 0.15%, and the average FRR was 0.15% for the CASIA V4 dataset.

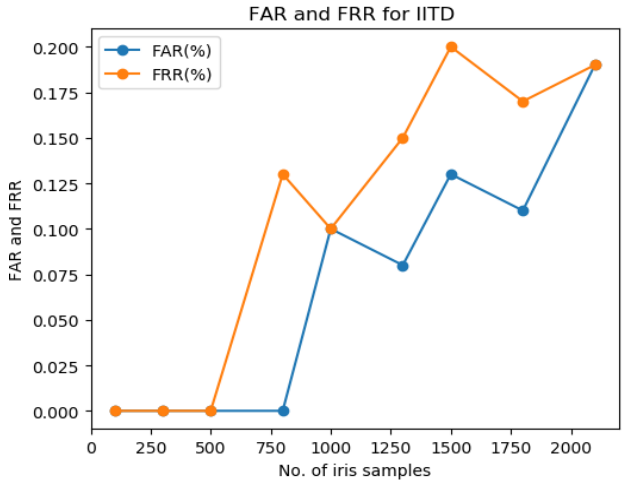

Figure 5. Plot of FAR and FRR in the IITD iris dataset.

The accuracy and EER of the IITD iris dataset was 99.77% and 0.27%, respectively. The analysis shows that the proposed method has improved performance in terms of FAR, FRR, TPR, TNR, accuracy, and F-Score. The EER is considerably low compared to that of the cancelable template generation based on random projection and double random phase encoding.

4.2. Comparison of the Proposed Approach with Existing Approaches

The performance of the proposed approach is compared with the state-of-the-art cancelable biometric schemes. The major advantage of the proposed signcrypted approach is lower EER and greater accuracy with more security. Table 3 represents a comparison of the EER of the proposed scheme with the existing approaches.

Table 3. Comparison of the EER and the accuracy of cancelable approaches (HGLD, signcryption) with the existing schemes.

Method	Dataset Used	Algorithm Used	EER in (%)
Tarek et al. [18]	CASIA V3	BAM neural network	3.56
Tarek et al. [19]	CASIA V3	Bidirectional memory model	2.00
Lai et al. [20]	CASIA V3	Index first one hashing	0.54
Kaur et al. [29]	IITD	Random distance	0.60
Gomez-Barrero et al. [21]	IITD	Bloom filter	4.3
Soliman et al. [22]	CASIA V3	Random projection	0.58
		Fractional Fourier transform	0.63
		Modified logistic map	1.17
Drozdowski et al. [25]	CASIA and IITD	Random permutation to iris code	1.99
Gomez-Barrero et al. [21]	CASIA	Bloom filter	0.7
Kabir et al. [27]	IITD	Normalization	0.62
Sadhya et al. [1]	CASIA V3	Randomized bit sampling	1.4
Ghammam et al. [11]	CASIA	Index of max hashing	1.47
Rajasekar et al. [12]	CASIA and IITD Iris Dataset	RP and DRPE	0.46
		2D Gabor + HECC approach	0.27
Proposed Cancelable Template Generation based on signcryption	CASIA and IITD Iris Datasets	HGLD + signcryption (HECC + bio hash function)	0.1

From the interpretation, it is clear that the proposed approach shows a lower EER of 0.1% compared to that the state-of-the-art existing approaches.

5. Conclusions

The proposed approach provides a novel cancelable template generation mechanism based on signcryption. Signcryption uses hyperelliptic curve cryptography for encryption and a bio hash function for the generation of bio hash vectors from the iris biometric. Iris preprocessing involves iris localization, iris segmentation, iris normalization, and iris feature extraction using the HGLD feature extraction mechanism. The cancelable templates are generated from the iris biometrics of both the CASIA and IITD iris datasets. The proposed methodology provides secure cancelable generation with lower EER and a higher accuracy rate. The qualitative research demonstrates that previous comparative approaches do expose some structure to the initial biometric; the proposed methods can modify original credentials without doing so. The quantitative study demonstrates that the suggested methods outperformed the existing methods. The proposed methods have the following advantages: (i) they are independent of the original biometric picture's color or greyscale content; and (ii) they do not divulge any details about the initial credentials. Future research will examine new techniques that include fusion strategies with the optimization procedure. Multimodal biometrics can be included in cancelable template generation, which produces better qualitative and quantitative metrics.

Author Contributions: Conceptualization, V.R., M.S. and D.K.; methodology, V.R., M.S., D.K. and D.S.; software, E.D. and S.K.; validation, E.D. and S.K.; writing—original draft preparation, V.R., M.S., D.K., D.S., E.D. and S.K.; writing—review and editing, V.R., M.S., D.K., D.S., E.D. and S.K; supervision, D.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Sadhya, D.; Raman, B. Generation of cancelable iris templates via randomized bit sampling. *IEEE Trans. Inf. Secur.* **2019**, *14*, 2972–2986. [CrossRef]
2. Rajasekar, V.; Predić, B.; Saracevic, M.; Elhoseny, M.; Karabasevic, D.; Stanujkic, D.; Jayapaul, P. Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm. *Sci. Rep.* **2022**, *12*, 622. [CrossRef] [PubMed]
3. Velliangiri, S.; Manoharn, R.; Ramachandran, S.; Venkatesan, K.; Rajasekar, V.; Karthikeyan, P.; Kumar, P.; Dhanabalan, S.S. An Efficient Lightweight Privacy-Preserving Mechanism for Industry 4.0 Based on Elliptic Curve Cryptography. *IEEE Trans. Ind. Inform.* **2021**, *18*, 6494–6502. [CrossRef]
4. Rajasekar, V.; Premalatha, J.; Sathya, K. Cancelable Iris template for secure authentication based on random projection and double random phase encoding. *Peer–Peer Netw. Appl.* **2021**, *14*, 747–762. [CrossRef]
5. Rajasekar, V.; Premalatha, J.; Sathya, K.; Saračević, M. Secure remote user authentication scheme on health care, IoT and cloud applications: A multilayer systematic survey. *Acta Poly Tech. Hung.* **2021**, *18*, 87–106. [CrossRef]
6. Singh, A.; Vashist, C.; Gaurav, P.; Nigam, A. A generic framework for deep incremental cancelable template generation. *Neurocomputing* **2022**, *467*, 83–98. [CrossRef]
7. Manisha; Kumar, N. CBRC: A novel approach for cancelable biometric template generation using random permutation and Chinese Remainder Theorem. *Multimed Tools Appl.* **2022**, *81*, 22027–22064. [CrossRef]
8. Pandey, F.; Dash, P.; Sinha, D. Attack-resistant and efficient cancelable codeword generation using random walk-based methods. *Arab. J. Sci. Eng.* **2022**, *47*, 2025–2043. [CrossRef]
9. Asthana, R.; Walia, G.S.; Gupta, A. Random area-perimeter method for generation of unimodal and multimodal cancelable biometric templates. *Appl. Intell.* **2021**, *51*, 7281–7297. [CrossRef]
10. Siddhad, G.; Khanna, P. Max-min threshold-based cancelable biometric templates for low-end devices. *J. Electron. Imaging* **2022**, *31*, 033025. [CrossRef]

11. Ghammam, L.; Karabina, K.; Lacharme, P.; Atighehchi, K. A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing. *IEEE Trans. Inf. Secur.* **2020**, *15*, 2869–2880. [CrossRef]
12. Rajasekar, V.; Premalatha, J.; Sathya, K. Enhanced biometric recognition for secure authentication using iris preprocessing and hyperelliptic curve cryptography. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8841021. [CrossRef]
13. El-Rahiem, A.b.d.; Fathi, E.; El Samie, A.b.d.; Amin, M. Efficient cancellable multi-biometric recognition system based on deep learning and bio-hashing. *Appl. Intell.* **2022**, 1–15. [CrossRef]
14. Rajasekar, V.; Varadhaganapathy, S.; Sathya, K.; Premalatha, J. An efficient lightweight cryptographic scheme of signcryption based on hyperelliptic curve. In Proceedings of the 2016 3rd International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 3–5 March 2016; pp. 394–397.
15. Sakr, A.S.; Pławiak, P.; Tadeusiewicz, R.; Hammad, M. Cancelable ECG biometric based on combination of deep transfer learning with DNA and amino acid approaches for human authentication. *Inf. Sci.* **2022**, *585*, 127–143. [CrossRef]
16. Choudhary, S.K.; Naik, A.K. Protected Biometric Identification with Multiple Finger Vein. In Proceedings of the 2022 2nd Asian IEEE Conference on Innovation in Technology (ASIANCON), Ravet, India, 26–28 August 2022; pp. 1–6.
17. Rathgeb, C.; Wagner, J.; Tams, B.; Busch, C. Preventing the cross-matching attack in Bloom filter-based cancelable biometrics. In Proceedings of the 3rd International Workshop on Biometrics and Forensics (IWBF 2015), Gjovik, Norway, 3–4 March 2015; pp. 1–6.
18. Tarek, M.; Ouda, O.; Hamza, T. Robust cancellable biometrics scheme based on neural networks. *IET Biom.* **2016**, *5*, 220–228. [CrossRef]
19. Tarek, M.; Ouda, O.; Hamza, T. Pre-image Resistant Cancelable Biometrics Scheme Using Bidirectional Memory Model. *Int. J. Netw. Secur.* **2017**, *19*, 498–506.
20. Lai, Y.L.; Jin, Z.; Teoh AB, J.; Goi, B.M.; Yap, W.S.; Chai, T.Y.; Rathgeb, C. Cancellable iris template generation based on Indexing-First-One hashing. *Pattern Recognit.* **2017**, *64*, 105–117. [CrossRef]
21. Gomez-Barrero, M.; Rathgeb, C.; Li, G.; Ramachandra, R.; Galbally, J.; Busch, C. Multi-biometric template protection based on bloom filters. *Inf. Fusion* **2018**, *42*, 37–50. [CrossRef]
22. Soliman, R.F.; Amin, M.; Abd El-Samie, F.E. A double random phase encoding approach for cancelable iris recognition. *Opt. Quantum Electron.* **2018**, *50*, 1–12. [CrossRef]
23. Soliman, R.F.; Amin, M.; Abd El-Samie, F.E. A modified cancelable biometrics scheme using random projection. *Ann. Data Sci.* **2019**, *6*, 223–236. [CrossRef]
24. Soliman, R.F.; Ramadan, N.; Amin, M.; Ahmed, H.H.; El-Khamy, S.; Abd El-Samie, F.E. Efficient cancelable Iris recognition scheme based on modified logistic map. *Proc. Natl. Acad. Sci. India Sect. A Phys. Sci.* **2020**, *90*, 101–107. [CrossRef]
25. Drozdowski, P.; Garg, S.; Rathgeb, C.; Gomez-Barrcro, M.; Chang, D.; Busch, C. Privacy-preserving indexing of Iris-codes with cancelable Bloom filter-based search structures. In Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO), Rome, Italy, 3–7 September 2018; pp. 2360–2364.
26. Bendib, I.; Meraoumia, A.; Haouam, M.Y.; Laimeche, L. A New Cancelable Deep Biometric Feature Using Chaotic Maps. *Pattern Recognit. Image Anal.* **2022**, *32*, 109–128. [CrossRef]
27. Kabir, W.; Ahmad, M.O.; Swamy, M.N.S. Normalization and weighting techniques based on genuine-impostor score fusion in multi-biometric systems. *IEEE Trans. Inf. Secur.* **2018**, *13*, 1989–2000. [CrossRef]
28. Kaur, H.; Khanna, P. Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing. *Future Gener. Comput. Syst.* **2020**, *102*, 30–41. [CrossRef]
29. Kaur, H.; Khanna, P. Random distance method for generating unimodal and multimodal cancelable biometric features. *IEEE Trans. Inf. Secur.* **2018**, *14*, 709–719. [CrossRef]