Optical and Quantum Electronics (2023) 55:970
https://doi.org/10.1007/s11082-023-04840-7

A robust cancellable face and palmprint recognition system based on 3D optical chaos-DNA cryptosystem

Haidy A. Ali Eldawy[1] · Walid El-Shafai[1,2] · Ezz El-Din Hemdan[3] · Ghada M. El-Banby[4] · Fathi E. Abd El-Samie[1]

Received: 1 February 2023 / Accepted: 7 April 2023 / Published online: 2 September 2023

Abstract

Several cancelable biometric procedures have been developed to preserve personal data security. This research presents a cancelable biometric authentication mechanism to ensure personal data security, while maintaining the biometric templates secure from hackers. Therefore, our major approach is to provide a new authentication system based on 3D chaotic maps, Piecewise Linear Chaotic Map (PWLCM), logistic map, and Deoxyribonucleic Acid (DNA) sequencing theory. The approach is based on confusion as well as a diffusion. Firstly, a 3D chaotic map is made up to allow 3D chaos creation, chaos histogram equalization, row rotation, column rotation, and XOR operation. Secondly, the PWLCM and the Logistic Map are used for generating the main values required to make use of the DNA theory to generate the key image. Thirdly, DNA theory is applied as a second encryption algorithm on the output of the 3D chaotic algorithm. Fourthly, the intermediate image is decoded, rotated 90 degrees anticlockwise, and used in the following step in the DNA encoding process. Finally, step 3 is repeated on columns to acquire the final encrypted image. The proposed framework hides all discriminative properties of biometric templates, resulting in a fully unspecified biometric pattern. Various face, as well as palmprint biometric datasets, have been examined and evaluated. Various evaluation factors are employed to examine the efficiency of the recommended cryptography algorithm including Area under the Receiver Operating Characteristic (AROC), False Acceptance Rate (FAR), histogram analysis, Histogram Deviation (D_H), correlation coefficient, Structural Similarity Index Metric (SSIM), and Peak Signal-to-Noise Ratio (PSNR). The computational results prove that the proposed cryptosystem is trustworthy. A comparative study of the recommended approach with various strategies is also provided. Simulation studies illustrate that the suggested approach produces an average AROC of approximately 1, an average FAR of 6.2×10^{-3}, an average D_H of 0.8755, and finally, an average PSNR of 8.2061.

Keywords Cancelable biometrics · 3D Chaos maps · PWLCM · Logistic map · DNA theory

Abbreviations

DNA	Deoxyribonucleic acid
PWLCM	Piecewise linear chaotic map

Extended author information available on the last page of the article

EER	Equal error rate
AROC	A receiver operating characteristic curve
FAR	False acceptance rate
D_H	Histogram deviation
PINs	Personal identification numbers
DSP	Digital signal processing
DRPE	Double random phase encoding algorithm
RPM 1	Random phase mask
RPM 2	Random phase mask
FRFT	Fractional Fourier transform
AF	"À Trous" filtering
AT	À Trous transform algorithm
A	Adenine
T	Thymine
C	Cytosine
G	Guanine
XOR	Exclusive OR
MD5	Message-digest mechanism 5
PSNR	Peak signal to noise ratio
SSIM	Structural similarity index metric
TPF	True positive rate
FPF	False positive rate
PTD	Probability of true distribution
PFD	Probability of false distribution
Var(G)	Variance (genuine correlation)
Var(F)	Variance (fake correlation)

List of Symbols

x_n	The initial value of the chaos map $0 < x_n < 1$
y_n	The initial value of chaos map $0 < y_n < 1$
z_n	The initial value of chaos map $0 < z_n < 1$
μ	Constant parameter = 4
γ	Control parameter $3.53 < \gamma < 3.81$
β	Control parameter $0 < \beta < 0.022$
α	Control parameter $0 < \alpha < 0.015$
N_2, N_4, N_6	Random numbers > 10,000
M	Number of columns
N	Number of rows
p	Control parameter $p \in (0, 0.5)$
d_1, d_2, d_3, d_4	Each of them represents a single byte
pixel	The pixel value of the key image
Rule	One of the 8 rules of DNA
process	One of DNA operations $(XOR, +, -)$
$C_{i,j}$	The correlation coefficient
i, j	The grayscale values of two neighboring pixels in the image
E	The expectation
$E(i)$	Mean of i
$E(j)$	Mean of j

$\sqrt{D(i)}$	Standard deviation of i
$\sqrt{D(j)}$	Standard deviation of j
μ_I	The average of an input image (I)
μ_T	The average of the encrypted image
σ_I^2	The variance of the input image
σ_T^2	The variance of the encrypted image
σ_{IT}	Signifies the covariance between the input and encrypted images
S_1 and S_2	Small values
q_i	The absolute difference between the pure and ciphered images' estimated histograms at a gray level i
n	The number of bits/pixel
O	The reference image
T	The encrypted image

1 Introduction

Biometric recognition has advanced rapidly, and it is now virtually and universally utilized. Biometric recognition approaches identify and check unique characteristics precisely, quickly, and properly to govern the access process in specialized applications (Arqub and Abo-Hammour 2014; Soliman et al. 2021a; Abo-Hammour et al. 2013; Algarni et al. 2020a; Ibrahim et al. 2020a). Therefore, restricting access and blocking attackers from damaging or identifying the templates are critical.

The two types of biometrics utilized by humans are physical and logical biometrics (Alarifi et al. 2020; Ibrahim et al. 2020b). The face, iris, retina, palmprint, and fingerprint have specific physical characteristics, but logical or behavioral characteristics, such as voice, signature, keystroke patterns, and walking style, are measured by the behavior of the body and its response to various conditions.

All of these biometric represent aspects or characteristics of our human body, which are used to ensure that no hackers may get admission to manage the services provided (El-Shafai et al. 2023a, 2022a; Elazm et al. 2023). Passwords have historically been used to protect the key for encryption from being stolen or hacked. Most people employ the same passwords across many applications and never change them as the utilization of different lengthy passwords is difficult. If an attacker attempts to get access to the database and a portion of the secret password is stolen, the other services may be at risk (El-Shafai et al. 2021a).

Organizations continuously look forward to preserve their data safely and improve the network service to prevent unauthorized access. Authentication and identification are performed to ensure that the permitted user can only access a secure and reliable location. Traditional encryption mechanisms, such as personal identification numbers (PINs) as well as passwords, have been used for years. For increased security, magnetic cards and PINs have been implemented (Faragallah et al. 2020; El-Shafai et al. 2023b; Hassan et al. 2022).

Some problems of the conventional methods arise from the fact that they recognize some characteristics related to the owner rather than the owner himself. The system can simply admit or control any outsider if these tokens are stolen or destroyed. There is a new methodology in verification strategies that uses biometrics in many applications, such as government services, commercial applications, and forensic evidence applications that rely

on human being supervision to identify biometrics (Nassar et al. 2023; Almomani et al. 2023).

Biometric templates should be guarded when an application requires a high degree of secrecy. This in turn increases the accuracy and secrecy of identifying people (Elazm et al. 2023; El-Shafai et al. 2022a). As illustrated in Fig. 1, the biometric system is divided into four levels: image sensor, processing unit, database, and output device (Ahmad et al. 2022). In the enrollment stage, a biometric system is learned to recognize a specific client. The client initially presents an identity, like an identity card. The biometric (e.g., fingers, hand, face, or iris) is then presented to the input (sensor) device. The characteristics or features are obtained and saved as a reference pattern for the next examinations. After enrollment, the next step is to confirm that the client is the person who enrolled. After the user supplies whatever identity he or she registered with, the captured biometric is presented, and a new template is generated. The system next verifies the new biometric pattern to the individual's reference pattern, which was saved upon enrolment, to see if the new and stored patterns are identical.

Biometric-based authentication systems have provided powerful security characteristics, particularly in telemedicine applications, to protect personal data against offline password threats (Ahmad et al. 2022). Even though biometrics solve numerous security problems, hackers have discovered strategies to attack biometric authentication processes and databases containing biometric information. Biometrics are difficult to secure since the hashing strategy used to safeguard passwords does not operate with biometric information. As a result, any business that uses biometrics to authenticate its members must guarantee that their biometric information is appropriately protected (Salama et al. 2022; Almomani et al. 2022a). Biometric encryption approaches provide excellent confidentiality, security, and uniqueness for permitted persons. Encryption keys boost the security of biometric cryptosystems. Original biometric characteristics are not stored directly in the server with these cryptosystems but are first processed and turned into distorted, transformed templates (El-Shafai et al. 2022b, 2022c).

Cancelable biometrics (El-Shafai et al. 2022d) play a vital role in biometric security by modifying the basic biometric into a new irreversible domain. Instead of saving the basic

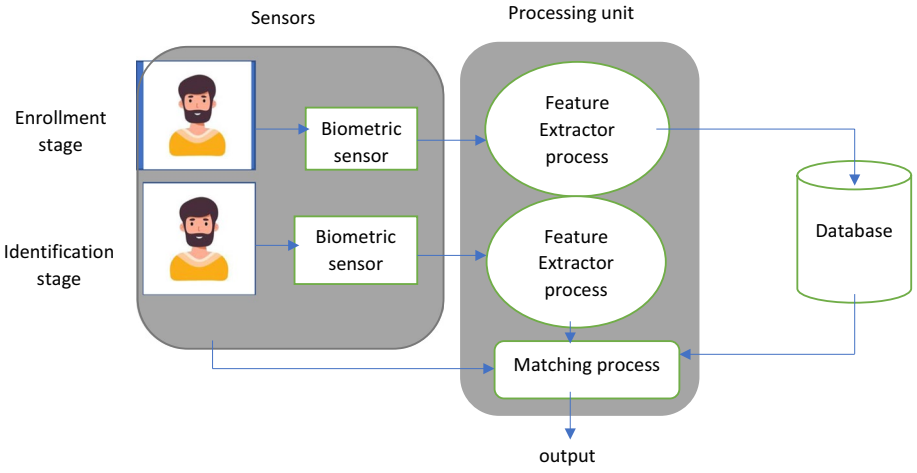


Fig. 1 Biometric system

characteristics directly into the server, cancelable biometrics are first generating by deform the biometric characteristics using various modification functions as shown in Fig. 2.

These cancelable templates have four significant properties (Ibrahim et al. 2020a): (i) diversity, (ii) non-invertiblity, (iii) revocablity, (iv) high performance. *Diversity* typically indicates that no two users should be assigned the same cancelable biometric pattern. *Non-invertiblity* indicates that original biometric characteristics cannot be retrieved using these cancelable biometric patterns. *Revocablity* indicates that if an individual's cancelable biometric pattern is stolen, a new cancelable pattern will be assigned to him/her without affecting the actual biometric identity. Finally, the high performance property specifies that the recognition accuracy of a cancelable biometric system should be as high as that of a standard biometric system. If one's allocated cancelable biometric template is hacked, a new template will be assigned to him by deleting the prior one, as is the case with ATM passwords.

The motivation behind the development of this work is to address the security and privacy concerns associated with biometric recognition systems. Biometric recognition systems are widely used for identification and authentication purposes, but they have a vulnerability to attacks such as spoofing and replay attacks, which can compromise the security of the system. The proposed system uses 3D optical chaos and DNA encryption to enhance the security of biometric recognition systems. The system is cancellable, which means that the biometric data can be modified without affecting the recognition performance, thus protecting the privacy of the users. The use of 3D optical chaos and DNA encryption ensures that the biometric data cannot be easily replicated or tampered. Overall, the motivation behind the development of this system is to provide a more secure and privacy-preserving biometric recognition system that is robust against various attacks and can be used in a wide range of applications, including access control, surveillance, and forensics.

In this research work, a new authentication system built on 3D chaotic maps, Piecewise Linear Chaotic Map (PWLCM), Logistic Map, and finally, Deoxyribonucleic acid (DNA) sequence theory is suggested. First, a 3D chaotic map is made up of the following processes: (1) 3D chaos creation, (2) chaos histogram equalization, (3) row rotation, (4) column rotation, and (5) XOR process. Secondly, PWLCM and Logistic Map are used for generating all of the main values required by DNA theory to generate the key image. Thirdly, DNA theory is applied as a second encryption algorithm to the output of the 3D chaotic algorithm. Fourthly, the intermediate image is decoded and used in the following step in the DNA encoding process. Finally, step 3 is repeated on columns to acquire the final encrypted image.

The rest of this paper is organized as follows: Sect. 2 includes some past works. Section 3 presents the suggested cancelable biometric authentication architecture. Section 4 gives an

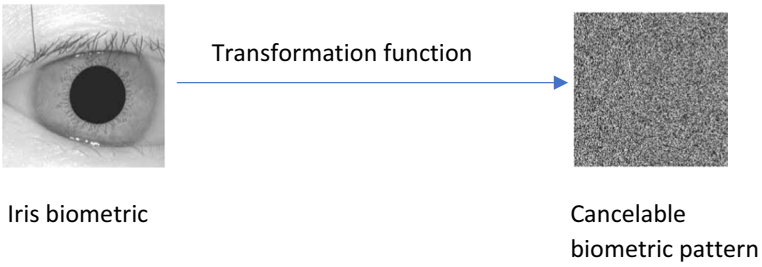


Fig. 2 Example of a cancelable biometric template generated by a transformation function

explanation of the assessment metrics that were used. Section 5 summarizes the computer simulation results and performance evaluations. Section 6 summarizes the final remarks.

2 Related work

Cancellable biometric methodologies are utilized in the verification system to provide distorted versions of biometrics (El-Hameed et al. 2022; Helmy et al. 2022a). If required, authorized features can be removed or replaced in hacking cases. The cancelable biometric strategy is devoted to preserving the highest precision level of the saved biometrics to improve user privacy.

Mohamed et al. (2022) developed an iris recognition authorization strategy. It is dependent on a mix of non-invertible transformations with encryption to disguise the iris template. They achieved a 99.9% recognition rate. Various security strategies for face authentication are provided in Ayoup et al. 2022a. They employed a variety of procedures to extract geometric characteristics. Another proposed approach is based on creating concealed templates after using Gabor filters. This approach presented two types of chaotic maps: logistic and modified logistic maps. With the chaotic logistic map, this methodology achieved 99.08% accuracy and 1.175% EER. Also, the genetic (GA) encryption algorithm (Arqub and Abo-Hammour 2014; Abo-Hammour et al. 2013) can be used to attain biometric image cancelability (Alshammri et al. 2022). The GA (Abo-Hammour et al. 2014; Abu Arqub et al. 2012) method chooses the appropriate secret key with the best length to increase encryption. The researchers of Soliman et al. (2018a) described a face biometric authentication method based on Double Random Phase Encoding (DRPE) algorithm. The bio-convolving approach was used to safeguard the safety and privacy of the individuals' faces. In addition, the same researchers (Soliman et al. 2018b) proposed a multi-biometric authentication architecture.

It is focused on combining multiple biometric pattern characteristics. A one-way iris pattern is created using the Fractional Fourier Transform (FRFT)-based approach. The cryptographic keys RPM1 and RPM 2 are employed in the described cancelable biometric strategy. RPM1 is the first cover for the left iris characteristic vector, and RPM2 is for the right iris feature pattern of the individual. The implemented strategy achieved an EER of 0.63% and an efficiency of 99.75%.

El-Hameed et al. (2022) proposed a cancelable geometric methodology for fingerprint recognition. It works by deducing feature pixels and then using polar and Cartesian coordinate processes to generate cancelable fingerprint characteristics. This method maintains cancelability while achieving high privacy and security accuracy. The researchers of Helmy et al. (2022a) presented a fingerprint recognition security technique based on numerous spiral curves and fuzzy principles. The equal error rate (EER) of this method is 1.17%.

The researchers of Hammad et al. (2019) used a 2-dimensional Gabor filter to extract features of a palmprint, followed by a two-dimensional palm Hash algorithm to mask the features and construct the cancelable palmprint vector. Leng et al. (2014), a method for multi-biometric characteristics is used to construct cancelable biometrics in order to obtain high privacy and secrecy depending on different feature fusion degrees. Qiu et al. (2019), a new palmprint pattern protection system is developed based on random comparison and noise data. An anisotropic filter (AF) is used to collect the palmprint's orientation information. The palmprint's orientation characteristic is then assessed using a chaotic matrix, resulting in a protected and cancelable palmprint pattern. Furthermore, as the last cancelable palmprint pattern, noise data having independent and identically dispersed distribution

is included to improve the template's privacy security. In addition, a method for producing cancelable palmprint patterns was developed using coupled nonlinear dynamic filters and various orientation palm codes (Qiu et al. 2019). In conclusion, cancelable biometric formats can be created using a variety of techniques, including random projection (Soliman et al. 2021b; Asaker et al. 2021; El-Gazar et al. 2022), hashing function (YYYY xxxx), and salting (Almomani et al. 2022b), but they all have the same basic goal of transforming the original biometric pattern into a distorted version, attempting to make it complicated for an enemy to recover the original template from the distorted one. Cancellable template models have been used to biometric characteristics from numerous attributes, such as the face and palmprint, to create several safe biometric architectures.

3 Proposed cancelable biometric authentication framework

In this session, we proposed a Cancellable biometric methodology based on two hybrid encryption techniques: pixel rotation with XOR-based encryption technique using 3D chaos and DNA theory as a second encryption algorithm to the output of 3D chaotic algorithm to provide distorted versions of biometrics. The 3D chaotic system is utilized for position permutation and the value transformation approach. In the position permutation strategy, the pixel position is permuted without affecting the pixel value of the actual image, but in the value transformation strategy, the pixel value is changed by another pixel value without modifying the position as in Helmy et al. (2022b). Figure 3 depicts the flowchart of the recommended cancelable biometric authentication architecture. The suggested framework's major stages are illustrated and summarised as follows:

(a) 3D Chaos generation.
(b) Chaos histogram equalization.
(c) Row rotation.
(d) Column rotation.
(e) XOR operation.
(f) Piecewise liner chaotic map and logistic map.
(g) MD5 hash.
(h) Deoxyribonucleic acid string (DNA).
(i) DNA cryptosystem.

3.1 3D chaos generation system

The logistic chaos map is used to generate 3D chaos in the proposed chaotic-based cryptosystem. The logistic map is one of the most basic and well-known chaotic maps, based on changing the placements of pixels in images and adjusting gray-level pixel values. An equation that describes the nonlinear logistic map chaos generation system is as follows:

$$x_{n+1} = \mu x_n \left(1 - x_n\right), \tag{1}$$

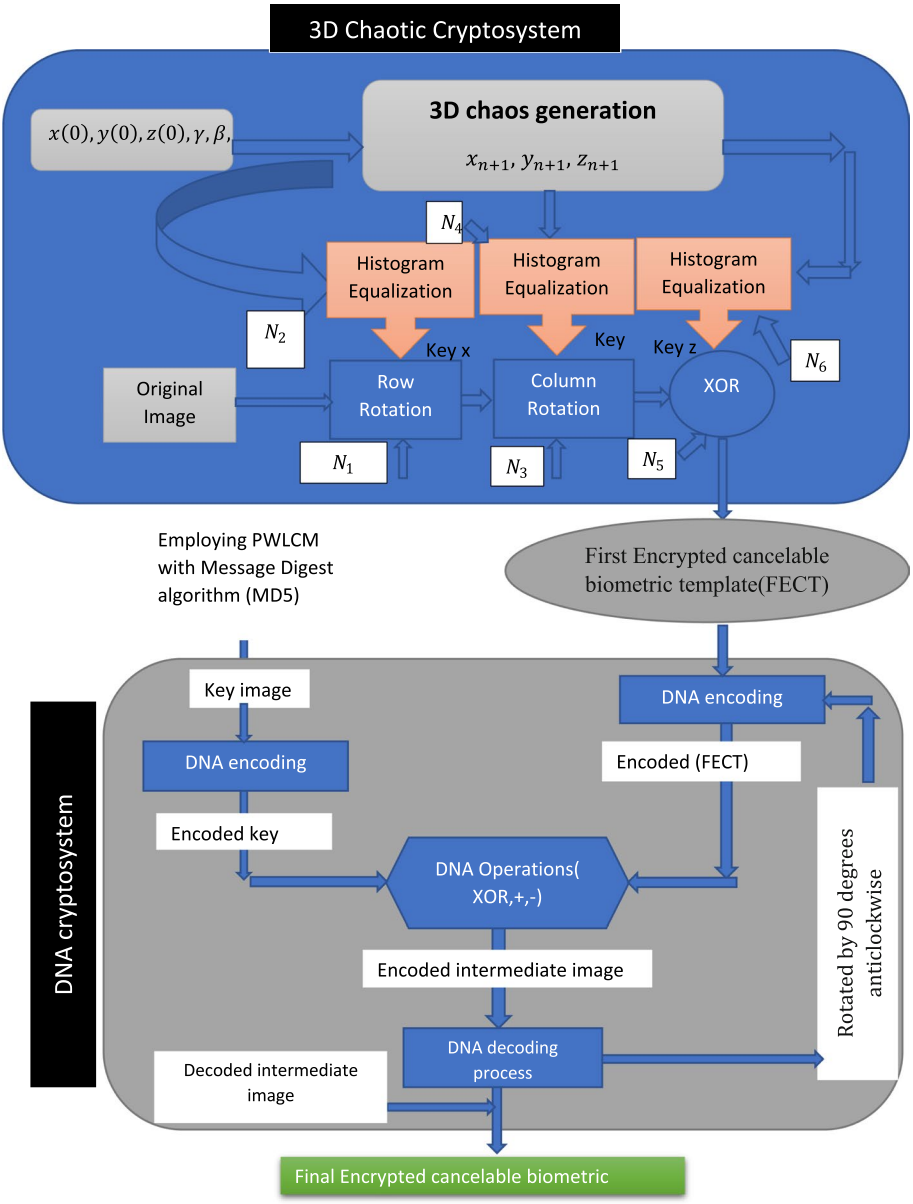


Fig. 3 The proposed cancelable biometric system

where $0 < x_n < 1$ and $\mu = 4$ is the condition to do this formula chaotic. The 3D logistic map chaos generation expressions are formulated as in Helmy et al. (2022b) and Ayoup et al. (2022):

$$x_{n+1} = \gamma x_n(1 - x_n) + \beta y_n^2 x_n + \alpha z_n^3, \tag{2}$$

$$y_{n+1} = \gamma y_n(1 - y_n) + \beta z_n^2 y_n + \alpha x_n^3, \tag{3}$$

$$z_{n+1} = \gamma z_n(1 - z_n) + \beta x_n^2 z_n + \alpha y_n^2, \tag{4}$$

where $3.53 < \gamma < 3.81, 0 < \beta < 0.022, 0 < \alpha < 0.015$, and the preliminary values of x, y, z in between 0 and 1. These parameters make the 3D logistic map more complicated and secure than 1D or 2D logistic maps.

3.2 Chaos histogram equalization

The histogram of X, Y, and Z has non-uniform distribution, as illustrated in Fig. 4a–c. The histogram should be equalized to raise the degree of security. The following equations are used to equalize the histogram for a grey image of *MXN* dimensions:

$$x = \left(integer\left(x \times N_2\right)\right) mod N, \tag{5}$$

$$y = \left(integer\left(y \times N_4\right)\right) mod M, \tag{6}$$

$$z = \left(integer\left(z \times N_6\right)\right) mod 256, \tag{7}$$

where N_2, N_4, N_6 are huge random numbers more than 10,000. We may also assume $N_2, N_4,$ andN_6 to be equal for the simplicity. Using $N_2 = N_4 = N_6 = 100,000, M = 256, N = 256$, Fig. 4d–f depict the equalized histogram.

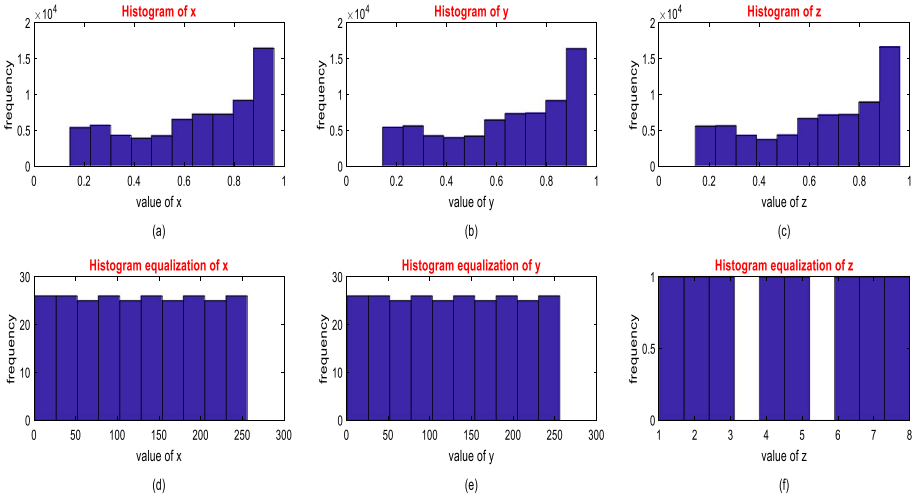


Fig. 4 Histogram Equalization of the 3D chaos system

3.2.1 Row rotation

Depending on the value of chaos x from Eq. (5), Helmy et al. (2022b) proposed a novel strategy for row rotation that would aid us in image pixel permutation. When the chaos value is even, the rows must be rotated left; when the chaos value is odd, the rows must be rotated right, as shown in Fig. 5.

3.2.2 Column rotation

Column rotation and row rotation have a lot in common. The value of chaos Y determines a column rotation in Eq. (6). When the chaos is an even number, we must rotate the columns up, and when the chaos is an odd value, we must rotate the columns down (Helmy et al. 2022b), as shown in Fig. 6.

3.2.3 XOR operation

The XOR operation is the final stage in this encryption procedure. First, the pixel value is changed to a new value via the XOR operation, which cannot be reversed without having the chaos key. Next, we XOR the chaos and row-column shifted the image to produce the encrypted image.

3.2.4 Piecewise liner chaotic map and logistic map

The Piecewise Linear Chaotic Map (PWLCM) and Logistic Map procedures are utilized to generate all of the parameters required by the approach. PWLCM offers various advantages, according to Ayoup et al. (2022), Eldesouky et al. (2022) and Faragallah et al. (2022), such as its representation simplicity and execution efficiency. It is utilized to create the key image, whereas the logistic map is used to govern the processes (operations) or DNA standards (rules) chosen for encoding and to reconstruct every row of the basic image. Equation (8) defines the PWLCM, whereas Eq. (9) represents the logistic map.

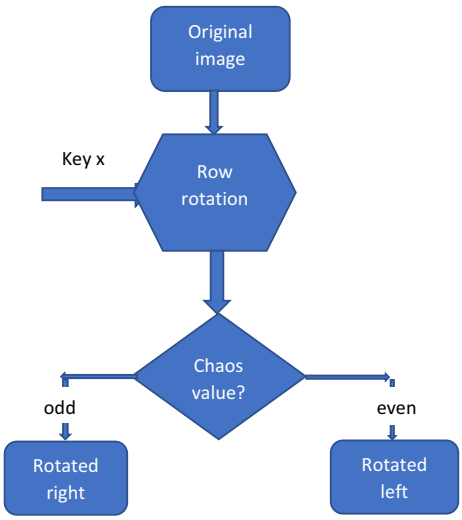


Fig. 5 Row rotation process

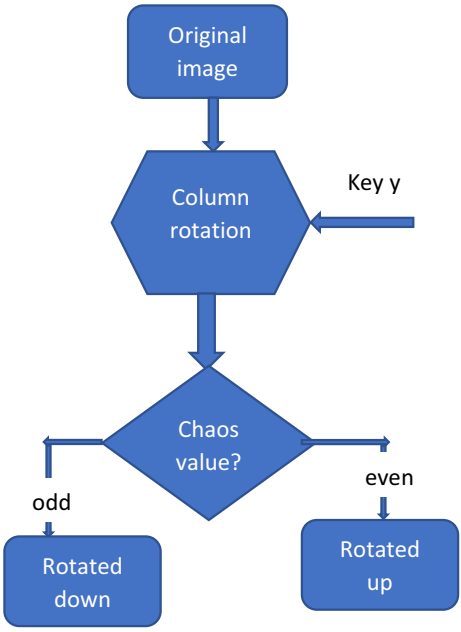


Fig. 6 Column rotation process

$$X_{n+1} = F_p(X_n) = \begin{cases} X_n/p & 0 < X_n < p \\ (X_n - p)/(0.5 - p) & p \le X_n < 0.5 \\ F_p(1 - X_n) & 0.5 \le X_n < 1 \end{cases}, \tag{8}$$

where $X_n \in (0, 1)$ and $p \in (0, 0.5)$. Assume that $p = 0.25678900$.

$$X_{n+1} = \mu X_n(1 - X_n), \tag{9}$$

where $X_n \in (0, 1)$ and $\mu \in (0, 4]$. Assign the value of μ=3.99999999 (Ayoup et al. 2022b).

3.2.5 MD5 hash

MD5 (Message-Digest Mechanism 5) is a widely used encryption algorithm that generates a 128-bit hash value from the data input, which is generally a 32-digit hexadecimal integer (El-Shafai et al. 2022e). The initial values of chaos maps are determined by the MD5 encryption estimated real value, as measured by Eq. (10):

$$X_0 = \mathrm{mod}(d_1 \oplus d_2 \oplus d_3 \oplus d_4, 256)/255. \tag{10}$$

The chaotic map's beginning number is X_0, and the estimated number of X_0 can either be 0 or 1 with a certain probability; if this happens, discard it and use Eq. (10) to get another. The parameters d_1, d_2, d_3, d_4 are calculated from the fundamental image's MD5 hashing result. The hash estimated value of the basic image is divided into four 32-bit bits. d_1, d_2, d_3, d_4 are the first 32 bits, each of which represents a single byte. Before using Eq. (10), just convert d_1, d_2, d_3, d_4 from 1 and 0 s to decimal.

Table 1 Eight encoding rules of DNA

Binary sequence	R1	R2	R3	R4	R5	R6	R7	R8
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

Table 2 XOR process for DNA sequence

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Table 3 Addition (+) process for a DNA sequence

Addition	A	C	T	G
A	C	A	G	T
T	G	T	C	A
C	A	C	T	G
G	T	G	A	C

Table 4 Subtraction (−) process for a DNA sequence

Subtraction	A	C	T	G
A	C	G	A	T
T	G	T	C	A
C	A	C	T	G
G	T	A	G	C

3.2.6 Deoxyribonucleic acid string (DNA)

DNA is divided into four separate nucleic acid bases: adenine (A), thymine (T), cytosine (C), and guanine (G), as well as other required components. A and T, as well as C and G, create complementary sequences (Eldesouky et al. 2022). The complementing rule is satisfied by eight rules. The fundamental image is encoded using four separate nucleo bases that follow eight different standards. The decimal number 201, for example, has a binary equivalent of '11001001'. '11001001' is encoded following to DNA principles, resulting in eight different forms: 'TACG', 'TAGC', 'ATCG', 'ATGC', 'CGTA', 'CGAT', 'GCTA', and 'GCAT'.

Furthermore, to encrypt the data, use numerous DNA sequence techniques like addition, subtraction, and exclusive OR (XOR). Tables 1, 2, 3 and 4 outline the DNA match rules and processes (Ayoup et al. 2022; Eldesouky et al. 2022; Faragallah et al. 2022).

3.2.7 DNA cryptosystem

In the DNA cryptosystem, we should apply the following steps:

1. Use Eqs. (8) and (11) to produce the key image

$$\text{pixel} = [X \times 256], \tag{11}$$

The recurrence value for PWLCM is $X \in (0, 1)$. Equation (10) determines the starting value of Eq. (8). Neighboring pixels in the key image are likely to be unrelated to one another. Pixels produced from a chaotic map are a great way to achieve these requirements. The predicted value of the next pixel generated differs from the current one.

2. The FECT and key images are encoded on rows using the DNA standards defined by Eqs. (9) and (12).

$$\text{Rule(standard)} = [X \times 8] + 1, \tag{12}$$

The initial result of Eq. (9) is obtained from Eq. (10). Table 1 contains a list of the eight DNA standards. Each pixel in a row is encoded with one of the DNA standards, and each row uses a new set of DNA standards until the entire image is encoded. Corresponding to DNA encoding standards, 8 bits of each image pixel are separated and encoded into 4 categories of nucleobases.

3. DNA operations are performed row by row between the Encoded (FECT) and the encoded key image. Equations (9) and (13) indicate the type of DNA procedures to be carried out. Tables 2, 3 and 4 outline the fundamentals of DNA processes.

$$\text{process(operation)} = [X \times 3] + 1, \tag{13}$$

Different types of DNA operations (XOR, +, −) are conducted in a row-by-row way until the encoded intermediate representation image appears.

4. By using a decoding methodology on the past intermediate representation image, you would be able to obtain the decoded intermediate one. Equation (12) expresses the decoding procedure. Using this process, we may obtain a preliminary cipher representation.
5. The first cipher image is rotated 90 degrees anti-clockwise. In this case, we merely study images by rows and then by columns.
6. Repeat steps 2 through 4 for the columns to create a Final Encrypted cancelable biometric template.

4 Authentication evaluation metrics

The visual examination is important in assessing cancelable biometrics since robust encryption and great cancelability arise from highly coveted features in the recommended cancelable biometric cryptosystem. Quality assessment does not rely just on direct observation. As a result, numerous measurements are used to assess the progress of the cancelable biometric architecture. Correlation criteria assess the relationship between a recorded biometric pattern and a biometric input pattern. The greater the factor value, the more similar the templates will be. Access to the system is granted if the correlation score for a checked user exceeds a certain

Fig. 7 The tested twelve biometric images of the LFW-deep funneled database

level. Mathematically, an authorised person's correlation ratio must be greater than a hacker attempting to get access to the database.

The receiver operating characteristic (ROC) curve may be used to assess the success of the presented cancelable biometric authentication system. The true positive factor (TPF) and the false-positive factor (FPF) are represented by the ROC curve as in Ibrahim et al. (2020b) and Hashad et al. (2020). The ROC curve idea is based on a decision variable. In every biometric identification system, the tested information includes genuine and false templates, allowing each pattern value to be dispersed around a given mean value.

As a result, the authentic template's mean value is greater than the false template's mean value. Furthermore, the encryption efficiency is evaluated by calculating correlation coefficients, histogram deviation, SSIM, MSE (Mean Square Error), PSNR (Peak Signal-to-Noise Ratio), Number of Pixel Change Rate (NPCR), UACI (Unified Average Changing Intensity), and histogram uniformity among protected and original biometrics. For cancelable biometric systems, the values of Correlation, PSNR, and SSIM should be at their lowest. But values for NPCR, MSE, and UACI should be at their highest levels. These authentication metrics will be explored in depth in order to assess the quality of the planned cancelable biometric authentication framework as follows:

Fig. 8 The tested twelve biometric images of the UFI database

4.1 Histogram analysis

The histogram depicts the distribution degree for every pixel strength in a biometric image. In the case of cancelable biometric technologies, the histogram must have both features for the protected biometric template, which is based on encryption methodology (Algarni et al. 2020b):

1. The cipher biometric image's histogram differs from the basic biometric image's histogram.
2. It must have an identical distribution, meaning all pixel values are distributed uniformly.

4.2 Correlation score

The correlation is a comparison of the biometric template and its distorted replica. It is calculated between two adjacent pixels of an image as in the following equation (Helmy et al. 2022b):

$$C_{i,j} = \frac{cov(i,j)}{\sqrt{D(i)}\sqrt{D(j)}}, \tag{14}$$

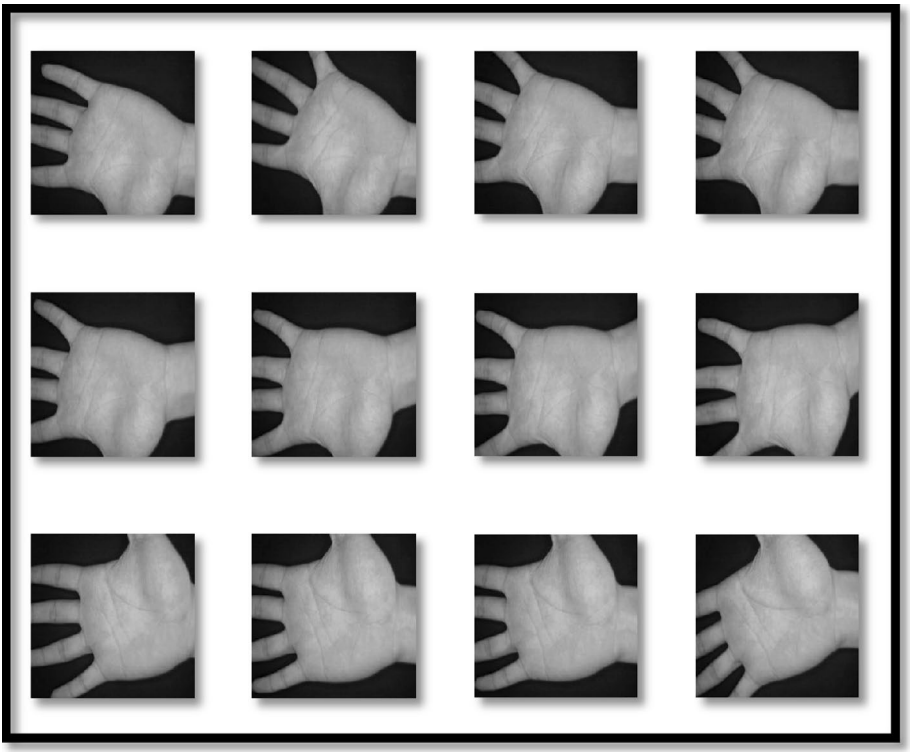


Fig. 9 The tested twelve biometric images of the ROI palmprint database

$$D(i) = \frac{1}{M} \sum_{ii=1}^{M} \left(i_{ii} - E(i)\right)^2, \tag{15}$$

$$cov(i,j) = E\{(i - E(i))(j - E(j))\}, \tag{16}$$

$$E(i) = \frac{1}{M} \sum_{ii=1}^{M} i_{ii}, \tag{17}$$

where M is the number of pixels, $C_{i,j}$ is the correlation coefficient, and i,j are grayscale values of two neighboring pixels in the basic image or ciphered image. The correlation assessment has two scenarios, which are detailed below:

1. When the correlation coefficient is near one, it explores the highest score, which occurs only when 2 biometric images are strongly correlated.
2. The $C_{i,j}$ score is close to or equal to zero, indicating a considerable difference between the permitted biometric image and its encrypted form, where the ciphered biometric pattern is completely independent of the primary one.

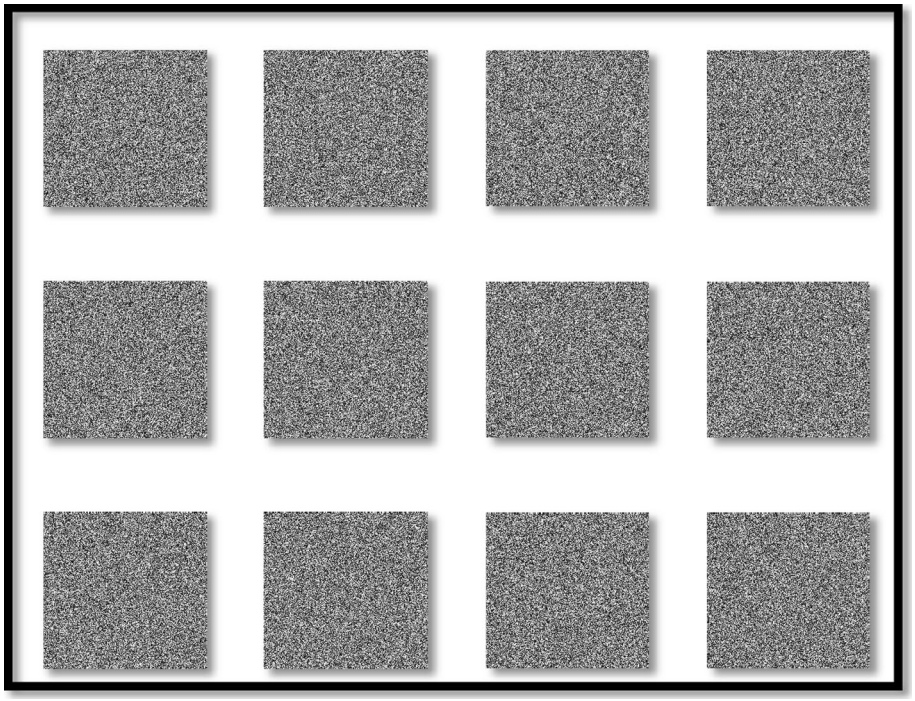


Fig. 10 The cancelable biometrics for the recommended cryptosystem for the LFW-deep funneled database

4.3 The probability of true distribution (PTD) and false distribution (PFD)

In permitted access scenarios, the PTD reflects the probability distribution of the statistical correlation. The PFD displays the statistical correlation's probability distribution in spoofed access conditions. Only if a biometric test score exceeds a specified level (Equal Error Rate (EER)), which is calculated at the intersection of the imposter and real distributions, is access permitted to the system. As in El-Shafai et al. (2021b), the inaccurate reject and wrong accept errors are equivalent at this junction point.

4.4 The receiver operating characteristic (ROC) curve analysis

Receiver operating characteristic (ROC) analysis is a graphical method of evaluating the efficiency of the structure. The sensitivity (true positive rate) of a ROC curve is depicted as a mathematical function of the specificity (false positive rate) at different intersection locations as in Faragallah et al. (2021a).

4.5 Structural similarity index metric (SSIM)

It is a strategy for determining the similarity between two images. The SSIM is used as a measure for encryption efficiency in this research. A strong encryption technique should

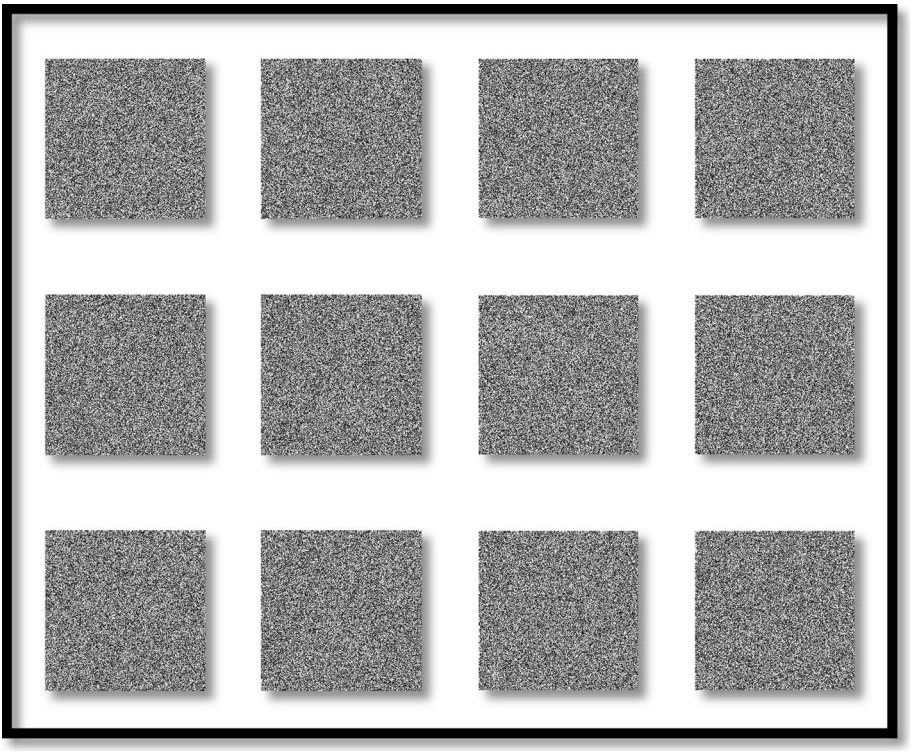


Fig. 11 The cancelable biometrics for the recommended cryptosystem for the UFI face database

have SSIM values (the difference between the actual and encrypted pictures) near zero, as in El-Shafai et al. (2021b). It is described with the following equation:

$$SSIM = \frac{\left(2\mu_I\mu_T + S_1\right)\left(2\sigma_{IT} + S_2\right)}{\left(\mu_I^2 + \mu_T^2 + S_1\right)\left(\sigma_I^2 + \sigma_T^2 + S_2\right)}, \tag{18}$$

where μ_I and μ_T are the averages of an input image (I) and the encrypted image T, respectively, σ_I^2 and σ_T^2 correspond to the variances of I and T, respectively, σ_{IT} signifies the covariance between them, and finally S_1 and S_2 are small values.

4.6 Statistical histogram deviation (D_H)

This parameter is used to assess the recommended cryptosystem's ciphering strength by determining the highest amount of deviations among the histograms of pure and ciphered images as in Alqahtani et al. (2022). It can be determined using Eq. (19):

$$D_H = \frac{\left(\frac{q_0+q_{255}}{2} + \sum_{i=1}^{254} q_i\right)}{M \times N}, \tag{19}$$

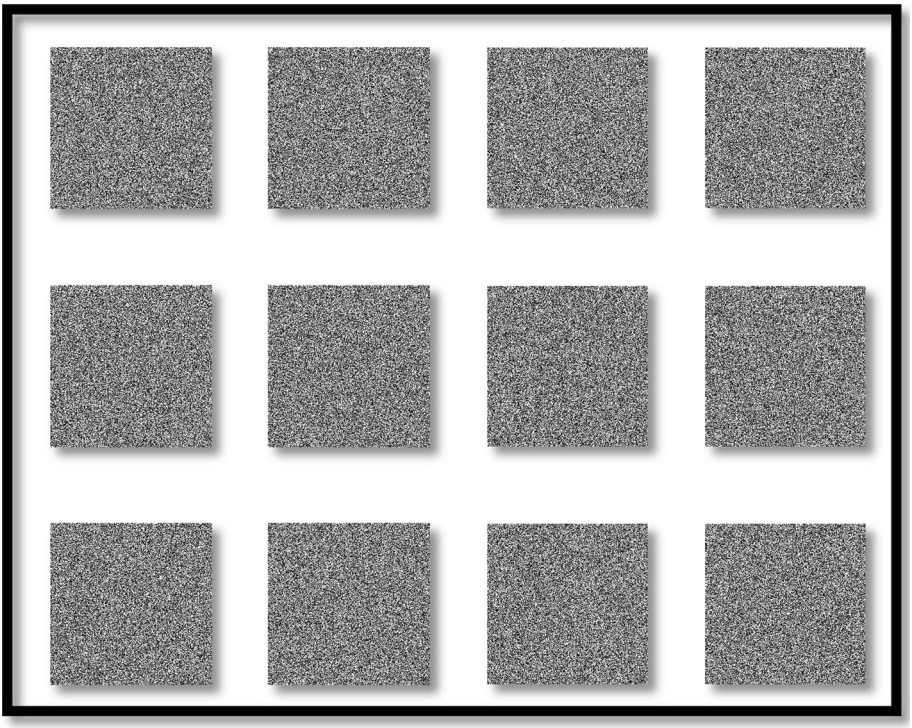


Fig. 12 The cancelable biometrics for the recommended cryptosystem for the ROI palmprint database

Table 5 Correlation coefficients of neighboring pixels in the tested twelve biometrics images and their ciphered of LFW deep funneled database

Biometric	Original biometric			Ciphered biometric		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Face 1	0.9862	0.9857	0.9758	− 0.0119	0.0003	0.0028
Face 2	0.9931	0.9863	0.9829	− 0.0061	− 0.0101	0.0022
Face 3	0.9869	0.9862	0.9752	− 0.0072	− 0.0074	0.0071
Face 4	0.9954	0.9967	0.9920	− 0.0026	− 0.0055	− 0.0007
Face 5	0.9899	0.9928	0.9846	− 0.0046	− 0.0068	− 0.0021
Face 6	0.9930	0.9928	0.9872	− 0.0036	− 0.0090	0.0044
Face 7	0.9830	0.9825	0.9685	− 0.0066	− 0.0050	0.0026
Face 8	0.9839	0.9846	0.9665	0.0009	− 0.0008	− 0.0031
Face 9	0.9904	0.9853	0.9783	− 0.0065	− 0.0083	0.0028
Face 10	0.9906	0.9893	0.9804	− 0.0155	− 0.0039	0.0013
Face 11	0.9917	0.9905	0.9790	− 0.0058	0.0023	− 0.0006
Face 12	0.9884	0.9891	0.9806	− 0.0029	− 0.0111	0.0037

where q_i is the absolute difference between the pure and ciphered images' estimated histograms at a gray level i. Hence, the greater the magnitude of D_H, the greater the deviation of

Table 6 Correlation coefficients of neighboring pixels in the tested twelve biometrics images and their ciphered of UFI database

Biometric	Original biometric			Ciphered biometric		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Face1	0.9111	0.8667	0.8407	− 0.0093	0.0070	− 0.0042
Face 2	0.9874	0.9787	0.9670	− 0.0034	0.0002	0.0049
Face 3	0.9716	0.9587	0.9471	− 0.0084	− 0.0053	0.0035
Face 4	0.9624	0.9600	0.9476	− 0.0066	− 0.0163	0.0046
Face 5	0.9356	0.9295	0.9004	− 0.0145	− 0.0098	− 0.0082
Face 6	0.9398	0.9359	0.8967	− 0.0016	− 0.0056	0.0041
Face 7	0.9309	0.9227	0.8975	− 0.0030	− 0.0075	0.0022
Face 8	0.9656	0.9676	0.9509	− 0.0051	− 0.0068	− 0.0004
Face 9	0.9630	0.9704	0.9515	− 0.0065	− 0.0023	0.0026
Face 10	0.9736	0.9608	0.9526	− 0.0077	0.0008	0.0002
Face 11	0.9624	0.9664	0.9496	− 0.0063	− 0.0111	0.0036
Face 12	0.9842	0.9837	0.9715	− 0.0029	0.0001	0.0056

Table 7 Correlation coefficients of neighboring pixels in the tested twelve biometrics images and their ciphered of the ROI palmprint database

Biometric	Original biometric			Ciphered biometric		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Palmprint 1	0.9968	0.9986	0.9972	− 0.0125	− 0.0058	0.0071
Palmprint 2	0.9977	0.9979	0.9975	− 0.0057	0.0042	− 0.0006
Palmprint 3	0.9974	0.9982	0.9970	− 0.0075	0.0032	− 0.0054
Palmprint 4	0.9975	0.9981	0.9972	− 0.0064	− 0.0042	− 0.0003
Palmprint 5	0.9973	0.9985	0.9966	− 0.0064	− 0.0043	− 0.0055
Palmprint 6	0.9971	0.9984	0.9959	− 0.0087	− 0.0042	0.0027
Palmprint 7	0.9972	0.9983	0.9956	− 0.0040	− 0.0104	− 0.0008
Palmprint 8	0.9971	0.9983	0.9953	− 0.0096	− 0.0026	0.0020
Palmprint 9	0.9969	0.9982	0.9946	− 0.0025	0.0027	0.0017
Palmprint 10	0.9970	0.9983	0.9953	− 0.0057	− 0.0059	0.0053
Palmprint 11	0.9970	0.9983	0.9954	0.0016	− 0.0104	− 0.0014
Palmprint 12	0.9977	0.9979	0.9946	− 0.0023	− 0.0053	− 0.0059

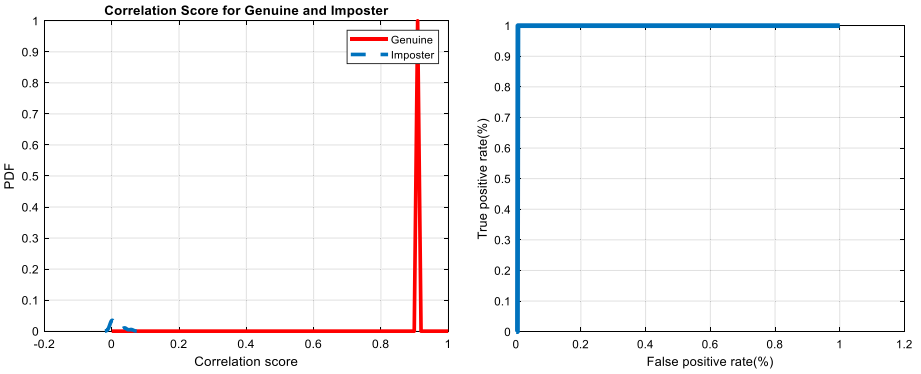
the cipher image from the main image.

4.7 PSNR metric

The peak signal-to-noise ratio (PSNR) is employed to assess the suggested cryptosystem's strength in the case of channel noise. It is assessed among the actual and ciphered images. PSNR is an abbreviation for the ratio of a signal's highest possible value (power) to the strength of distorting noise that influences the quality of its representation. The value of $PSNR \in [0, \infty]$. The PSNR ratios between the cypher image and the basic image should be

Table 8 Correlation and SSIM values for the twelve biometrics images of the LFW deep funneled database

Twelve biometrics images of the LFW deep funneled database	Correlation/SSIM with a false face		Correlation/SSIM with genuine face	
	Correlation	SSIM	Correlation	SSIM
Face 1	0.0123	0.0096	0.9058	0.9009
Face 2	0.0231	0.0099	0.9066	0.9022
Face 3	0.0433	0.0069	0.9042	0.8992
Face 4	0.0014	0.0088	0.9047	0.9001
Face 5	0.0034	0.0076	0.9050	0.9005
Face 6	0.0032	0.0045	0.9044	0.8997
Face 7	0.0037	0.0094	0.9048	0.9000
Face 8	0.0399	0.0062	0.9051	0.9002
Face 9	0.0003	0.0080	0.9054	0.9008
Face 10	0.0585	0.0073	0.9057	0.9012
Face 11	0.0009	0.0101	0.9054	0.9007
Face 12	0.0055	0.0081	0.9038	0.8993
Average	0.0162	8.033×10^{-3}	0.9051	0.9004



a) PTD and PFD of the proposed algorithm at noise variance =0.02

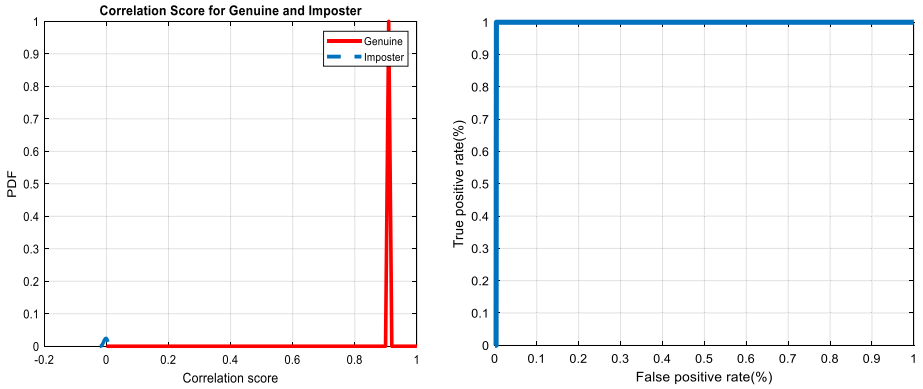
b) ROC curve of the proposed algorithm at noise variance =0.02

Fig. 13 The authentication outcomes of the cryptosystems on the LFW deep funneled dataset

low for an efficient encryption procedure, as in Alqahtani et al. (2022). The PSNR is calculated analytically as indicated in Eq. (20):

$$PSNR = 10\log_{10}\frac{(2^n - 1)^2}{MSE}, \tag{20}$$

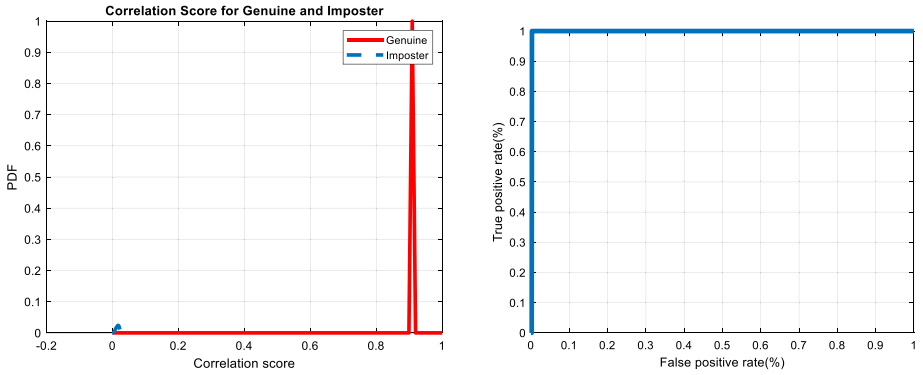
where n is the number of bits/pixel, and MSE is the Mean Squared Error. The value of PSNR ϵ [0,∞]. MSE can be calculated by the following equation:



a) PTD and PFD of the proposed algorithm at noise variance =0.02

b) ROCcurveof the proposed algorithm at noise variance =0.02

Fig. 14 The authentication outcomes of the cryptosystems on the UFI database



a) PTD and PFD of the proposed algorithm at noise variance =0.02

b) ROC curve of the proposed algorithm at noise variance =0.02

Fig. 15 The authentication outcomes of the cryptosystems on the ROI palmprint database

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{x=M} \sum_{y=1}^{y=N} \left[O(x,y) - T(x,y) \right]^2, \tag{21}$$

where O is the reference image, T is the encrypted image.

4.8 Number of pixel change rate (NPCR)

The NPCR measure is defined as a percentage of different pixel amounts between two ciphered images. If the ciphering procedure produces a higher NPCR value, the ciphering technique given is resistant to differential attacks. The NPCR metric is calculated as shown in (22) and (23) as in El-Shafai et al. (2022d):

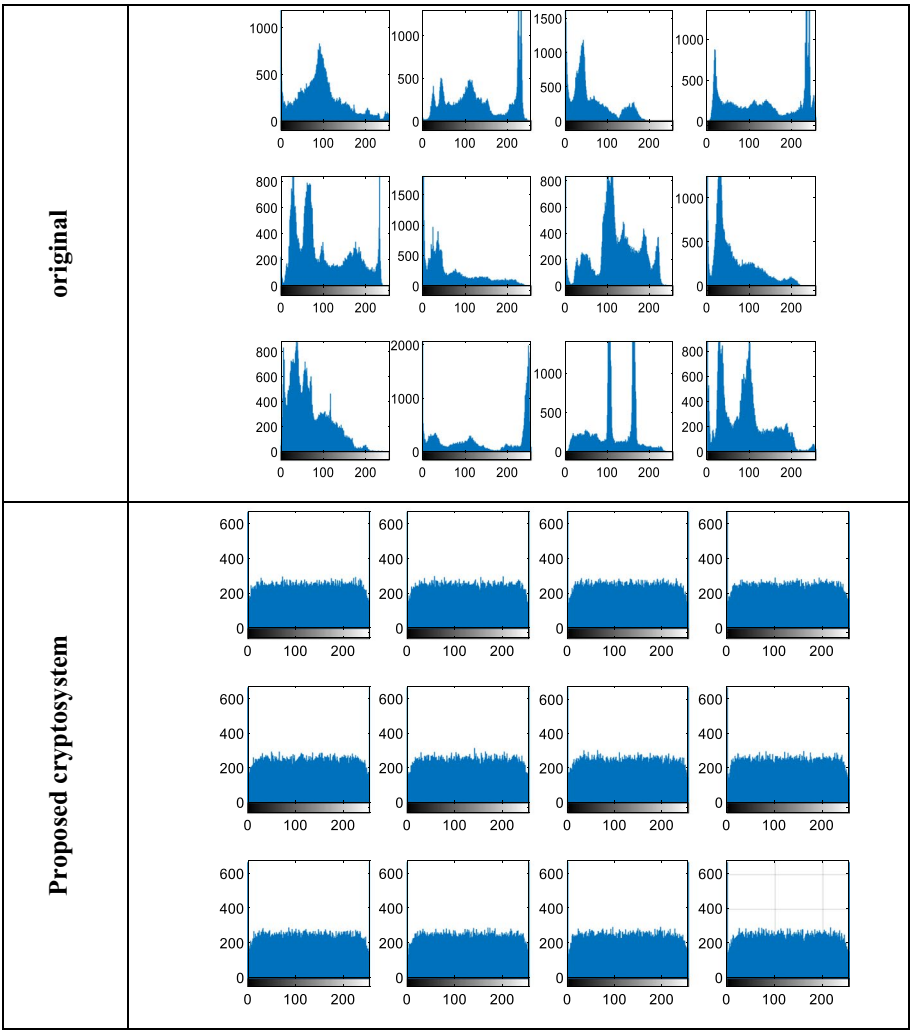


Fig. 16 Results of the proposed cryptosystem's histogram for the original and cipher biometrics of the LFW deep funneled dataset

$$NPCR = \frac{\sum_{i,j} g(i,j)}{M \times N} \times 100 \tag{22}$$

$$g(i,j) = \begin{cases} 0 & O(i,j) = T(i,j) \\ 1 & otherwise \end{cases} \tag{23}$$

$g(i,j)$ denotes the difference between related pixels of the plain image and the encrypted image**.** The estimated NPCR value of a ciphered image must be near to 100.

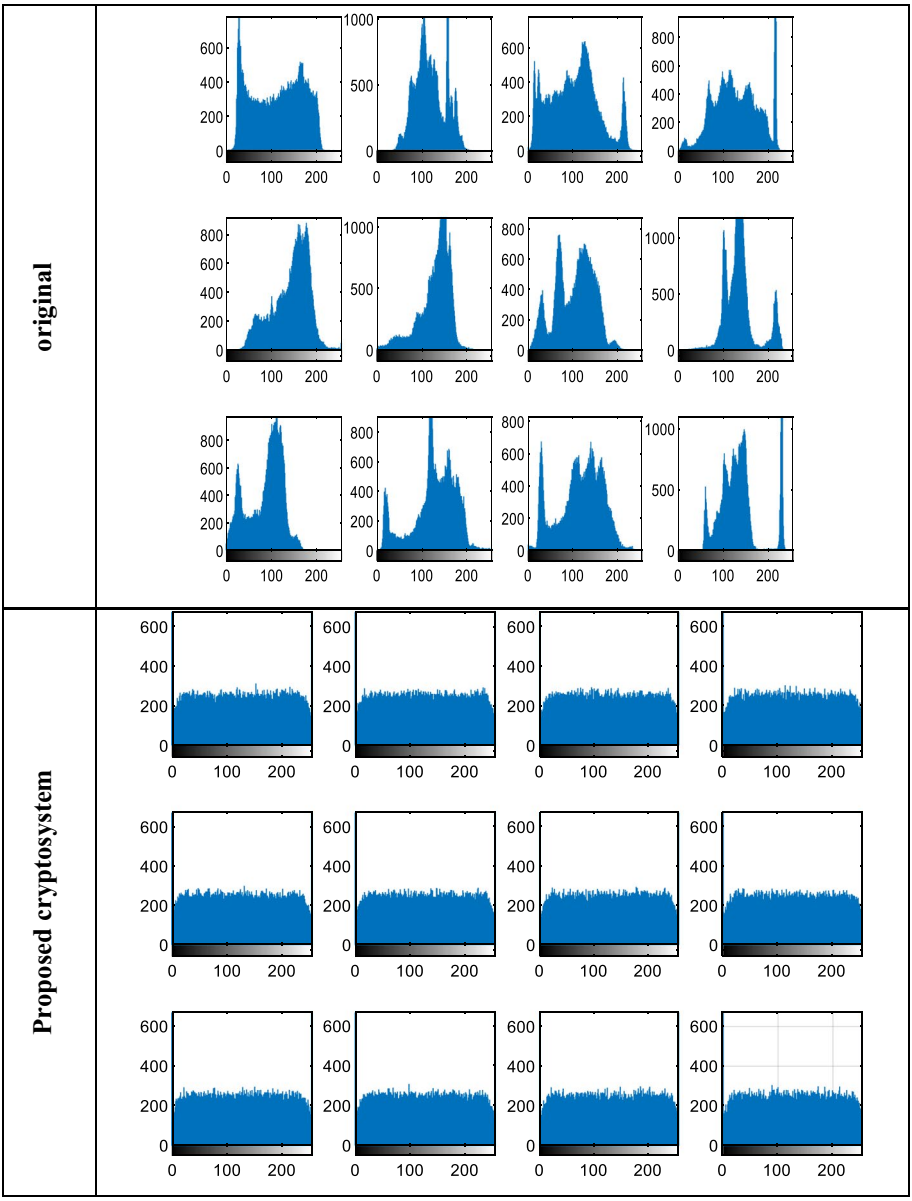


Fig. 17 Results of the proposed cryptosystem's histogram for the original and cipher biometrics of the UFI database

4.9 Unified average changing intensity (UACI)

It is employed to measure the intensity value difference between two images. The value of UACI in cancelable biometric technology must be high as in El-Shafai et al. (2022d). It can be computed as in Eq. (24):

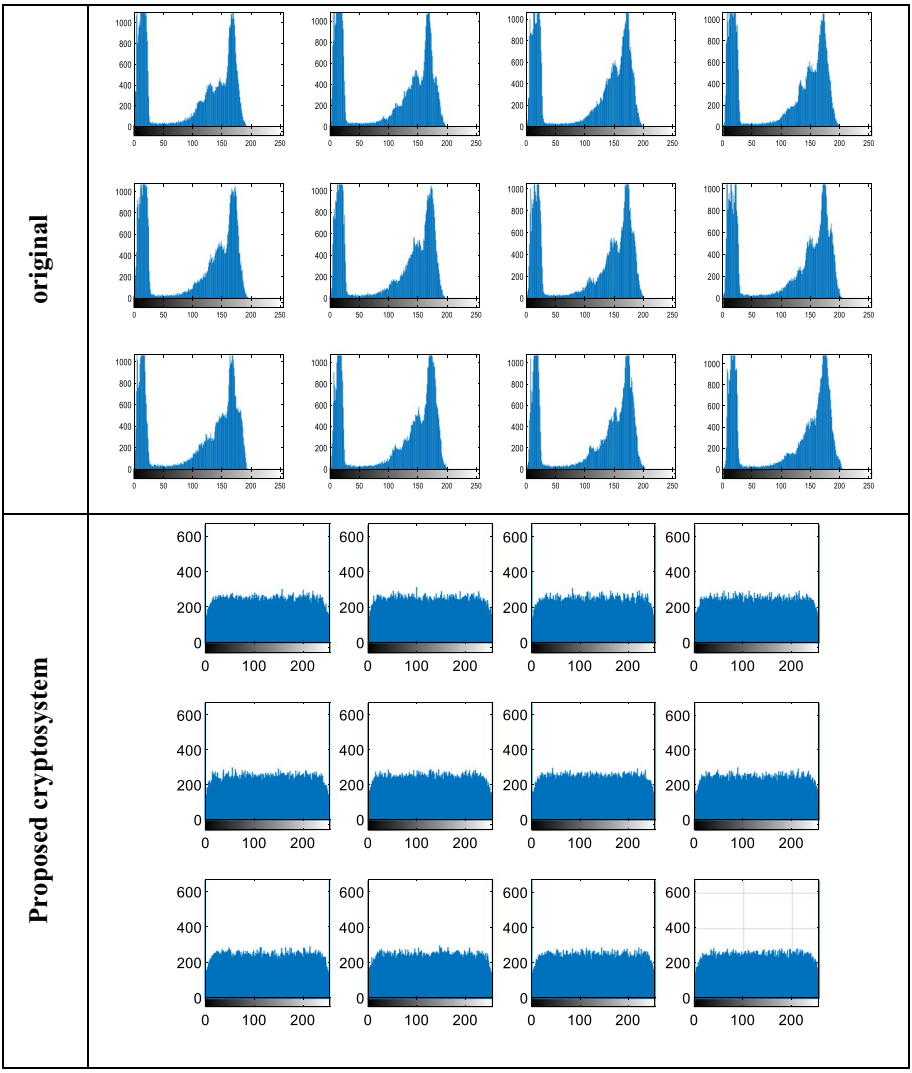


Fig. 18 Results of the proposed cryptosystem's histogram for the original and cipher biometrics of the ROI palmprint database

$$UACI = \frac{1}{M \times N}\left(\sum_{i,j}\frac{|O(i,j) - T(i,j)|}{255}\right) \times 100 \tag{24}$$

Table 9 Correlation and SSIM values for the twelve biometrics images of the UFI database

Twelve biometrics images of the UFI database	Correlation/SSIM with a false face		Correlation/SSIM with genuine face	
	Correlation	SSIM	Correlation	SSIM
Face 1	0.0011	0.0090	0.9054	0.9008
Face 2	0.0038	0.0103	0.9053	0.9005
Face 3	0.0092	0.0098	0.9046	0.8999
Face 4	0.0029	0.0105	0.9063	0.9019
Face 5	0.0038	0.0101	0.9066	0.9020
Face 6	0.0025	0.0112	0.9046	0.8999
Face 7	0.0010	0.0096	0.9058	0.9010
Face 8	0.0030	0.0113	0.9056	0.9011
Face 9	0.0077	0.0093	0.9053	0.9004
Face 10	0.0068	0.0093	0.9050	0.9003
Face 11	0.0030	0.0105	0.9068	0.9021
Face 12	0.0014	0.0107	0.9050	0.9004
Average	3.85×10^{-3}	0.0101	0.9055	0.9008

Table 10 Correlation and SSIM values for the twelve biometrics images of the ROI palmprint database

Twelve biometrics images of the ROI palmprint database	Correlation/SSIM with a false face		Correlation/SSIM with genuine face	
	Correlation	SSIM	Correlation	SSIM
Palmprint 1	0.0139	0.0086	0.9051	0.9003
Palmprint 2	0.0169	0.0077	0.9053	0.9005
Palmprint 3	0.0156	0.0080	0.9056	0.9010
Palmprint 4	0.0193	0.0080	0.9045	0.8999
Palmprint 5	0.0119	0.0082	0.9054	0.9008
Palmprint 6	0.0132	0.0085	0.9053	0.9005
Palmprint 7	0.0181	0.0079	0.9043	0.8995
Palmprint 8	0.0109	0.0084	0.9064	0.9018
Palmprint 9	0.0186	0.0081	0.9050	0.9003
Palmprint 10	0.0185	0.0076	0.9049	0.9001
Palmprint 11	0.0184	0.0087	0.9048	0.9001
Palmprint 12	0.0057	0.0081	0.9045	0.8997
Average	0.0150	8.15×10^{-3}	0.9050	0.9003

Table 11 FAR, Histogram Deviation, PSNR, and AROC of the proposed cancelable system for all the datasets

Metrics	LFW deep funneled samples	UFI samples	ROI palmprint samples	Average
FAR	0.0049	0.0061	0.0076	6.2×10^{-3}
AROC	0.9958	0.9948	0.9934	0.9946
D_H	0.7242	0.8402	1.0622	0.8755
PSNR	7.5473	9.2309	7.8401	8.2061

Table 12 All the metrics (FAR, D_H, PSNR and AROC) of the LFW deep funneled dataset at different noise analyses

Noise variance	FAR	D_H	PSNR	AROC
0.01	0.0014	0.7242	7.5473	0.9989
0.02	0.0076	0.7242	7.5473	0.9934
0.03	0.0139	0.7242	7.5473	0.9876
0.04	0.0363	0.7242	7.5473	0.9665
0.05	0.0659	0.7242	7.5473	0.9365
0.06	0.0759	0.7242	7.5473	0.9259

Table 13 All the metrics (FAR, D_H, PSNR and AROC) of the UFI dataset at different noise analyses

Noise variance	FAR	D_H	PSNR	AROC
0.01	9.0832×10^{-4}	0.8402	9.2309	0.9992
0.02	0.0030	0.8402	9.2309	0.9974
0.03	0.0136	0.8402	9.2309	0.9878
0.04	0.0256	0.8402	9.2309	0.9768
0.05	0.0477	0.8402	9.2309	0.9559
0.06	0.0779	0.8402	9.2309	0.9282

Table 14 All the metrics (FAR, D_H, PSNR and AROC) of the ROI palmprint dataset at different noise analyses

Noise variance	FAR	D_H	PSNR	AROC
0.01	9.5700×10^{-4}	1.0622	7.8401	0.9992
0.02	0.0050	1.0622	7.8401	0.9957
0.03	0.0131	1.0622	7.8401	0.9884
0.04	0.0225	1.0622	7.8401	0.9797
0.05	0.0315	1.0622	7.8401	0.9712
0.06	0.0356	1.0622	7.8401	0.9671

Table 15 Comparison between the proposed cryptosystem and the traditional authentication approaches

System	MSE	PSNR	NPCR	UACI	CF	AROC	FAR
Proposed	12983.15	7.031	99.57	36.75	-2.6×10^{-3}	0.9946	6.2×10^{-3}
Nagar et al. (2010)	68.2024	29.8268	36.4149	0.0316	0.3575	0.7187	53.32
El-Shafai and Hemdan (2021)	107.0064	27.8707	47.386	0.0508	0.3504	0.8737	53.46
El-Shafai et al. (2021c)	91.9136	28.531	49.936	25.1084	− 0.005	0.8630	53.76
Badr et al. (2021)	83.4411	28.951	49.995	23.558	0.1574	0.8271	53.49
Faragallah et al. (2021b)	94.8593	28.394	99.418	9.3219	− 0.0017	0.9414	52.49
El-Shafai et al. (2022d)	101.2931	28.109	99.995	11.5172	− 0.0025	0.8812	44.81

5 Simulation results and discussions

The images used in the study are 256×256 images with an 8-bit per pixel resolution.

The suggested cryptosystem has the benefit of being able to deal with any sort of image (grayscale/color) of varying sizes and characteristics. The proposed cryptosystem is implemented on the Intel(R) processor Core (TM) i5-10210U CPU @ 1.60 GHz, an operating system of Windows 10, 8.00 GB RAM. The experimental results are obtained using MATLAB R2019a. The simulation analyses are reviewed visually and by various criteria for an efficient evaluation of the proposed cryptosystem, such as histogram uniformity, correlation coefficient, histogram deviation, Structural Similarity (SSIM) Index, Peak Signal-to-Noise Ratio (PSNR), FAR (False Acceptance Rate), and AROC. We examine two various datasets of faces (UFI database-LFW deep funneled) and ROI palmprint dataset to evaluate the recommend cancelable biometric authentication architecture. In simulation studies, the first two trial samples are for 12 different biometric faces of various persons, while the remaining samples are for different palmprint images of various users, as shown in Figs. 7, 8 and 9.

The recommended cryptosystem's ciphering performance for each of the evaluated biometric samples is shown in Figs. 10, 11 and 12. From the perspective of a visual encryption assessment, the suggested cancelable biometric architecture achieves high performance. Tables 5, 6, 7 and 8 present Correlation coefficients of neighboring pixels in the tested twelve biometrics images and their ciphered of all examined databases.

Distortion and encryption so that the actual biometrics may be kept securely in a cloud server. Figures 13, 14 and 15 show the ROC, PFD, and PTD curves of the authentication stage for the proposed encryption technique for all analyzed biometric samples. The PFD and PTD intersection point specifies the threshold crossing rate, which is then used to verify whether or not this individual is a real user.

Figures 16, 17 and 18 show the histograms of the original and ciphered biometrics for the offered cryptosystem of all tested biometric datasets. The recommended cryptosystem is shown to provide relatively uniform and flat histogram results, demonstrating its better decision-making. Hence, applying this cryptosystem on the ROI palmprint biometrics database histogram, for example, achieves security features and makes this database secure from intruders. Two biometrics images have been examined for all simulation testing in the verification process. Both belong to different users—one is the real user, and the other is an impostor. To assess the performance of the proposed encryption strategy, the correlation and SSIM values are checked between the two examined encrypted patterns (false and genuine) and the real stored secured biometric patterns. Our research considers that the physical environment contains some noise that might impact the saved or tested biometric patterns. Therefore, noise is a factor in all experimental data.

Tables 8, 9 and 10 present the results of the fake/genuine correlation analysis and the SSIM evaluation for a selection of patterns from the three biometrics datasets. In Table 8, the average correlation/SSIM values of the LFW deep funneled database in the case of the false face are 0.0162 and 8.033×10^{-3} respectively, while in the case of the genuine face, the average correlation/SSIM values are 0.9051 and 0.9004, respectively. In Table 9, the average values of the UFI database correlation/SSIM for the false face are 3.85×10^{-3} and 0.0101, respectively, whereas the average values for a genuine face are shown as 0.9055 and 0.9008, respectively. In Table 10, the average ROI palmprint database correlation/SSIM values for the false face are 0.0150 and 8.15×10^{-3} respectively, even though the average values for a real face are 0.9050 and 0.9003, respectively. This indicates that palmprint authentication is successful because the results for a real person are close to one, while the results for a false person are close to zero. According to the outcomes in the tables, the proposed technique produces the highest correlation coefficients and SSIM scores in genuine biometrics enrollment, while it achieves the lowest results in false biometrics enrollment.

Several criteria have been studied to ensure the efficacy of the proposed cipher scheme, such as FAR, AROC, PSNR, and Histogram Deviation (D_H). Table 11 shows the mathematical evaluation of the FAR, AROC, Histogram Deviation, and PSNR.

According to Table 11, the values of PSNR between the original image and the ciphered image for all the datasets range from (7.5473 to 9.2309), indicating the proposed algorithm's effectiveness. Tables 12, 13 and 14 show the current influence of various Gaussian noise variances on the evaluated biometrics for the suggested cancelable approach, with average FAR, PSNR,D_H, and AROC values. The measured FAR, D_H, PSNR, and AROC values demonstrate that the proposed architecture has a low noise sensitivity.

In Table 15, further trials are done to test the performance success of the recommend authentication approach with the traditional authentication approaches (El-Shafai et al. 2022d, 2021c; Nagar et al. 2010; El-Shafai and Hemdan 2021; Badr et al. 2021; Faragallah et al. 2021b) in order to further evaluate the overall effectiveness of the discussed cryptosystem for creating an efficient cancelable biometric authentication mechanism.

6 Conclusion and future work

This research studied an enhanced encryption technique for generating and constructing a more secure cancelable biometric authorization system. In order to provide a strong cancelable biometric identification system, this proposal's key contribution combines 3D chaotic maps, Piecewise Linear Chaotic Map (PWLCM), and Logistic Map with DNA sequence theory. This technique is constructed on confusion as well as diffusion approach. First, the 3D chaotic map is based on the following steps: (1) 3D Chaos creation, (2) chaos histogram equalization, (3) row rotation, (4) column rotation, and (5) XOR process. Secondly, PWLCM and Logistic Map are used for generating all of the main values required by DNA theory. Thirdly, DNA theory is applied as a second encryption algorithm to the output of the 3D chaotic algorithm. So, the proposed framework hides the whole discriminative properties of biometric templates, resulting in a fully unspecified biometric pattern. According to research, numerous biometric datasets may be encrypted using the specified cryptosystem technique. It also demonstrates its ability to protect biometric patterns compared to conventional approaches. The proposed cancelable biometric approach exhibits an average FAR of 6.2×10^{-3}, an average D_H of 0.8755, an average AROC of approximately 1, and an average PSNR of 8.2061. We recommend developing multi-biometric templates based on hybrid encryption techniques for future work to improve efficiency and secure biometric pattern storage against threats.

Acknowledgements The authors are very grateful to all the institutions in the affiliation list for successfully performing this research work. The authors would like to thank Prince Sultan University for their support.

Authors' contributions All authors are equally contributed.

Funding The authors did not receive support from any organization for the submitted work.

Availability of data and materials All data are available upon request from the corresponding author.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

Ethical approval and consent to participate All authors are contributing and accepting to submit the current work.

Consent for publication All authors are accepting to submit and publish the submitted work.

References

Abo-Hammour, Z.E., Alsmadi, O., Momani, S., Abu Arqub, O.: A genetic algorithm approach for prediction of linear dynamical systems. Math. Probl. Eng. 2013 (2013)

Abo-Hammour, Z., Abu Arqub, O., Momani, S., Shawagfeh, N.: Optimization solution of Troesch's and Bratu's problems of ordinary type using novel continuous genetic algorithm. Discrete Dyn. Nat. Soc. **2014** (2014)

Abu Arqub, O., Abo-Hammour, Z., Momani, S., Shawagfeh, N.: Solving singular two-point boundary value problems using continuous genetic algorithm. In: Abstract and Applied Analysis, vol. 2012. Hindawi (2012)

Ahmad, M., Alkanhel, R., El-Shafai, W., Algarni, A.D., El-Samie, F.E.A., Soliman, N.F.: Multi-objective evolution of strong s-boxes using non-dominated sorting genetic algorithm-II and chaos for secure telemedicine. IEEE Access **10**, 112757–112775 (2022). https://doi.org/10.1109/ACCESS.2022.3209202

Alarifi, A., Sankar, S., Altameem, T., Jithin, K.C., Amoon, M., El-Shafai, W.: A novel hybrid cryptosystem for secure streaming of high efficiency H. 265 compressed videos in IoT multimedia applications. IEEE Access **8**, 128548–128573 (2020)

Algarni, A.D., El Banby, G., Ismail, S., El-Shafai, W., El-Samie, F.E.A., Soliman, F., N.: Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. Entropy **22**(12), 1361 (2020a)

Algarni, A.D., El Banby, G.M., Soliman, N.F., El-Samie, F.E.A., Iliyasu, A.M.: Efficient implementation of homomorphic and fuzzy transforms in random-projection encryption frameworks for cancellable face recognition. Electronics **9**(6), 1046 (2020b)

Almomani, I., Ahmed, M., El-Shafai, W.: DefOff: defensive/offensive system based on hiding technologies. In: 2022a 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), pp. 214–219. IEEE (2022a)

Almomani, I., Alkhayer, A., El-Shafai, W.: A crypto-steganography approach for hiding ransomware within HEVC streams in android IoT devices. Sensors **22**(6), 2281 (2022b)

Almomani, I., El-Shafai, W., AlKhayer, A., Alsumayt, A., Aljameel, S.S., et al.: Proposed biometric security system based on deep learning and chaos algorithms. Comput., Mater. Contin. **74**(2), 3515–3537 (2023)

Alqahtani, F., Amoon, M., El-Shafai, W.: A Fractional Fourier based medical image authentication approach. CMC-Comput. Mater. Contin. **70**(2), 3133–3150 (2022)

Alshammri, G.H., Samha, A.K., Hemdan, E.E.D., Amoon, M., El-Shafai, W.: An efficient intrusion detection framework in software-defined networking for cybersecurity applications. CMC-Comput. Mater. Contin. **72**(2), 3529–3548 (2022)

Arqub, O.A., Abo-Hammour, Z.: Numerical solution of systems of second-order boundary value problems using continuous genetic algorithm. Inf. Sci. **279**, 396–415 (2014)

Asaker, A.A., Elsharkawy, Z.F., Nassar, S., Ayad, N., Zahran, O., El-Samie, A., Fathi, E.: A novel cancellable Iris template generation based on salting approach. Multimedia Tools Appl. **80**(3), 3703–3727 (2021)

Ayoup, A.M., Khalaf, A.A., Alraddady, F., Abd El-Samie, F.E., El-Safai, W., Eldin, S.M.S.: Cancelable multi-biometric template generation based on dual-tree complex wavelet transform (2022)

Ayoup, A.M., Khalaf, A.A., El-Shafai, W., Abd El-Samie, F.E., Alraddady, F., Eldin, S.M.S.: Cancellable multi-biometric template generation based on Arnold cat map and aliasing. CMC-Comput. Mater. Contin. **72**(2), 3687–3703 (2022a)

Ayoup, A.M., Khalaf, A.A., Alraddady, F., Abd El-Samie, F.E., El-Safai, W., Eldin, S.M.S.: Selective cancellable multi-biometric template generation scheme based on multi-exposure feature fusion. Intell. Autom. Soft Comput. **33**(1), 549–565 (2022b)

Badr, I.S., Radwan, A.G., El-Rabaie, E.S.M., Said, L.A., El Banby, G.M., El-Shafai, W., Abd El-Samie, F.E.: Cancellable face recognition based on fractional-order Lorenz chaotic system and Haar wavelet fusion. Dig. Signal Process. **116**, 103103 (2021)

Elazm, L.A.A., El-Shafai, W., Ibrahim, S., Egila, M.G., Shawkey, H., et al.: Efficient hardware design of a secure cancellable biometric cryptosystem. Intell. Autom. Soft Comput. **36**(1), 929–955 (2023)

Eldesouky, S., El-Shafai, W., Ahmed, H.E.D.H., El-Samie, F.E.A.: Cancelable electrocardiogram biometric system based on chaotic encryption using three-dimensional logistic map for biometric-based cloud services. Secur. Priv. **5**(2), e198 (2022)

El-Gazar, S., El Shafai, W., El Banby, G.M., Hamed, H.F., Salama, G.M., Abd-Elnaby, M., Abd El-Samie, F.E.: Cancelable speaker identification system based on optical-like encryption algorithms. Comput. Syst. Sci. Eng. **43**(1), 87–102 (2022)

El-Hameed, H.A.A., Ramadan, N., El-Shafai, W., Khalaf, A.A., Ahmed, H.E.H., Elkhamy, S.E., El-Samie, F.E.A.: Cancelable biometric security system based on advanced chaotic maps. Vis. Comput. **38**(6), 2171–2187 (2022)

El-Shafai, W., & Hemdan, E. E. D. (2021). Robust and efficient multi-level security framework for color medical images in telehealthcare services. J. Ambient Intell. Hum. Comput. 1–16

El-Shafai, W., Almomani, I.M., Alkhayer, A.: Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication. IEEE Access **9**, 35004–35026 (2021a)

El-Shafai, W., Khallaf, F., El-Rabaie, E.S.M., El-Samie, F.E.A.: Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. J. Ambient. Intell. Hum. Comput. **12**(10), 9007–9035 (2021b)

El-Shafai, W., Mohamed, F.A.H.E., Elkamchouchi, H.M., Abd-Elnaby, M., Elshafee, A.: Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. IEEE Access **9**, 77675–77692 (2021c)

El-Shafai, W., Almomani, I., Ara, A., et al.: An optical-based encryption and authentication algorithm for color and grayscale medical images. Multimed Tools Appl (2022a). https://doi.org/10.1007/s11042-022-14093-3

El-Shafai, W., Khallaf, F., El-Rabaie, E.S.M., El-Samie, F.E. A.: Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services. J. Ambient Intell. Hum. Comput. 1–28 (2022b)

El-Shafai, W., Khallaf, F., El-Rabaie, E.S.M., El-Samie, A., Fathi, E.: Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. Neural Comput. Appl. 1–25 (2022c)

El-Shafai, W., Abd El-Hameed, H.A., Khalaf, A.A., Soliman, N.F., Alhussan, A.A., Abd El-Samie, F.E.: A hybrid security framework for medical image communication. CMC-Comput. Mater. Contin. **73**(2), 2713–2730 (2022d)

El-Shafai, W., Mesrega, A.K., Ahmed, H.E.H., El-Bahnasawy, N.A., Abd El-Samie, F.E.: An efficient multimedia compression-encryption scheme using latin squares for securing Internet-of-things networks. J. Inf. Secur. Appl. **64**, 103039 (2022e)

El-Shafai, W., Abd El-Hameed, H.A., El-Hag, N.A., Khalaf, A.A.M., Soliman, N.F., et al.: Proposed privacy preservation technique for color medical images. Intell. Autom. Soft Comput. **36**(1), 719–732 (2023b)

El-Shafai, W., Elsayed, M.A., Rashwan, M.A., Dessouky, M.I., El-Fishawy, A.S., et al.: Optical ciphering scheme for cancellable speaker identification system. Comput. Syst. Sci. Eng. **45**(1), 563–578 (2023a)

Faragallah, O.S., Afifi, A., El-Shafai, W., El-Sayed, H.S., Naeem, E.A., Alzain, M.A., et al.: Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications. IEEE Access **8**, 42491–42503 (2020)

Faragallah, O.S., Naeem, E.A., El-Shafai, W., Ramadan, N., Ahmed, H.E.D.H., Elnaby, M.M.A., et al.: Efficient chaotic-Baker-map-based cancelable face recognition. J. Ambient Intell. Hum. Comput. 1–39 (2021a)

Faragallah, O.S., El-Sayed, H.S., El-Shafai, W.: Efficient opto MVC/HEVC cybersecurity framework based on arnold map and discrete cosine transform. J. Ambient Intell. Hum. Comput. 1–16 (2021b)

Faragallah, O.S., El-Shafai, W., Sallam, A.I., Elashry, I., EL-Rabaie, E.S.M., Afifi, A., et al.: Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication. J. Ambient Intell. Hum. Comput. **13**(2), 1215–1239 (2022)

Hammad, M., Luo, G., Wang, K.: Cancelable biometric authentication system based on ECG. Multimedia Tools Appl. **78**(2), 1857–1887 (2019)

Hashad, F.G., Zahran, O., El-Rabaie, S., Elashry, I.F., Elbanby, G., Dessouky, M.I., et al.: Cancelable fingerprint recognition based on encrypted convolution kernel in different domains. Menoufia J. Electron. Eng. Res. **29**(2), 133–142 (2020)

Hassan, H.A., Hemdan, E.E., El-Shafai, W., et al.: Intrusion detection systems for the internet of thing: a survey Study. Wirel. Pers. Commun. (2022). https://doi.org/10.1007/s11277-022-10069-6

Helmy, M., El-Shafai, W., El-Rabaie, E.S.M., El-Dokany, I.M., Abd El-Samie, F.E.: A hybrid encryption framework based on Rubik's cube for cancelable biometric cyber security applications. Optik **258**, 168773 (2022a)
Helmy, M., El-Shafai, W., El-Rabaie, S., El-Dokany, I.M., El-Samie, F.E.A.: Efficient security framework for reliable wireless 3D video transmission. Multidimens. Syst. Signal Process. **33**(1), 181–221 (2022b)
Ibrahim, S., Egila, M.G., Shawkey, H., Elsaid, M.K., El-Shafai, W., Abd El-Samie, F.E.: Hardware implementation of cancellable biometric systems. In: 2020a 4th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 1145–1152. IEEE (2020a)
Ibrahim, S., Egila, M.G., Shawky, H., Elsaid, M.K., El-Shafai, W., El-Samie, A., Fathi, E.: Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption. Multimedia Tools Appl. **79**(19), 14053–14078 (2020b)
Leng, L., Teoh, A.B.J., Li, M., Khan, M.K.: Analysis of correlation of 2DPalmHash Code and orientation range suitable for transposition. Neurocomputing **131**, 377–387 (2014)
Mohamed, F.A.H.E., El-Shafai, W., Elkamchouchi, H.M., ELfahar, A., Alarifi, A., Amoon, M., et al.: A cancelable biometric security framework based on RNA encryption and genetic algorithms. IEEE Access **10**, 55933–55957 (2022)
Nagar, A., Nandakumar, K., Jain, A.K.: A hybrid biometric cryptosystem for securing fingerprint minutiae templates. Pattern Recogn. Lett. **31**(8), 733–741 (2010)
Nassar, M., Ali, A.M., El-Shafai, W., Saleeb, A., AbdEl-Samie, F.E., et al.: Hybrid of distributed cumulative histograms and classification model for attack detection. Comput. Syst. Sci. Eng. **45**(2), 2235–2247 (2023)
Qiu, J., Li, H., Zhao, C.: Cancelable palmprint templates based on random measurement and noise data for security and privacy-preserving authentication. Comput. Secur. **82**, 1–14 (2019)
Salama, G.M., El-Gazar, S., Omar, B., Nassar, R.M., Khalaf, A.A., El-Banby, G.M., et al.: Cancelable biometric system for IoT applications based on optical double random phase encoding. Opt. Express **30**(21), 37816–37832 (2022)
Soliman, R.F., El Banby, G.M., Algarni, A.D., Elsheikh, M., Soliman, N.F., Amin, M., Abd El-Samie, F.E.: Double random phase encoding for cancelable face and iris recognition. Appl. Opt. **57**(35), 10305–10316 (2018a)
Soliman, R.F., Amin, M., El-Samie, A., Fathi, E.: A double random phase encoding approach for cancelable iris recognition. Opt. Quant. Electron. **50**(8), 1–12 (2018b)
Soliman, N.F., Khalil, M.I., Algarni, A.D., Ismail, S., Marzouk, R., El-Shafai, W.: Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication. Multimedia Tools Appl. **80**(3), 4789–4823 (2021a)
Soliman, N.F., Algarni, A.D., El-Shafai, W., Abd El-Samie, F.E., El Banby, G.M.: An efficient GCD-based cancelable biometric algorithm for single and multiple biometrics. CMC-Comput. Mater. Contin. **69**(2), 1571–1595 (2021b)

Authors and Affiliations

Haidy A. Ali Eldawy[1] · Walid El-Shafai[1,2] · Ezz El-Din Hemdan[3] · Ghada M. El-Banby[4] · Fathi E. Abd El-Samie[1]

✉ Walid El-Shafai
walid.elshafai@el-eng.menofia.edu.eg; eng.waled.elshafai@gmail.com

Haidy A. Ali Eldawy
haidymohamed88@yahoo.com

Ezz El-Din Hemdan
ezzvip@yahoo.com

Ghada M. El-Banby
ghadaelbanby75@gmail.com

Fathi E. Abd El-Samie
fathi_sayed@yahoo.com

[1] Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[2] Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia

[3] Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[4] Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt