# Efficient Implementation of An Elliptic Curve Cryptosystem for Cancelable Biometrics

Ahmed A. Asaker
*Reactors Department*
*Egyptian Atomic Energy Authority*
Cairo, Egypt
https://orcid.org/ 0000-0002-6725-9952

Zeinab F. Elsharkawy
*Engineering Department*
*Egyptian Atomic Energy Authority*
Cairo, Egypt
zeinab_elsharkawy@yahoo.com

Sabry Nassar
*Reactors Department*
*Egyptian Atomic Energy Authority*
Cairo, Egypt
sabrynassar39@gmail.com

Nabil Ayad
*Reactors Department*
*Egyptian Atomic Energy Authority*
Cairo, Egypt
n_ayad1951@yahoo.com

O. Zahran
*Faculty of Electronic Engineering*
*Menoufia University*
Menoufia, Egypt
osama_zahran@el-eng.menofia.edu.eg

Fathi E. Abd El-samie
*Faculty of Electronic Engineering*
*Menoufia University.*
Menoufia, Egypt
fathi_sayed@yahoo.com

***Abstract*— With the increasing demands for biometric systems in our daily life for automatic identification of individuals, recently iris recognition system has gained a lot of attention attributed to its reliability, uniqueness, difficulty to be imitated and high accuracy in comparison with other available biometric recognition systems. Unfortunately, templates in traditional iris recognition system are unprotected and vulnerable to various threats, such as attacks at the iris reader level or at the database level. Hence, there is a need for developing a system for securing the existing iris recognition system for keeping the original biometrics safe and secure. In this paper, we introduce a hybrid model for protecting iris recognition system through combining an elliptic curve cryptosystem with a new salting-based cancelable iris recognition scheme. The obtained experimental results on CASIA-IrisV3 database proved that the proposed system guarantees a high degree of security and privacy protection without affecting the accuracy.**

***Keywords*—Iris Recognition System, Cancelable Biometrics, Elliptic Curve Cryptography, Hamming Distance, Normalized Cross Correlation, Receiver Operating Characteristics.***

## I. INTRODUCTION

Recent years have seen an exponential growth in the use of various biometric technologies for trusted automatic recognition of humans, whereas biometric techniques permit easier recognition depending on an individual's behavioral or physical features. Biometrics possess the ability to differentiate between a deceptive user and authorized one, which is one of the distinguished rationales that make them popular [1, 2]. In iris recognition, a person is identified by his/her iris, which is the circular disk between the inner pupil and the outer white sclera in the eye. Recently, iris recognition became a famous technique that is commonly used because of its reliability, discriminability, accuracy performance and stability [3].

Generally, for both verification and identification tasks in iris recognition system, initially, each individual has to enroll his/her iris data into the local iris reader. During this process, the individual's eye image is captured, the iris region is localized, and the effects of eyelids and eyelashes that represent noise in the iris images are eliminated. Then, the localized irises are transformed from polar to rectangular coordinates for normalization in order to distinguish the irises regardless of the position, rotation and size, and exclude dimensional inconsistencies between irises. After that, discriminating features (e.g. IrisCodes) are extracted and coded from the normalized irises. IrisCodes are stored in the database server located remotely as shown in Fig. 1. During the authentication process, only the right person can be verified or identified successfully through the matching of his/her IrisCode with the enrolment database [4].

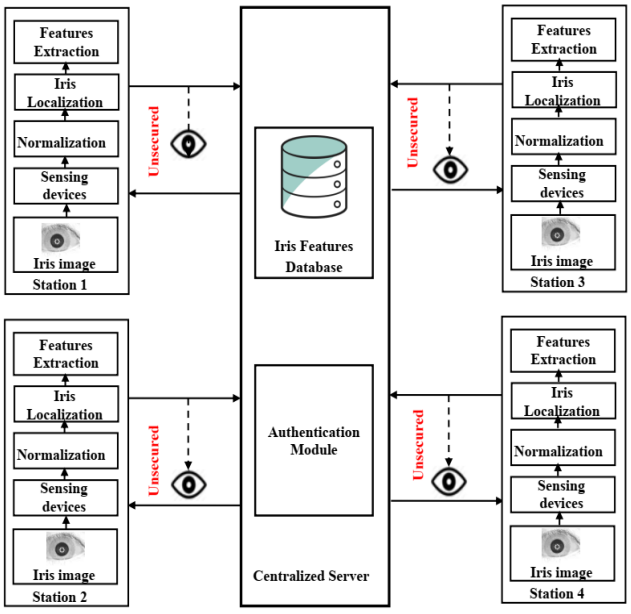



Fig. 1: Traditional iris recognition system [5].

As the biometric applications expand, confidentiality and security cannot be overlooked. Since IrisCodes contain highly discriminatory information of individuals, the exposure of an individual's IrisCode to an adversary may lead to security breaches such as masquerade attack and replay attack. Furthermore, due to the fact that human iris is permanently associated to each individual, the exposure of an individual's IrisCode implies a permanent loss of identity. The invariance of the individual's biometric information over time is one of the characteristics behind the exponential use of biometric recognition systems for authentication purposes. However, this invariability is one of biometrics' problems, because an individual's biometrics cannot be replaced when compromised. In addition, multiple IrisCodes can be cross-matched by destroying multiple databases, which may cause serious user privacy violations.

Subsequently, in order to alleviate this problem, it is desirable that a biometric recognition system does not keep the original biometric information in database storage, and also does not use the original biometric information for recognition. In contrary, the system only keeps the noninvertible transformed or salted versions and uses these versions for recognition. When it is discovered that these data have been stolen, other transformation or salting methods can be used to replace the biometric data, but users should capture their biometric data again. In addition, it is desired that the impostors cannot recover the original biometrics from these transformed and/or salted data [6, 7].

In this paper, we propose a novel hybrid system that effectively combines feature transformation and a biometric cryptosystem to protect the iris template. In this system, the IrisCode extracted in the local iris reader is blended pixel-wise with a user-specific binary synthetic pattern using XOR operation for creating a cancelable IrisCode. After that, a specially designed elliptic curve cryptosystem is used to encrypt the cancelable IrisCode and generate a protected IrisCode. Finally, the protected IrisCode is sent to the centralized server for storage, and similarity comparison is performed between the received cancelable IrisCode and all registered IrisCodes. The proposed system guarantees a high degree of privacy/security protection without affecting the performance accuracy.

The rest of this paper is organized as follows. In Section II, previous techniques for protecting biometrics are revisited and summarized. In Section III, the detailed mathematics of ECC are re-visited and summarized. In Section IV, the different stages of the proposed iris recognition system are presented. Section V presents the experimental results and discussions. Finally, the concluding remarks of this work are presented in Section VI.

## II. Related Work

For securing biometric information, different methods have been proposed in recent years. According to the review article of Jain *et al.* [8], biometric protection techniques can be classified into three main categories: feature transformation, biometric cryptosystems, and hybrid systems.

In feature transformation, the biometric information is noninvertibly transformed, and the transformed versions are used for recognition instead of using the original data [6]. For feature transformation and generation of cancelable biometric templates, a number of recent methods can be used. In [9], random projection was used as a method of protection for iris recognition systems, during which random projections are applied directly on the iris images generating cancelable iris templates. However, this method usually degrades the system accuracy.

BioHashing methods [10], which are essentially extensions of random projection, are also widely used for generating cancelable biometric templates. In BioHashing, the biometric distinctive features are firstly extracted from the input biometric data, and then a set of orthogonal random vectors based on user-specific random numbers are calculated. The BioHash template is the dot product of the biometric feature vector with one of orthogonal random vectors.

Another means of producing cancelable biometric templates is employing the salting approach [11]. In the salting approach, biometric information is mixed with an auxiliary data such as a user-specific synthetic pattern. The independence of patterns ensures the discriminability between users. Additionally, the auxiliary data are revocable and can be reinitiated when compromised.

Biometric cryptosystem [8] is the second approach of providing a higher assurance of biometric system security, in which, different encryption techniques are applied on the biometric information to be transformed into an unreadable data format. In [12], 2D chaotic sequences from multi-scroll chaotic attractors were used for encrypting the biometric data. In [13], a lossless encryption algorithm based on chaotic theory using Arnold and Henon maps was proposed for generating ciphered fingerprint data. In [14], a specially designed fingerprint encryption/decryption algorithm that combines 2D chaotic map and elliptic curve cryptography was proposed. In [15], a fully-homomorphic encryption technique was used to provide protection for preserving the privacy of biometric data.

The third approach for protecting the biometric data employs hybrid systems [6], in which a combination of different technologies is utilized for providing higher assurance of system security. In [16], biometric patterns are secured by using a combination of visual cryptography and least significant bit steganography. In [17], a hybrid system was proposed, in which the iris template is encrypted using triple data decryption and two-fish algorithms, and then using least significant bit steganography, the cipher data is embedded into a cover image for producing a stego-image.

In spite of the existence of several techniques for protecting biometric information, most of these techniques affect negatively on the system accuracy compared to traditional biometric recognition systems. This motivated us to design a new lightweight, robust and secure system that effectively enhances the security of biometric recognition systems without affecting the accuracy.

## III. Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) is an asymmetric cryptographic technique that uses two different keys for the encryption and decryption process. It is one of the most effective encryption techniques due to its higher security, smaller key size and fewer computations, less memory usage and lower power consumption [18, 19]. The difficulty of solving the elliptic curve discrete logarithm problem (ECDLP) from the adversaries is one of the advantages of ECC [18].

An elliptic curve over a prime field $F_l$ is defined by [18]:

$$y^2 = \{x^3 + jx + k\} \ (mod\ l) \qquad (1)$$

where $l \neq 2,3$, $j, k \in F_l$ and satisfy the condition $4j^3 + 27k^2 \neq 0\ (mod\ l)$.

The elliptic curve group ($F_l$) is composed of all points ($x$, $y$) which satisfy the elliptic curve equation given in Eq. (1) and the point of infinity $O$ [18].

The essential elliptic curve operations that have been used in the proposed cryptosystem are point addition, point

subtraction, point doubling and point multiplication with a scalar [18].

## IV. PROPOSED SYSTEM

This research presents a novel hybrid iris template protection system that combines feature transformation with biometric cryptosystem effectively to protect users' iris data during storage and transmission.

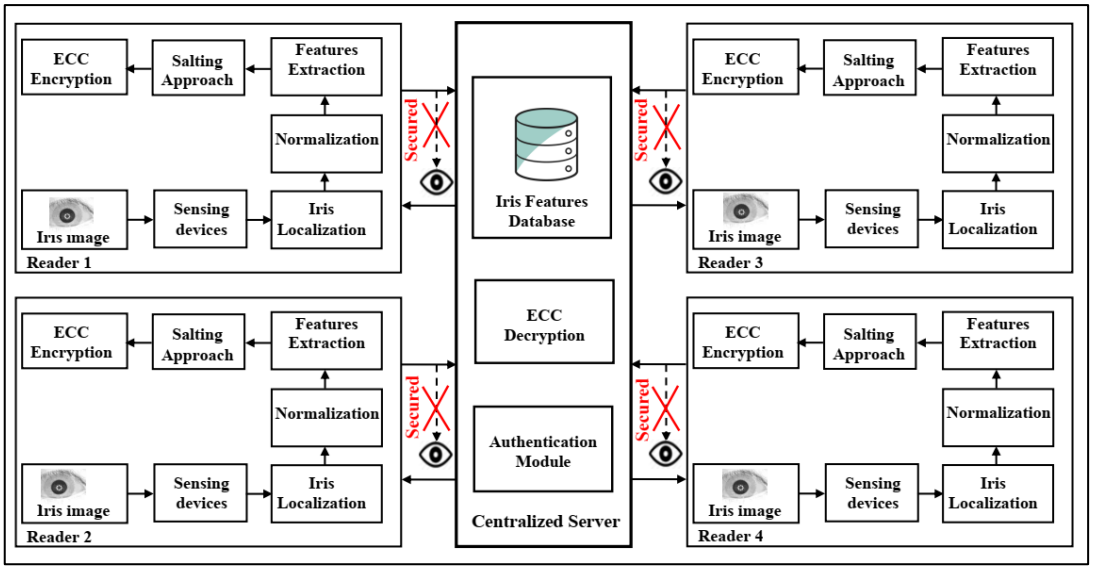



Fig. 2: The schematic diagram of the proposed iris recognition system.

Suppose $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are two different points that lie on an elliptic curve. The point addition operation can be achieved by obtaining the gradient ($S$) as follows [18]:

$$S = \frac{y_2 - y_1}{x_2 - x_1} \ mod\ l \quad (2)$$

$$x_3 = \{S^2 - x_1 - x_2\} \ mod\ l \quad (3)$$

$$y_3 = \{S\,x_1 - S\,x_3 - y_1\} \ mod\ l \quad (4)$$

$$R = P_1 + P_2 = (x_3, y_3) \quad (5)$$

The subtraction operation between two different points $P_1$ and $P_2$ can also be implemented as follows [18]:

$$P_1(x_1, y_1) - P_2(x_2, y_2) = P_1(x_1, y_1) + P_2(x_2, -y_2) \quad (6)$$

Point doubling operation for a point $P = (x_1, y_1)$ that lies on the elliptic curve can also be implemented using the following formula [18]:

$$S = \frac{3\,x_1^2 + j}{2\,y_1} mod\ l \quad (7)$$

where $j$ represents the coefficient of elliptic curve equation.

$$x_3 = \{S^2 - 2\,x_1\} \ mod\ l \quad (8)$$

$$y_3 = \{Sx_1 - Sx_3 - y_1\} \ mod\ l \quad (9)$$

$$2P = P + P = (x_3, y_3) \quad (10)$$

Scalar multiplication is the main operation on the elliptic curve cryptography that consumes more time in the proposed cryptosystem for encrypting and decrypting the biometric data. Multiplying the scalar $k$ with any point $P$ on the elliptic curve is performed to obtain another point $R$ ($R=kP$) on the elliptic curve, which can be implemented depending on point addition and point doubling, as shown below [18]:

$$R = 15P = 2\,(2(2P + P) + P) + P \quad (11)$$

If $k$ is large enough, it is mathematically infeasible to be obtained from given $P$ and $R$ [18].

In this section, the proposed iris recognition system is explained in detail. The proposed system is composed of four stages. Firstly, IrisCode extraction stage, in which distinctive features are extracted from each iris image in order to produce a bit-wise unique pattern (eg. IrisCode), is implemented. Secondly, cancelable IrisCode creation stage, in which a cancelable IrisCode is created by blending the original IrisCode pixel-wise with a user-specific binary synthetic pattern, is implemented. Thirdly, the iris cryptosystem, in which a specially designed elliptic curve cryptosystem is employed for encrypting the cancelable IrisCode, is implemented. Finally, pattern matching and decision making is implemented.

Consequently, the iris feature templates can be stored and transmitted from local iris readers to the remote centralized server and between multiple servers, more securely. The schematic diagram of the proposed system is shown in Fig. 2. The proposed system consists of $n$ iris readers and one centralized server. Iris readers are equipped with iris sensing devices, IrisCode extraction, cancelable IrisCode creation, and ECC encryption function. The centralized server consists of a database and an installed ECC decryption function that is used to decrypt the protected IrisCode received from the reader for further pattern matching and decision making through an authentication module.

### *A. Enrolment IrisCode Extraction (Reader A):*

In the proposed system, an iris image is taken for each user in the local iris reader. Iris localization is performed to detect and localize the boundary of the iris region from the eye image and isolate dark areas including eyelids, eyelashes and other types of noise to improve the matching performance. In our work, the coarse-to-fine approach [20] was applied for finding the iris boundaries. The dark regions

are isolated through thresholding the gray-scale iris image. Thresholding of the gray-scale image and getting the binary output will show the darker parts of the image in white. These parts represent both the pupil and the remaining effects of other noise. Then, by applying the Dougman integral differential operator given in Eq. (12) twice [4], the center and radius of both the pupil circle and the iris circle are obtained.

$$\max_{(r,xo,yo)} \left| G(r) * \frac{d}{dr} \oint_{r,xo,yo} \frac{I(x,y)}{2\pi r}\, ds \right| \quad (12)$$

Irises may be captured in different sizes with varying imaging distance. The radial size of the pupil may change according to illumination variations. Subsequently, the resulting deformation of the iris texture will affect the performance of subsequent feature extraction and matching stages. Therefore, the iris region needs to be normalized to compensate for these variations. Daugman's rubber sheet model was used in our work for mapping the pixels of the localized iris region into a normalized coordinate system [4]. In this system, every pixel on the iris image is defined by an angle varying from 0 to 360 degrees, and a radial coordinate ranging from 0 to 1. The normalized iris image is transformed into a binary matrix by convolving the upper-half part of the normalized iris with 1D Log-Gabor filters. The function generates real and imaginary parts, which are phase quantized to obtain an IrisCode in the form of 0 and 1 [21].

### *B. Enrolment Cancelable IrisCode Creation (Reader A):*

In this study, biometric salting is used to generate a cancelable IrisCode. In this technique, the extracted IrisCode in the local iris reader is blended pixel-wise with a user-specific binary synthetic pattern using XOR operation for generating a cancelable IrisCode. The independence of the binary synthetic patterns ensures the discriminability between different users and also satisfies the unlinkability of the proposed system. The binary synthetic patterns are revocable and can be regenerated when compromised. The proposed method for generating cancelable IrisCode can be described in the following four steps:

- Choose a unique binary synthetic pattern for each user. This binary pattern has the same size as the original IrisCode.
- The selected binary synthetic pattern is combined in a bit-wise manner with its associated original IrisCode for generating a cancelable IrisCode.
- Once the cancelable IrisCode is generated, the original IrisCode will be discarded.
- Input iris images for both enrolment and authentication are usually not aligned, and then if the user-specific binary synthetic pattern is applied during authentication at the wrong rotation, it will not generate a signature similar to what was enrolled (with a different orientation). Hence, an alignment step is added during the authentication stage, in which all possible rotations of the user-specific binary synthetic pattern was evaluated before combining it with the query IrisCode, by randomly shifting every binary synthetic pattern between +8 and -8 degrees, then measuring the similarity between the resultant template and the enrolled one for every shift. Until getting the best matching score, the query cancelable template is saved.

### *C. Enrolment Protected IrisCode Creation (Reader A)*:

In this step, a specially designed elliptic curve cryptosystem is employed in the local iris reader for encrypting the cancelable IrisCode.

At the beginning of the encryption process, both local iris reader $A$ and centralized server $B$ should be adjusted to a coefficients values ($j$ & $k$) of elliptic curve equation. A prime number $l$, the elements of the elliptic curve $E_l(j, k)$ group and a reference point $G(x, y)$ are selected from the elliptic curve group. Given the centralized server $B$ public key ($Q_B$), an individual's cancelable IrisCode ($P$) is encrypted in the local iris reader as follows:

- Selecting a private key ($d_A$) randomly from the interval [1, $l$ – 1], and then generating a public key ($Q_A = d_A * G$) using Eq. (11).
- Computation of the elliptic curve group.
- Partitioning the cancelable IrisCode ($P$) into binary-blocks ($m_i$) of size ($q$), where $2^q$-1 is less than the number of points in the elliptic curve group, and $i$ represents the IrisCode binary-block index.
- Assigning a distinctive point on the elliptic curve for each binary-block value by building a mapping table.
- Mapping each cancelable IrisCode binary-block ($m_i$) into a point over the elliptic curve based on its value and the mapping table for generating representative data points $P_1$ ($x_i$,$y_i$).
- Computing the initial key ($P_2 = Q_B * d_A$) using Eq. (11).
- Obtaining encrypted representative data points ($P_3$ ($x_i$,$y_i$) = $P_1 + P_2$) using Eq. (5).
- Based on the mapping table, obtaining the corresponding binary-block value for each data point, which is used to generate the protected IrisCode ($P_4$).
- Sharing of the protected IrisCode ($P_4$) and reader $A$ public encryption key ($Q_A$) to the centralized server $B$ for storage.

### *D. Authentication (Centralized Server B):*

In authentication, another iris image for each individual is collected. In the local iris reader, distinctive features are extracted for each query iris image, and a cancelable IrisCode is created. This is followed by the creation of the query protected IrisCode. After that, the query protected IrisCodes is transmitted from the local iris reader to the remote centralized server, where the enrolment protected IrisCodes and the received data are decrypted for further pattern matching.

Given the reader A public key ($Q_A$) and the elliptic curve domain parameters {$j$, $k$, $l$, $G$}, the individual's enrolment and query protected IrisCode ($P_4$) is decrypted in the remote centralized server as follows:

- Selecting a private key ($d_B$) randomly from the interval [1, $l$ – 1], and then generating a public key ($Q_B = d_B * G$) using Eq. (11).

- Obtaining the elliptic curve group.
- Constructing the mapping table.
- Computing the initial key ($P_2 = Q_A * d_B$) using Eq. (11).
- Partitioning the protected IrisCode ($P_4$) into binary-blocks ($N_i$), where $i$ is the binary-block number.
- According to its value and mapping table, each binary-block ($N_i$) is mapped to a point on the elliptic curve to generate an encrypted representative data point $P_3$ ($x_i$,$y_i$).
- Obtaining the original representative data points ($P_1$ ($x_i$, $y_i$) = $P_3 - P_2$), using Eq. (6).
- Recovering the individual's cancelable IrisCode ($P$) by obtaining the binary-block value that corresponds to each data point based on the mapping table.

The recovered individual's query cancelable IrisCode is verified against the enrolled version by computing the Hamming distance (HD) given in Eq. (13) between the two IrisCodes. The HD is the number of non-equivalent bits between the enrolled and query binary IrisCodes [4].

$$HD = \frac{1}{N}\sum_{j=1}^{N} A_j \oplus B_j \qquad (13)$$

where $A_j$ and $B_j$ are the $j^{th}$ bits of the query and enrolled binary IrisCodes, respectively, and $N$ is the number of bits in each IrisCode. If the score is smaller than the threshold, the user is authenticated, otherwise it is rejected.

Hence, input iris images for both enrolment and authentication are usually not aligned. Therefore, during pattern matching, the query IrisCode must be shifted circularly by left-right movement in order to analyze and compensate for all potential rotations in this case [21].

## V. Experimental Results and Discussions

In this part, detailed results are presented to describe the performance of the proposed iris recognition system. Moreover, a comparative study between the proposed and state-of-the-art iris protection schemes is presented.

The proposed system is evaluated on CASIA-IrisV3-Interval database. For CASIA-Iris-Interval, the iris images were captured by using a close-up near-infrared ray camera. It consists of eye images of 249 subjects and 395 classes. The iris images in CASIA-Iris-Interval are very clear and the iris texture can be easily seen with naked eye, which makes this subset well suited for studying the detailed iris texture and features [22]. In our experiments and evaluations, different snapshots of the right and left eye images of different classes have been considered.

In order to evaluate the performance of the proposed iris recognition system, two HD scores are measured, which are genuine HD, and imposter HD, and compared with the HD scores in the case of traditional unprotected iris recognition systems. For genuine HD, we acquire a reference iris image of each class which is matched with other images of the same class resulting in a total of 600 matching operations. In case of imposter HD, one template of a class is matched with other templates of other classes resulting in a total of 600 matching operations.

In the case of traditional unprotected iris recognition scenario, a kernel probability density estimate was computed for the genuine and imposter HD distributions as shown in Fig. 3. The mean and standard deviation values for the genuine HD distribution are 0.2747 and 0.0460, respectively, while these values for the imposter HD are 0.4754 and 0.0114, respectively.

In the case of the proposed iris recognition scenario, a kernel probability density estimate was computed for the genuine and imposter HD results as shown in Fig. 4. The mean and standard deviation values of the genuine HD distribution are 0.2747 and 0.0460, respectively, and the mean and standard deviation values of the imposter HD are 0.4754 and 0.0114, respectively. By comparing the simulation results given in Fig. 3 and Fig. 4, it can be seen that the performance in the two cases is the same.

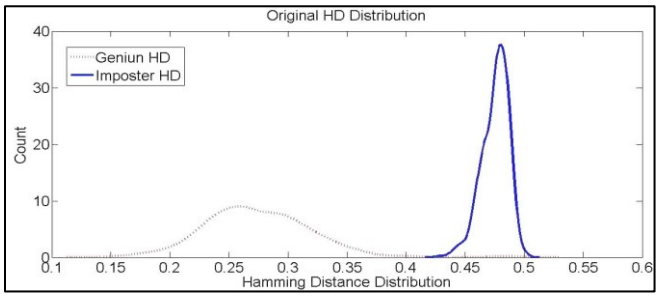



Fig. 3: HD plot for the traditional iris recognition system.

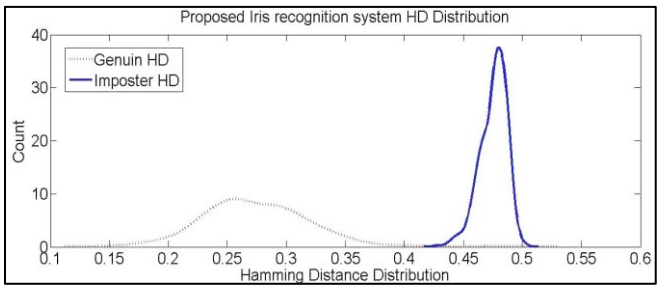
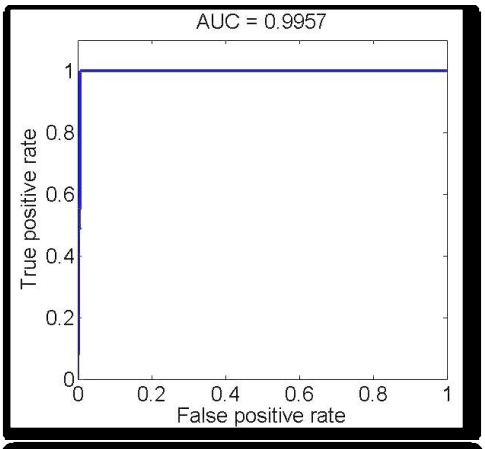



Fig. 4: HD plot for the proposed iris recognition system.

(a)




(b)

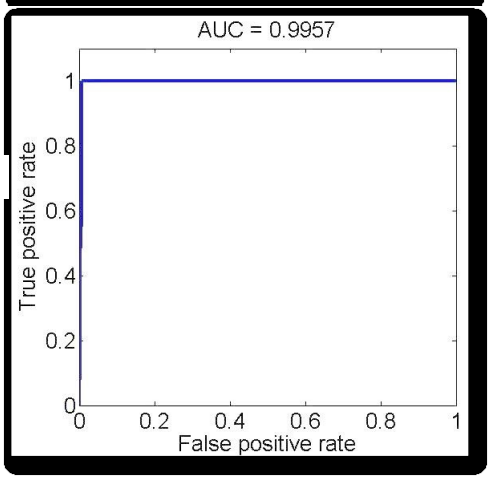



Fig. 5: ROC curves for (a) traditional iris recognition system, and (b) proposed system.

Furthermore, the receiver operating characteristic (ROC) curve and the area under ROC curve (AUC) are used for evaluating the performance of the proposed system [21]. The ROC curve is obtained by plotting the true positive rate (TPR) versus the false positive rate (FPR). The TPR represents the probability of rightly accepting a genuine IrisCode as illustrated in Eq. (14), while the FPR represents the probability of wrongly accepting an imposter IrisCode as a genuine iris pattern as given in Eq. (15) [33]. The equal error rate (EER) is the point at which the false negative rate (FNR) given in Eq. (16) and the FPR hold equality at a particular threshold value as shown in Eq. (17) [33]. The area under ROC Curve (AUC) can also be used as an indicator for the system accuracy. The higher the AUC value is, the better the system accuracy (1 being perfect; 0.5 no better than a random guess) [21]. Fig. 5 shows the ROC curves of the traditional iris recognition system and the proposed iris recognition system. It can be seen that the performance of the proposed system is similar to that of the original system.

$$\text{True Positive Rate (TPR)} = \frac{\text{Positives correctly classified}}{\text{Total positives}} \quad (14)$$

$$\text{False Positive Rate (FPR)} = \frac{\text{Negatives incorrectly classified}}{\text{Total negatives}} \quad (15)$$

$$\text{False Negative Rate (FNR)} = 1 - \text{TPR} \quad (16)$$

$$\text{Equal Error Rate (EER)} = \frac{\text{FPR}+\text{FNR}}{2} \quad (17)$$

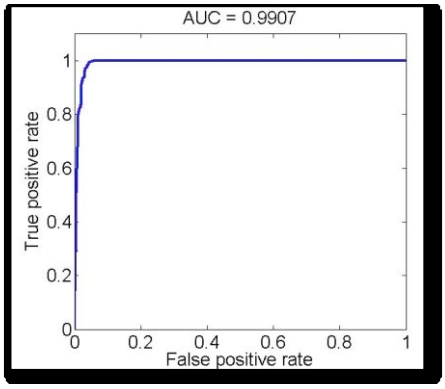
In addition, the performance of the proposed iris recognition system is analyzed in the presence of different types of noise. Fig. 6 (a) illustrates the ROC curve after adding a salt and pepper noise to the gray-scale iris images with a noise density of 0.05. Fig. 6 (b) shows the ROC curve after adding Poisson noise to the gray-scale iris images. Fig. 6 (c) shows the ROC curve after adding the zero-mean Gaussian white noise with a variance of 0.01 to the gray-scale iris images. Obviously, the influence of moderate noise on the proposed iris recognition system is acceptable.

To ensure the confidentiality of the proposed iris recognition system, the protected IrisCodes generated by the proposed system should be highly irrelevant to the original IrisCodes [5]. To measure the similarity between the original IrisCode and the protected IrisCode created from the same iris image, the normalized correlation coefficient (NCC) is computed. Then, a kernel probability density estimate is computed for the normalized correlation coefficient. As can be seen in Fig. 7, the normalized cross correlation between the original IrisCode and the protected version of the same iris is very close to zero with mean and standard deviation values of 0.0556 and 0.0078, respectively, which proves the complete difference between the protected IrisCode created by the proposed system and the original IrisCode.

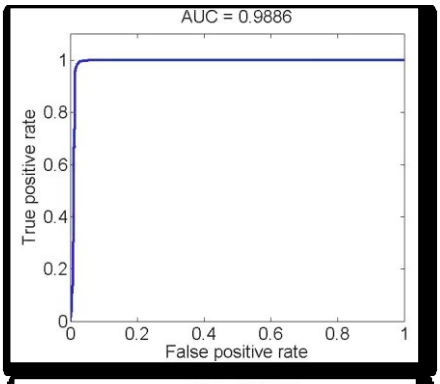
Furthermore, the unlinkability of the proposed system is investigated by measuring the cross-matching HD between an individual's original IrisCode obtained from other less secure applications and the enrolment protected IrisCode database and comparing it with both genuine HD and imposter HD [24].

As can be seen in Fig. 8, the cross-matching HD distribution looks like an imposter distribution, but with smaller standard deviation (very much sharper). This means that if an attacker could break into the enrolment protected IrisCodes database in the database server, and try to perform a cross-matching with different IrisCodes obtained from other common or less secure applications, he/she could not determine whether this matching is genuine or imposter according to the matching result. Therefore, he/she could not determine whether the two IrisCodes are for the same user or not.

(a)



(b)




(c)

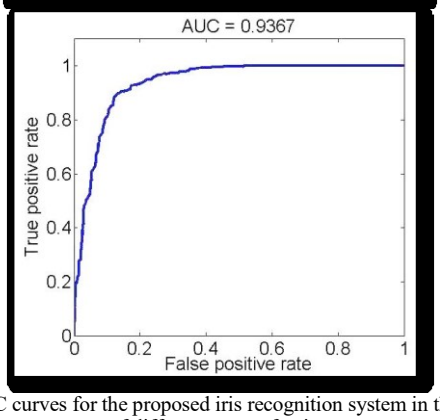



Fig. 6: ROC curves for the proposed iris recognition system in the presence of different types of noise.
(a) Salt and proper noise. (b) Poisson noise. (c) Gaussian white noise.

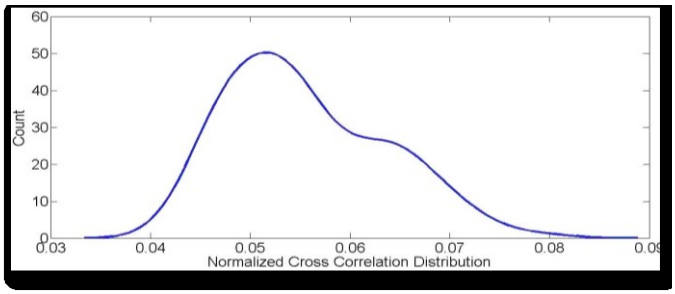



Fig. 7: NCC distribution plot between the original IrisCodes and protected versions of the same iris image.

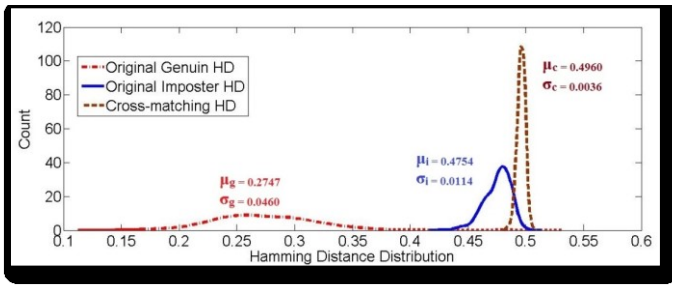



Fig. 8: Genuine HD and imposter HD versus cross-matching HD.

Finally, in our experiments, we compare the proposed iris recognition system with some state-of-the-art iris biometric protection systems using the same database (CASIA-Iris-Interval). The results summarized in Table 1 illustrate a superior performance for the proposed iris recognition system compared to those of the other considered systems.

TABLE I. COMPARISON WITH THE STATE-OF-THE-ART TECHNIQUES

| Technique (Year) | Performance (EER %) |
|---|---|
| Hyperelliptic Curve Cryptography (2020) [23] | 2.5 |
| Fully homomorphic encryption (2020) [15] | 1.38 |
| Local Ranking (2018) [24] | 1.32 |
| Modified Logistic Map (2018) [25] | 1.17 |
| randomized response technique (2018) [26] | 1.03 |
| Fully homomorphic encryption (2021) [27] | 0.95 |
| Double Random Phase Encoding (2018) [28] | 0.63 |
| Random Projection (2018) [29] | 0.58 |
| Binary Confidence Matrix (2021) [30] | 0.51 |
| Random Projection and Double Random Phase Encoding (2021) [31] | 0.46 |
| Salting Technique (2020) [11] | 0.43 |
| Comb Filtering (2020) [32] | 0.38 |
| **Proposed iris recognition system** | **0.37** |

## VI. CONCLUSION

In this paper, we proposed a novel hybrid iris template protection system that combines both feature transformation and a biometric cryptosystem. In the local iris reader, a binary IrisCode is extracted for each iris image and blended pixel-wise with a user-specific binary synthetic pattern using XOR operation for creating a cancelable IrisCode. Then, the cancelable IrisCode is encrypted employing a specially-designed elliptic curve cryptosystem for generating a protected IrisCode that can be sent more securely to the centralized server for storage and further pattern matching. Experimental analysis for the proposed iris recognition system in terms of performance and security on CASIA-IrisV3 database was conducted and compared with that of the traditional iris recognition system. It has been proven that the recognition accuracy of the proposed iris recognition system is not affected in comparison with the original counterpart, while providing a robust protection against several major privacy/security attacks. In particular, the proposed iris recognition system guarantees revocability, whereas a compromised protected IrisCode can be cancelled and reissued. This preserves privacy, whereas it is computationally difficult for recovering the original IrisCode from a protected version. It has a good immunity against the cross-matching problem. On the other hand, the protected IrisCodes can be stored and transmitted from local iris readers to the remote centralized server and between multiple servers in the multi-server environment more, securely. Additionally, the proposed system was evaluated in the presence of different types of noise with moderate levels and it is proven that noise effect on the proposed iris recognition system is acceptable. Finally, a comparative study between the proposed system and the other state-of-the-art systems was introduced. It is proved that the proposed system is superior over other existing iris biometric protection systems tested on the same database.

## REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transaction on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-20, 2004.

[2] Israa Majeed Alsaadi, "Study On Most Popular Behavioral Biometrics, Advantages, Disadvantages And Recent Applications : A Review", International Journal of Scientific and Technology Research, Vol. 10, No.1, January 2021.

[3] Muzhir Shaban Al-Ani and Salwa Mohammed Nejrs, "Efficient Biometric Iris Recognition Based on Iris Localization Approach", UHD Journal of Science and Technology, Vol. 3, No. 2, Jul 2019.

[4] J. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Trans. Pattern Anal. Mach. Intell., Vol. 15, No. 11, pp. 1148-1161, November 1993.

[5] Tuy Nguyen and Hanho Lee, "High-Secure Fingerprint Authentication System using Ring-LWE Cryptography", IEEE Access, Vol. 7, pp. 23379-23387, 2019.

[6] Vishal M. Patel, Nalini K. Ratha, and Rama Chellappa, "Cancelable Biometrics", IEEE Signal Processing Magazine, Vol. 32, No. 5, pp. 54-65, September 2015.

[7] Mahesh Kumar Morampudi , Munaga V.N.K. Prasad a, Mridula Verma and U.S.N. Raju, "Secure and verifiable iris authentication system using fully homomorphic encryption, Computers and Electrical Engineering 89, 2021

[8] A. K. Jain, K. Nandakumar, A. Nagar. Biometric Template Security. EURASIP Journal on Advances in Signal Processing, 2008.

[9] Randa F. Soliman, Mohamed Amin and Fathi E. Abd El-Samie, "A Modified Cancelable Biometrics Scheme Using Random Projection", Springer-Verlag GmbH Germany, Annals of Data Science, August 2018.

[10] S. Umer, B. C. Dhara, and B. Chanda, "A Novel Cancelable Iris Recognition System Based on Feature Learning Techniques", Information Sciences 406–407, 102-118, 2017.

[11] Ahmed A. Asaker, Zeinab F. Elsharkawy, Sabry Nassar, Nabil Ayad, O. Zahran, and Fathi E. Abd El-samie, "A Novel Cancelable Iris Template Generation Based on Salting Approach", Multimedia Tools and Applications, 2020.

[12] F. Han, J. Hu, X. Yu and Y. Wang, "Fingerprint image encryption via multi-scroll chaotic attractors", Applied Mathematics and Computation 185, Elsevier, pp. 931-939, 2007.

[13] G. Mehta, M. K. Dutta, J. Karasek and P. S. Kim, "An efficient and lossless fingerprint encryption algorithm using Henon Map & Arnold Transformation", International Conference on Control Communication and Computing, IEEE, pp. 485-48, 2013.

[14] D. M. S. Bandara, Yunqi Lei, Ye Luo "Fingerprint Image Encryption Using a 2D Chaotic Map and Elliptic Curve Cryptography", International Journal of Computer and Information Engineering, Vol:12, No:10, 2018.

[15] Mahesh Kumar Morampudi, Munaga V. N. K. Prasad, and U. S. N. Raju, "Privacy-Preserving Iris Authentication Using Fully Homomorphic Encryption", Springer – Multimedia Tools and Applications, 79, pp. 19215–19237, 2020.

[16] Deepak Aeloor, and Amrita A. Manjrekar, "Securing Biometric Data with Visual Cryptography and Steganography", International Symposium, SSCC 2013 Mysore, India, Proceedings, Springer-Verlag Berlin Heidelberg, August 2013.

[17] Oluwakemi Christiana Abikoye, Umar Abdulraheem Ojo, Joseph Bamidele Awotunde and Roseline Oluwaseun Ogundokun "A safe and secured iris template using steganography and cryptography, Multimedia Tools and Applications, August 2020.

[18] D. Hankerson, A. Menezes, and S. Vanstone, "Guide to Elliptic Curve Cryptography", Springer, New York, 2004.

[19] Zeinab Vahdati, Sharifah Yasin, Ali Ghasempour and Mohammad Salehi, "Comparison of ECC and RSA Algorithms in IOT Devices", Journal of Theoretical and Applied Information Technology, Vol.97. No 16, August 2019.

[20] Mohamed Essam, M. Abd Elnaby, Magdi Fikri, and Fathi E. Abd ElSamie, "A Fast Accurate Algorithm for Iris Localization Using a Coarse-to-Fine Approach", IEEE Japan-Egypt Conference on Electronics, Communications and Computer, Alexandria, Egypt, 6-9 March 2012.

[21] Randa F. Soliman, Mohamed Amin, and Fathi E. Abd El-Samie, "On Mixing Iris-Codes", Springer Nature Switzerland AG, 2019.

[22] CASIA database v3-interval (http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp).

[23] Vani Rajasekar ,1 J. Premalatha,2 and K. Sathya "Enhanced Biometric Recognition for Secure Authentication Using Iris Preprocessing and Hyperelliptic Curve Cryptography" Wireless Communications and Mobile Computing, Article ID 8841021, 2020.

[24] Dongdong Zhao, Shu Fang, Jianwen Xiang, Jing Tian, and Shengwu Xiong, "Iris Template Protection Based on Local Ranking", Hindawi Security and Communication Networks, Article ID 4519548, February 2018.

[25] Randa Soliman, Noha Ramadan, Said El-Khamy, and Fathi E. Abd El-Samie, "Efficient Cancelable Iris Recognition Scheme Based on Modified Logistic Map", The National Academy of Sciences, India, September 2018.

[26] Zhao D, Hu X, Tian J, Xiong S and Xiang J, "Iris template protection based on randomized response technique and aggregated block information", IEEE 29Th International Symposium on Software Reliability Engineering, ISSRE, IEEE, pp 248–258, 2018.

[27] Mahesh Kumar Morampudi, Munaga V.N.K. Prasad, Mridula Verma and U.S.N. Raju, "Secure and verifiable iris authentication system using fully homomorphic encryption", Computers and Electrical Engineering, Vol. 89, 2021.

[28] Randa Soliman, Ghada El Banby, Mohamed Elsheikh, and Fathi E. Abd El-Samie, "Double Random Phase Encoding for Cancelable Face and Iris Recognition", Applied Optics Vol. 57, No. 35, December 2018.

[29] Randa F. Soliman, Mohamed Amin, and Fathi E. Abd El-Samie, "A Modified Cancelable Biometrics Scheme Using Random Projection", Springer-Verlag GmbH Germany, Annals of Data Science, August 2018.

[30] Chai, T.-Y.; Goi, B.-M. and Yap, W.-S, "Towards Better Performance for Protected Iris Biometric System with Confidence Matrix", Symmetry, Vol. 13, No. 910, 2021.

[31] Vani Rajasekar, J. Premalatha and K. Sathya, " Cancelable Iris template for secure authentication based on random projection and double random phase encoding", Vol. 14, pp. 747–762, Peer-to-Peer Networking and Applications , January 2021.

[32] Randa F. Soliman, Mohamed Amin, and Fathi E. Abd El-Samie, "Cancelable Iris Recognition System Based on Comb Filter", Multimedia Tools and Applications, Vol. 79, pp. 2521-2541, January 2020.

[33] Selvapandian A, Manivannan K (2018) Fusion Based Glioma Brain Tumor Detection and Segmentation Using ANFIS Classification, Computer Methods and Programs in Biomedicine 166, pp. 33–38.