Wireless Personal Communications
https://doi.org/10.1007/s11277-023-10823-4

RESEARCH

A Proposed Cancelable Biometrical Recognition System (CBRS) Based on Developed Hénon Chaotic-Map

Ayman H. Abd El-aziem[1] · Ahmed Abdelhafeez[1] · Tamer H. M. Soliman[2,3]

Accepted: 18 December 2023

Abstract
Nowadays, human biometrics are widely used in authentication systems. In reaction to violent attacks, cancelable biometric patterns are developed from the original templates to increase the security level of biometric characteristics. This study proposes a solution for a cancelable biometrical recognition system (CBRS) based on the created Hénon chaotic-map idea, which increases key space and hence privacy. The suggested CBRS system ensures that the original biometric traits are updated and encrypted before they are saved in the database, protecting them from unwanted cyber-attacks. It makes efficient encryption of face biometric templates possible. The extraction of biometric characteristics is the first step in this design. Following that, the obtained biometric characteristics are encrypted using the suggested model, which causes pixel confusion and diffusion by developing a Henon chaotic map with variable block sizes at different modes of operation. Various face biometrics datasets were used to test the proposed approach. Various metrics, including security and statistical analyses, demonstrate the effectiveness of the approach, including histogram analysis, correlation coefficient analysis, maximum deviation factor analysis, irregular deviation factor analysis, number of pixels change rate analysis, unified average changing intensity analysis, time analysis, and key space analysis. Furthermore, the performance of the proposed approach was assessed using the receiver operating characteristic curve, which was constructed to assess the system's performance. Results of the analysis show that the suggested technique is very effective, resilient, and dependable, as evidenced by its great performance across diverse recognition databases when compared to traditional and modern algorithms, hence improving the security and reliability of biometric-based access management. The proposed method yields an average AROC of around 1, a correlation coefficient of about 0.00013, and an entropy close to one.

✉ Ayman H. Abd El-aziem
ayman.hasanein.comp@o6u.edu.eg

Ahmed Abdelhafeez
aahafeez.scis@o6u.edu.eg

Tamer H. M. Soliman
tamer.hasan.comp@o6u.edu.eg; thms78@gmail.com

[1] Faculty of IS & CS, October 6, University, Giza, Egypt

[2] AD Research and Development Center, Cairo, Egypt

[3] AD College, Cairo University, Cairo, Egypt

Published online: 29 January 2024

Keywords Face recognition · Hénon chaotic map · Cancellable biometrics

1 Introduction

The concept of chaos is prevalent in various natural phenomena and nonlinear systems. Chaotic systems possess favorable cryptographic features, including easy implementation and superior security and encryption rates [1–3]. In chaos theory, a system is considered chaotic when its behavior does not repeat despite being governed by deterministic equations. This means the system's future outcomes are determined by its initial conditions. Accessing systems through traditional authentication methods has its limitations. The use of chaotic signals in communication and engineering has become popular due to their advantageous properties for various applications. Numerous methods have been proposed to apply the nonlinear dynamics of chaotic systems to enhance communication systems' authentication [4–6]. Moreover, colossal attention has been given to combining well-constructed channel codes and cypher chaotic techniques with joint crypto-coded structures [2, 5]. With this collaborative structure, the most crucial channel codes used, such as turbo codes, LDPC codes, and polar codes, can support both enhancing the communication system performance and security behavior.

On the other hand, biometric recognition is highly effective in cryptography. The widespread use of biometric systems in cloud environments has raised concerns about system security and possible privacy violations [7]. Storing biometric data in these systems can make it vulnerable not only to attacks by adversaries through public networks but also to illegal disclosure in captive environments. A biometric system is a recognition system that uses physical or behavioral traits to identify individuals. These physical traits include fingerprints, hand geometry, ECG, iris scans, face and voice recognition [8]. Conversely, the category of behavioral identification comprises voice, signature, typing patterns, and walking style. The unique traits of an individual's body can be utilized to guarantee that only authorized personnel are granted access to the system [9].

Moreover, Biometric data is classified as sensitive information since, unlike passwords, biometric characteristics cannot be reset or cancelled. In biometric authentication systems, a sensor module is commonly used to acquire pictures, followed by a pre-processing module for aligning and reducing noise, a segmentation module for identifying areas, and a feature extraction module. Protecting biometric information is crucial in biometric systems as these characteristics are highly personal and sensitive information. Unlike passwords, they cannot be changed or revoked. Therefore, it is essential to prioritize the security of biometric systems to prevent any unauthorized access or misuse of this information. Ratha [10] introduced the concept of cancelable biometrics to ensure biometric data protection. In conventional biometric cryptosystems, the initial biometric templates are capable of being encrypted and saved in an encrypted format within the database. In the authentication process, a decryption step is necessary. However, cancelable biometric systems utilize encrypted biometric templates within a statistical framework to verify identity. Decrypting stored templates is unnecessary in a traditional biometric cryptosystem [11]. Cancelable biometrics refers to a deliberate alteration of the initial biometric templates, enabling enrollment and verification to be carried out in the transformed domain.

Numerous studies on multimodal biometric systems utilize traditional cancelable biometrics, which have been developed over the past few decades [12–17]. In addition, many researchers have only integrated chaotic performance into their security algorithms

[18–22]. However, only a limited number of studies have investigated the utilization of chaotic behavior in algorithms for multimodal biometric systems.

Based on facial recognition, this paper proposes a cancelable biometrical recognition system (CBRS) for creating cancelable biometric templates that provide a high level of security based on the developed Hénon Chaotic Map (DHCM). The CBRS proposed method ensures complete distortion and encryption of the original biometric characteristics before storing them in the database. The effectiveness of this approach is measured using different encryption evaluation metrics and Experimental analysis.

Due to the privacy and security problems associated with biometrics recognition, our current work remains a challenging research topic. To address this concern, the literature suggests cancelable biometrics, in which a biometric picture of a sample is deformed or altered so that obtaining the original biometric image from the distorted one becomes impossible. Moreover, cancelable biometrics has an important feature that allows it to be reissued in case of compromise. Our work proposes using the Hénon chaotic map to expand the range of chaos in biometric protection schemes instead of relying solely on standard Hénon chaotic maps with limited range or traditional cryptographic techniques.

The cryptographic primitives have been extensively researched and theoretically studied by the research community, resulting in solid constructions with well-defined limitations. Mainly, biometric security is assessed using abstract entropy concepts or the lowest associated data entropy. However, the accuracy of biometric systems varies significantly according to different theories. Cryptographic algorithms do not apply to biometric systems due to their unpredictable identification/verification procedures. We attempted to overcome this gap in our study by utilizing a cryptographic chaotic map, as we can ensure strong security measures are in place. To address the limitations of previous methods, we propose a cancelable biometric system where the user's biometric information is encrypted.

The paper is organized as follows. Section 2 will focus on explaining the mathematical foundation of two-dimensional chaotic maps, precisely the Hénon Chaotic system and its related construction principles. Section 3 introduces the main contribution of this paper, which is the design of the CBRS encryption algorithm. Moreover, in this section, we will explore the time analysis of our proposed CBRS scheme. Moving on to Sect. 4, by analyzing both the simulation and experimental encryption evaluation metrics, the results of the CBRS algorithm can provide better security behavior. Finally, some concluding remarks are provided in Sect. 5.

2 The Proposed Development Hénon Chaotic Map (DHCM)

2.1 Hénon Chaotic System

The Hénon Chaotic map is a two-dimensional chaotic map that transfers a point (x_i, y_i) to a new point in the same plane. [23–25] is a description of it.

$$\begin{aligned} x_{i+1} &= 1 - rx_i^2 + y_i \\ y_{i+1} &= bx_i, \quad i = 0, 1, 2, \ldots \end{aligned} \tag{1}$$

The Hénon Chaotic map is a basic two-dimensional chaotic map that exhibits quadratic nonlinearity. It is based on two parameters, r and b, with r = 1.4 and b = 0.3 in the standard Hénon Chaotic map. Figure 1a depicts the Hénon Chaotic map as chaotic behavior within the range of [1.5, 2.3] for its canonical values. However, it behaves periodically outside

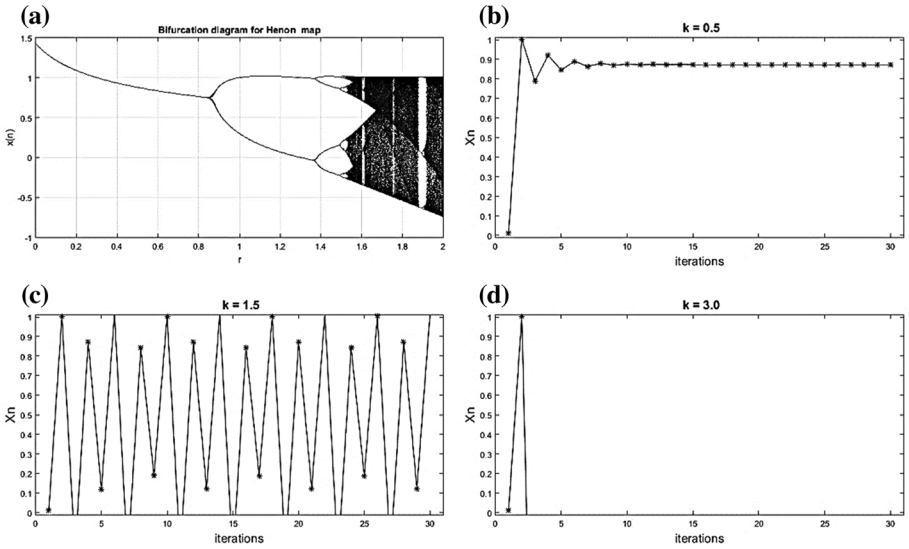


Fig. 1 Analysis of Hénon chaotic map, **a** The bifurcation diagram of Henan chaotic for r∈[0, 2, 1] and b = 0.3, **b** Iteration property for r = 0.5, **c** Iteration property for r = 1.99, **d** Iteration property for r = 2.5

this range or converges to a constant value. Meanwhile, Figs. 1b, c, d demonstrate how the Iteration property of the Hénon Chaotic map's behavior is affected by the value of r. The initial value and the parameter r heavily influence the Hénon strange attractor's behaviour.

The Hénon map was the first to exhibit a strange attractor with a fractal structure. The Hénon map's simplicity makes it suitable for numerical studies, leading to numerous computer investigations. However, there is still much to discover regarding all possible bifurcations when altering the parameters r and b. The Hénon chaotic map utilizes two variables for image encryption, with the encryption process involving three steps of operations [26]:

Step 1 The chaotic system of Hénon may be decomposed into a succession of one-dimensional chaotic maps. The one-dimensional Hénon chaotic map is defined as follows:

$$x_{i+2} = 1 - rx_{i+1}^2 + bx_i \tag{2}$$

where b = 0.3 and r = [1.07, 1.4]. The parameters *r, b*, starting value × 0, and initial value x_1 might represent the key.

Step 2 To modify the pixel values of an image, we utilize a Hénon chaotic map. The first step involves obtaining the map through Eq. (2). Following this, a transformation matrix is generated for the pixel values.

Step 3 The XOR operation will be performed bit by bit between the transformation matrix of pixel values and the pixel values of the picture. The end result will be a cypher picture. b = 0.3, r = 1.4, × 0 = 0.01 and × 1 = 0.02 are the parameters used.

2.2 The Proposed DHCM

We have created a DHCM with a chaotic function suitable for cryptographic applications. This map is written as follows:

$$x_{i+1} = \left(r \times x_i + y_i\right) \bmod 1$$
$$y_{i+1} = \frac{b}{1-x}, \quad i = 0, 1, 2 \tag{3}$$

Behavior analysis in Fig. 2 illustrates that the proposed DHCM has significantly broadened the range of the parameter r, encompassing an extensive chaotically spectrum of values from 0 to infinity (∞). This increase in available chaotic values of parameter r has made it suitable for encryption purposes. Thus, the proposed DHCM can use any variable r value as part of the encryption key.

3 A Proposed CBRS Encryption Algorithm Based on the DHCM

The proposed CBRS encryption method, as illustrated in Fig. 3, is an image encryption technique that employs the proposed DHCM. This algorithm is divided into two sections that use both confusion and diffusion approaches [27]. The algorithm's confusion part entails employing the suggested DHCM to mix the locations of the pixels inside the picture.

The proposed DHCM is utilized by the diffusion algorithm to encrypt an image, resulting in a shuffled image. The cryptosystems of this algorithm meet the high-security performance standards required to satisfy the classic Shannon principles of confusion and diffusion. The CBRS encryption algorithm has been implemented in three modes of operation, namely, Cipher Block Chaining (CBC) mode, Cipher Feedback (CFB) mode, and Output Feedback (OFB) mode. These modes have been tested across different block sizes (W_1, W_2, and W_3) using the proposed CBRS algorithm.

According to the proposed algorithm, the authentication process for the current user or entry is explained in two scenarios. Once the person authenticates, their encrypted

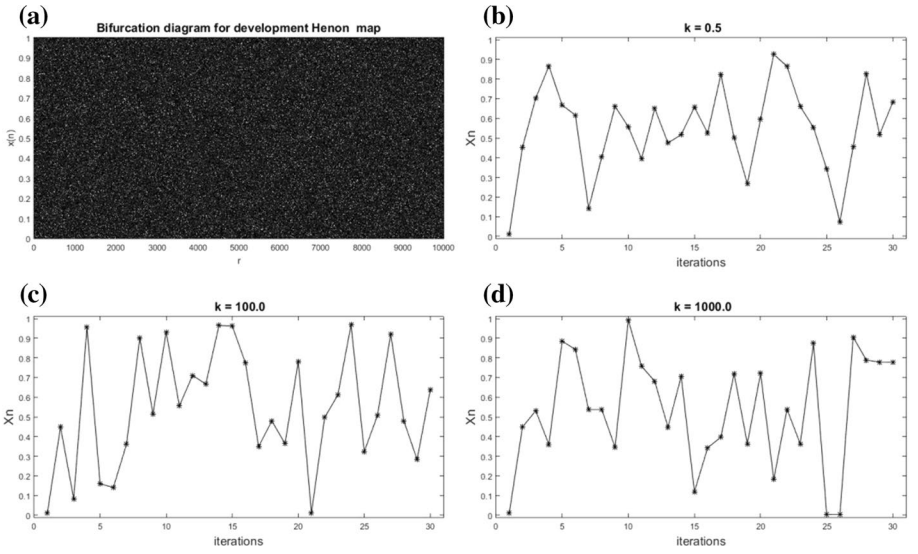


Fig. 2 Behavior analysis of the proposed DHCM, **a** The bifurcation diagram, **b** Iteration property r = 0.9 for r [0,103], **c** Iteration property r = 20, and **d** Iteration property r = 10,000 for r [0,10^6]

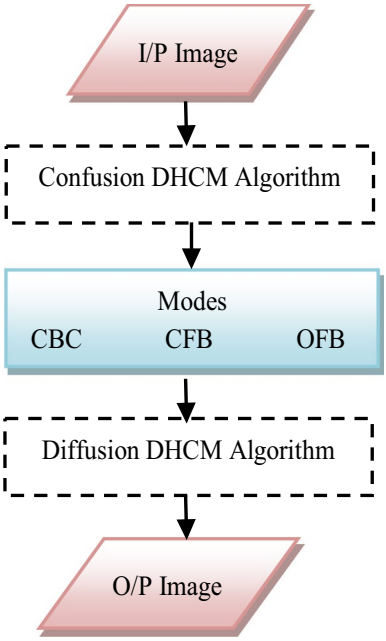


Fig. 3 A proposed CBRS encryption algorithm based on the DHCM

distortion template is highly correlated with the one saved in the database. Another strategy involves authenticating the encrypted template of the imposter user who has the lowest correlation score. During the authentication process, a simulated noise attack is added to the input biometric template to replicate the actions of an imposter user. The noise variance can change due to various factors, such as the sensor's thermal effect or environmental changes like light and clouds. These noises are represented as Gaussian noise that varies multiplicatively.

4 Encryption Evaluation Metrics and Experimental Results

The results obtained by the proposed DHCM encryption algorithm were compared with those of other encryption algorithms. In addition, some security evaluations in terms of number of pixels change rate (NPCR), unified average changing intensity (UACI), and entropy metrics are presented for the proposed DHCM. Only one sample from the biometric databases is used to validate the DHCM-based cancelable biometric system. Different performance metrics are evaluated to validate the proposed cancelable biometric system. In addition to visual inspection, we consider various factors like processing time, correlation coefficients, and histogram analysis ROC. In the following sub-sections, the simulation outcomes of different authentication evaluation metrics are obtained to measure the efficiency of the proposed biometric security system. The results were obtained by analyzing 512×512 grayscale biometric images using MATLAB software. Finally, based on prior research on symmetric encryption algorithms, the proposed cancelable biometric security system utilizing DHCM is superior.

4.1 Security and Statistical Analysis

To examine the simulation outcome, we utilize MATLAB environment simulation. Various measures are used to analyze the amount of encryption objectively. Figure 4 shows the encrypted photos of Lena generated by the proposed technique for multiple blocks. We implemented the proposed model with three alternative W (block size) values, with the initialization vector, and (IV) was a part of the encrypted Cameraman picture. Where: W_1, W_2 and W_3 have a resolution of 128×128 pixels, 64×64 pixels and 32×32 pixels respectively. We calculate the Histogram of all images, the correlation coefficient (CC) between the original image and the cypher image, as well as the maximum deviation factor (MDF) and irregular deviation factor (IDF) to evaluate the effectiveness of encryption and its resistance to statistical attacks.

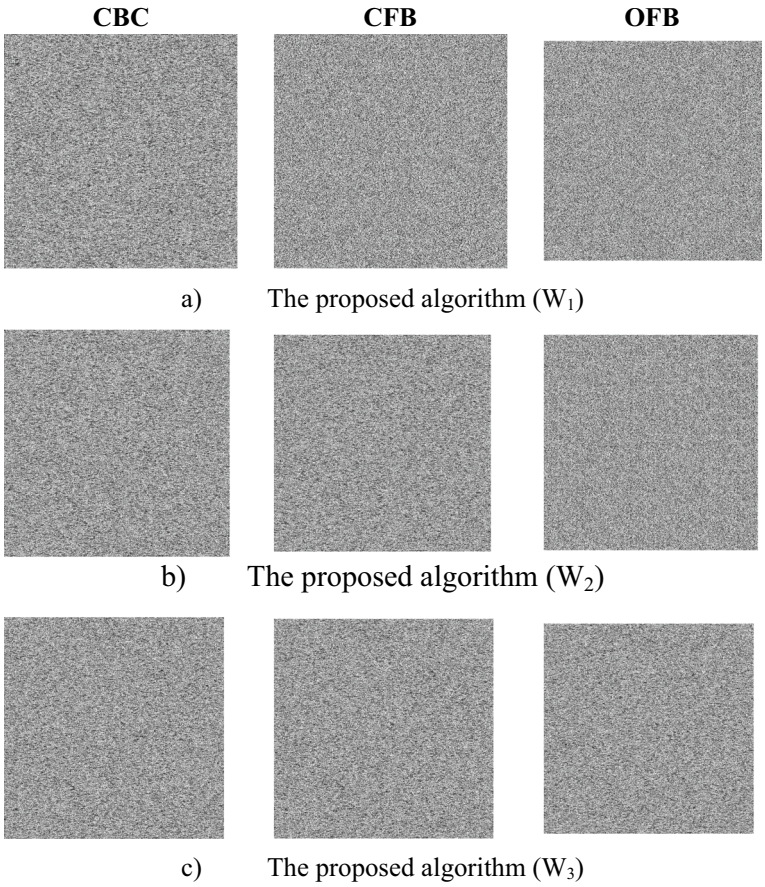


Fig. 4 The encrypted image in each mode of operation with distinct blocks using the suggested technique

4.1.1 Histogram Analysis

In the image analysis, Fig. 5 presents the original Lena.bmp image with a size of 512×512 pixels. Meanwhile, the Figure showcases the corresponding Histogram. In Fig. 6, we can see the Histogram of encrypted images created by our algorithm in different modes of operation. It is clear that the histograms demonstrate a consistent and even distribution across various block sizes and modes of operation, indicating the success of our proposed method. The resulting image differs significantly from the original due to the influence of other modes of operation as well as the dispersion induced by our suggested Hénon chaotic map. Among these types of operation is the employment of a chaotic cryptosystem rather than depending simply on the chaotic Hénon map. Figure 7 presents a detailed analysis of various original images and their encrypted biometric data.

Figure 7 illustrates the ciphered templates of the examined biometric database samples with the proposed model applied to the different images for the used database. It is noticeable that the proposed algorithm succeeds in hiding the details of the ciphered image compared to the original image. The Histogram reflects the distribution of pixel levels in the picture. It should be as uniform as possible for high-quality encryption. Histograms of encrypted images with the proposed and traditional encryption algorithms are shown in Fig. 7. It is observed that the templates obtained with the proposed encryption algorithm have more uniform histograms.

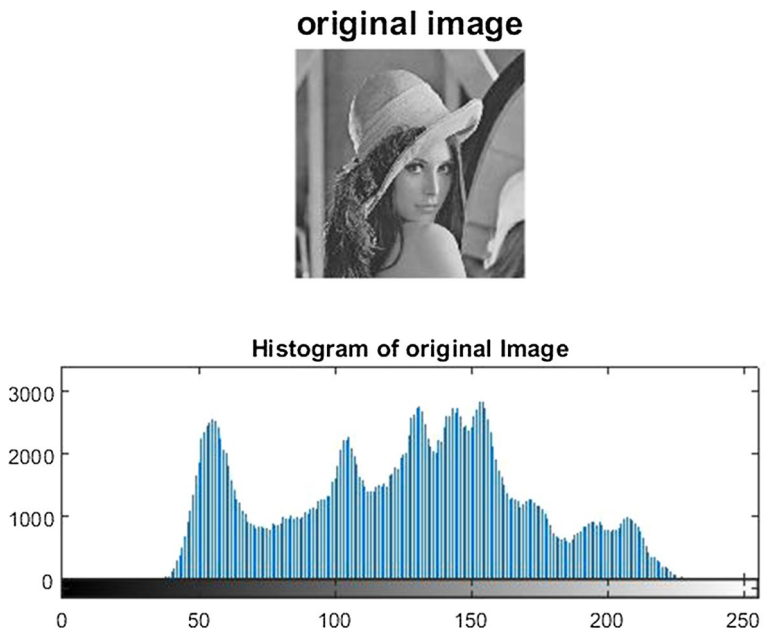


Fig. 5 The Histogram of the original image

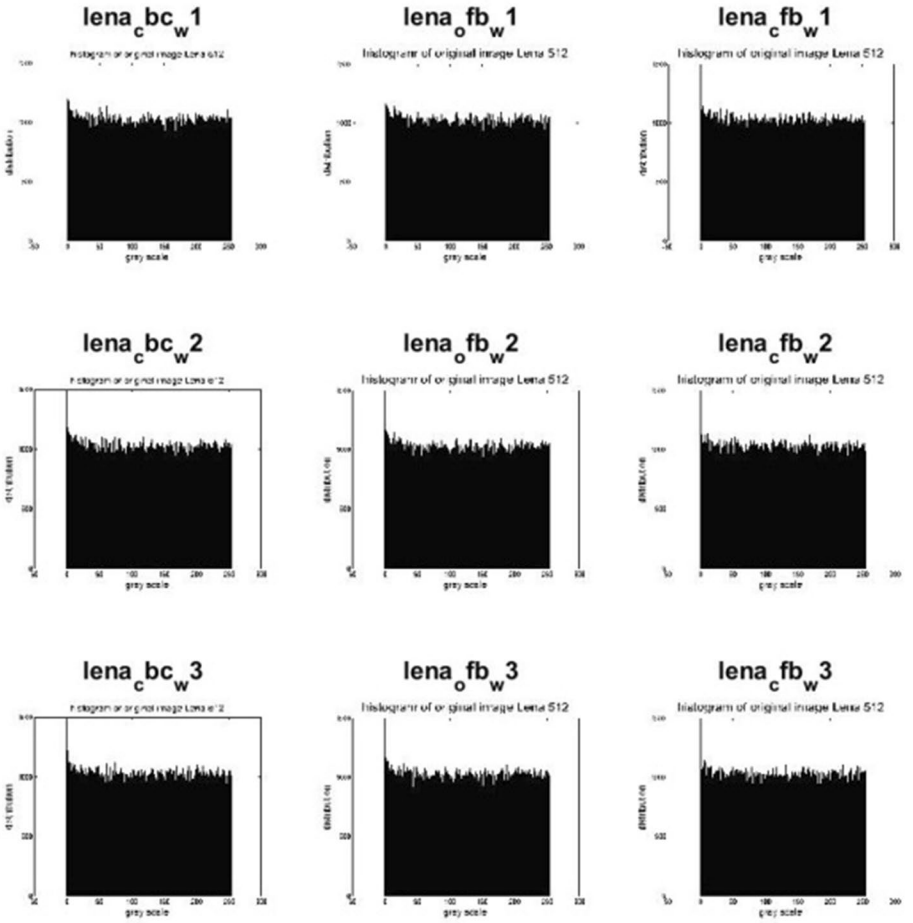


Fig. 6 The Histogram of the encrypted image using the proposed algorithm in three modes of operation with different block sizes ($W_1 \ldots W_3$)

4.1.2 Entropy Analysis

The degree of randomness of encrypted templates is estimated with entropy. The smallest entropy value is zero, while the optimum value is 8. Thus, the higher the entropy, the more uniform the image distribution is. Therefore, an efficient cryptosystem must offer an information entropy up to or close to 8.

4.1.3 Correlation Coefficient Analysis

If the encrypted image looks identical to the original image and the encryption method fails to conceal the original image's information, the encryption process is considered a failure. The CC between the two would be one, indicating a high level of dependence.

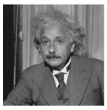
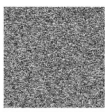
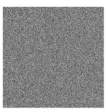
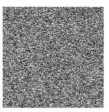
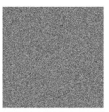
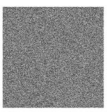
Original images						
Entropy of originals	6.8738	7.3479	7.1390	7.5245	7.4934	7.0818
Histogram of the original images						
Encrypted images						
Entropy of encrypted	7.9969	7.9993	7.9991	7.9960	7.9992	7.9993
The encrypted images' histogram						

Fig. 7 Original and encrypted biometric histogram analysis and entropy

When the CC is zero, it shows that the original image and its encryption are not the same. Therefore, a successful encryption process results in smaller CC values. The CC is measured by a specific method:

$$\varsigma_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{4}$$

$$\operatorname{cov}(x, y) = \frac{1}{L}\sum_{l=1}^{L}\left(x_l - E(x)\right)\left(y_l - E(y)\right) \tag{5}$$

where L is the number of pixels involved in the computations, the quality of the encryption technique is determined by how near the value is to zero. The CC between the original picture and the encrypted image produced by our proposed CBRS algorithm with different modes of operation and block sizes ($W_1 \ldots W_4$) is shown in Table 1. Because fewer XOR operations are required in any mode of operation with a bigger block size, the CC lowers as the block size grows. The link between block size and CC must be considered.

Table 1 The ς_{xy} between original and encrypted images generated using the proposed CBRS algorithm

Mode of operation	W_1	W_2	W_3	W_4
CBC	0	0.0002	0.0008	0.0044
CFB	0	0.0018	0	0.0041
OFB	0	0.0006	0.0011	0.0034

4.1.4 MDF Analysis

The MDF metric is used to evaluate the efficacy of encryption in preserving image quality. This metric can be computed using the following formula [28]:

$$D_H = \frac{\left(\frac{d_0+d_{255}}{2} + \sum_{i=1}^{254} d_i\right)}{M \times N} \tag{6}$$

To encrypt an image, D_H (Difference Histogram) values are determined by calculating the amplitude of the absolute difference curve at a grey level I while considering the image's dimensions, represented by M and N. When the D_H value is higher, it signifies that the encrypted image has better quality. In Table 2, the MDF measurement factor for encrypted images is displayed. Based on the results, it is apparent that employing CBC mode with W_3 outperformed OFB mode with W_2. In comparison to the other modes, the CFB mode with W_4 produced the worst results. Notably, CBC with W_3 had the best results.

4.1.5 IDF Analysis

This analysis concentrates on the impact of encryption on the encrypted image's IDF. To compute this variation, we determine the absolute histogram deviations of the mean value using the following method:

$$H_D(i) = \left|H(i) - M_H\right| \tag{7}$$

The irregular deviation D_I is calculated as follows:

$$D_I = \frac{\sum_{i=0}^{255} H_D(i)}{M \times N} \tag{8}$$

Regarding encryption quality, a lower D_I value signifies superior performance [29]. Assessing the quality of image encryption can be done reliably using the IDF metric. When this metric is consistent with other measurements, it strongly indicates encryption quality. In cases of discrepancies between the metrics, the IDF test should be the determining factor for evaluating the encryption algorithm. According to the test, the CFB mode with W_3 with the value 180,296 performs better. However, the CFB mode with W_4 performs the worst among all modes with a value of 181,114.

Table 2 MDF metric of the proposed CBRS algorithm

Mode of operation	W_1	W_2	W_3	W_4
CBC	187,898	187,779	188,346	187,220
CFB	187,973	187,010	187,320	1,878,500
OFB	188,285	188,285	188,100	187,940

4.1.6 NPCR and UACI Analysis

Two additional tests, namely NPCR and UACI, are employed to evaluate the differences between the original and decrypted. The protocol for conducting the tests is strictly followed [30]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \tag{9}$$

When analyzing C_1 and C_2, we consider the width and height of each, which we denote by W and H. To quantify the level of dissimilarity between the two images, we use NPCR, which is calculated as the percentage of differing pixels out of the total number of pixels in C_1 and C_2:

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \tag{10}$$

The encryption quality is determined by the average intensity of discrepancies between two pictures. Higher NPCR and UACI values suggest more robust encryption. In various modes and block sizes, the better value is to use CFB with W_3, which gives a value of 28.6469, but the worst case is to use CBC with W_4, which offers a value of 28.5549. The NPCR between the encrypted and original images in different modes with different block sizes gives better results at 99.61 with the methods at W_1.

4.2 Time Analysis

As part of our analysis, we have also conducted tests on processing time. This refers to the duration required for encrypting or decrypting data. It is worth noting that a shorter processing time results in faster encryption speed. We studied how block size influences the processing time of our encryption approach, which we implemented using CBC, CFB, and OFB modes. The algorithm's completion time is measured from beginning to end. Table 3 indicates the encryption processing time for various modes of operation and block sizes. Based on the data in Table 3, it is possible to conclude that the mode of operation does not affect the processing time. However, a decrease in block size results in an increase in processing time. This is due to the fact that the number of XOR operations necessary for any mode of operation grows as block size decreases.

Table 3 The processing time of the encryption process versus block size measured in seconds

Mode of operation	W_1	W_2	W_3	W_4
CBC	1.13	1.43	2.55	3.11
CFB	1.23	1.69	2.20	3.28
OFB	1.43	1.76	2.13	2.58

4.3 Key Space Analysis

To be considered adequate, an encryption scheme must withstand various attacks. Additionally, it must be responsive to secret keys, and the keyspace should be extensive enough to prevent brute-force attacks. The following sections outline our proposed algorithm's keyspace analysis and testing results.

4.3.1 Exhaustive Key Search

To create a safe picture cryptosystem, the key space must be large enough to prevent brute-force assaults. A thorough key search will need 10 k operations to complete, where k is the key size in bits. A prospective invader may try every conceivable key, which might be a time-consuming operation. The suggested approach for chaotic maps encryption determines the key by the parameters r and b, as well as the beginning values $\times 0$ and $\times 1$. This key sensitivity 10–14 additional parameters p, q of the Arnold cat map, parameter a, denoting the angle of rotation of chaotic maps encryption are used as secret keys. In this situation, the computations will necessitate:

$$T = \frac{10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 255}{1 \times 10^{9} \times 60 \times 60 \times 24 \times 365} = 3.25 * 10^{39} years \tag{11}$$

This task is nearly impossible to accomplish. The keyspace is extensive enough to withstand any attempts at brute-force attacks.

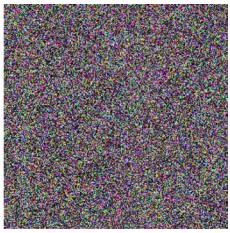
4.3.1.1 Key Sensitivity Analysis A reliable method for encrypting images should prioritize the confidentiality of the secret key. This means that even a minor alteration in the secret key should result in a completely distinct encrypted image. To test the sensitivity of the proposed image encryption using DHCM, we followed these steps:

- In the images presented in Fig. 8a, b, we can see the original and encrypted images, respectively. Our proposed algorithm was applied using the parameter of *DHCM* and the secret key k_1 as: $r = 11$, $b = 0.3$, $x_0 = 0.01$, $x_1 = 0.02$, $p = 1$, $q = 2$, and $R = 10$.
- By slightly modifying the secret key k_2 to become $r = 11$, the same original image is encrypted, as shown in Fig. 8c.
- Additionally, the original image undergoes re-encryption through slight modifications of the secret key k_3, resulting in a new encrypted version as $r = 11.2$, as shown in the Fig. 8d encrypted image.

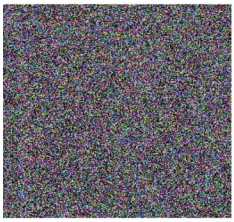
After careful analysis, we have compared three encrypted images. We have displayed the initial image along with the three encrypted versions that were produced. However, it can be challenging to compare these encrypted images by just looking at them. Therefore, we have computed the CC between the corresponding pixels in each of the three encrypted images. The results of this analysis are shown in Fig. 8. Additionally, we have measured the NPCR between the three encrypted images.

According to the output of Fig. 5, there is no discernible relationship between the three encrypted images despite being generated with slightly varying secret keys. Additionally, Fig. 9 displays the outcomes of several decryption efforts on an encrypted image using secret keys that differ somewhat from the one used to encrypt the original image shown

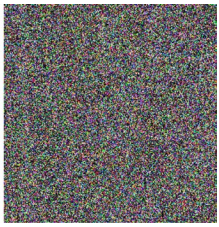
a) Original image



b) Encrypted image-I using key k_1



c) Encrypted image-II using key k_2



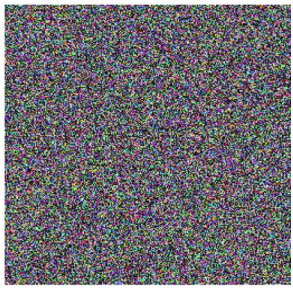
d) Encrypted image-III using key k_3

Fig. 8 The key sensitive result using the proposed Hénon chaotic map

a) Original image

b) Encrypted image using k_1

c) Decrypted image using k_1



d) Decrypted image using k_2

Fig. 9 Effect of the Key sensitive analysis on Decryption by using Hénon chaotic map

in Fig. 9a. Figure 9b illustrates the original and encrypted images. It is evident from the photos post-decryption that utilizing a slightly different key for decryption results in failure to reproduce the original image. This emphasises the necessity for secure image cryptosystems with high key sensitivity, where the cypher image cannot be decrypted accurately. It is worth noting that the encryption and decryption keys differ only slightly, yet even a minor difference in the key leads to complete failure in decryption. Therefore, the suggested image encryption method is highly key-sensitive.

4.4 ROC and Comparison with Other Recent Studies

The proposed cancelable biometric system based on DHCM has been compared with the related studies in CC, NPCR, UACR, Entropy, and Receiver Operating Characteristic (ROC) have been considered in this comparison. The used biometric traits are ciphered by the DHCM encryption-based cancelable biometric system and compared to the results of the recent encryption algorithms. In addition, we evaluate the security performance analysis in terms of ROC. Validation of a DHCM encryption-based cancelable biometric system is introduced by examining simulation outcomes of different biometric database samples. Different performance metrics were utilized to validate the proposed model-based cancelable biometric system.

Table 4 displays the CC difference between the original and encrypted images, together with the UACI metric, which measures the average difference in intensity between an original and encrypted image. In contrast, the NPCR metric counts the number of pixel changes. Entropy, on the other hand, determines the information entropy of the encrypted picture using a process distinct from the encryption method. It is noticed that the entropy values of the cancelable palm print templates encrypted with the proposed algorithm are close to 8 (the optimum value). This proves the high randomness of cancelable templates obtained with the proposed encryption algorithm.

Two other security metrics, namely NPCR and UACI, are employed to prove the effect of one-bit modification in the plain image on the encrypted one. Table 5 illustrates the NPCR and UACI values, which are both near the optimum values. We reached an average value of 99.6564% for NPCR and 33.5535% for UACI. Hence, the cancelable biometric security system is highly sensitive to even minor modifications of the original traits and can resist differential attacks.

Table 4 The encryption evaluation measurements of the encrypted images

Approach	CC	NPCR	UACR	Entropy
Chaotic Baker Map	0.00	99.35	20.77	7.4379
RC6	0	99.62	28.20	7.9978
Hènon map	0	28.55	99.6418	7.9992
Algorithm-1[31]	0.002	99.26	24.268	7.2561
Algorithm-2 [32]	0.0042	.9956	33.6	7.3661
System based on DRPE algorithm [33]	0.0004	99.41	26.41	7.7295
System based on OSH algorithm [33]	0.0045	98.16	15.54	7.7612
System based on RNA-GA algorithm [33]	0.0002	99.61	33.45	7.9956
Proposed algorithm	0.00013	99.65	33.55	7.9992

Table 5 Comparative analysis of the proposed algorithm

Approach	AROC
Proposed	0.9999
Model [32]	0.9999
Soliman et al. [34]	0.8630
El-Hameed et al. [35]	0.7187
Ibrahim et al. [36]	0.8837
Ratha et al. [37]	0.8738
Kaur and Khanna [38]	0.8684

The proposed algorithm provides high degrees of confusion and diffusion in the encrypted biometric templates. Several experimental tests have been performed to illustrate the efficacy of the proposed algorithm in generating completely deformed biometric traits. The utilized assessment metrics prove that the proposed algorithm outperforms the related works from the encryption assessment perspective on different types of biometrics. Furthermore, the proposed cancelable biometric recognition system based on the DHCM hybrid encryption algorithm provides high performance.

Based on Table 4, we can conclude that the CC serves as a measuring factor when testing different algorithms. Overall, the algorithms showed a reasonable correlation. Based on our analysis, the proposed CBRS algorithm that utilizes the DHCM outperformed all other algorithms regarding various factors.

The ROC curve is adopted for the performance assessment of biometric systems. In addition, the area under ROC (AROC) is an indicator of the accuracy level of the biometric recognition system. Figure 10 gives the AROC curves for the cancelable biometric recognition systems based on the proposed algorithm. The results reveal higher AROC values with the proposed encryption algorithm. Hence, the cancelable biometric system based on the proposed encryption algorithm is superior to the other methods. The proposed DHCM algorithm provides high performance with AROC with values of 0.9999 compared with further recent research.

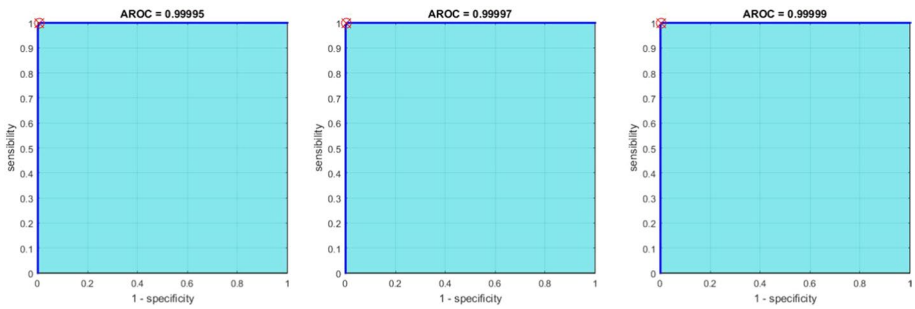


Fig. 10 AROC for 0.01, 0.02 and 0.03 at the third-row noise variance

5 Conclusions

In this paper, a superior technique for cancelable Biometrical recognition was introduced. The process is based on the proposed DHCM. The primary aim of this method is to employ the Hénon chaotic map in biometric data to strengthen biometric security and prevent unauthorized access. In our approach, we guarantee the complete distortion and encryption of the original biometric characteristics to avoid any unauthorized access to the database's stored information. Our approach to securely ciphering and distorting stored biometrics has been thoroughly tested and proven successful through comprehensive investigation tests. Our method is a superior option for securing biometric patterns compared to traditional encryption methods. Furthermore, the suggested approach has proven efficient in encrypting and modifying various biometric datasets, making it suitable for modern access technology and cancelable biometric recognition. The effectiveness of this proposed approach is demonstrated through multiple metrics, including security and statistical analyses. The analysis results indicate high effectiveness, robustness, and reliability, which are shown by excellent performance on various recognition databases. In future work, this proposed method can be added with a fuzzy set to enhance the image due to fuzzy can deal with vague and uncertain information. Moreover, we plan to design multi-level joint crypto chaotic coded techniques that utilize different cancelable biometric concepts. Consequently, wireless communication links will have improved reliability and confidentiality through a modified coded construction with cancelable biometric recognition. Also, we intend to build cancelable biometric recognition systems based on deep feature extraction and feature encryption to allow more robustness.

For future work, we recommend using multi-biometric templates based on hybrid encryption techniques to improve performance and protect biometric pattern storage from assaults. Use a unimodal cancelable biometric system that operates on bio-signals and Empirical Mode Decomposition (EMD) to deconstruct the bio-signals into different Empirical Mode Functions to improve the security and reliability of biometric-based access control.

Author Contributions Software, AHA; Validation, AA; Writing—original draft, THMS; investigation, AA; Supervision, AHA: All authors have read and agreed to the published version of the manuscript.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB).

Data Availability This is not relevant.

Declarations

Conflict of Interests The authors state that they have no conflicts of interest.

References

1. Zheng, J., Zhang, L., Feng, Y., & Wu, Z. (2023). Blockchain-based key management and authentication scheme for IoT networks with chaotic scrambling. *IEEE Transactions on Network Science and Engineering, 10*(1), 178–188.
2. Tamer H. M., Fengfan Y., & Saqib E. (2015). A proposed chaotic-switched turbo coding design and its application for half-duplex relay channel. *Discrete Dynamics in Nature and Society Journal*.
3. Annovazzi-Lodi, V., Lorenzo, L., & Aromataris, G. (2022). Challenge-response authentication scheme with chaotic lasers. *IEEE Journal of Quantum Electronics, 58*(1), 1–7.
4. Cui, J., Yu, J., Zhong, H., & Liu, L. (2023). Chaotic map-based authentication scheme using physical unclonable function for internet of autonomous vehicle. *IEEE Transactions on Intelligent Transportation Systems, 24*(3), 3167–3181.
5. Soliman, T., Yang, F. & Ejaz, S. (2015). A polar coding scheme for secure data transmission based on 1D chaotic-map. In: *Proceedings of International Conference on Computer Information Systems and Industrial Applications*.
6. Karabacak, M., Peköz, B., & Arslan, H. (2021). Arraymetrics: Authentication through chaotic antenna array geometries. *IEEE Communications Letters, 25*(6), 1801–1804.
7. Gurjit, S. W., et al. (2019). Adaptive weighted graph approach to generate multimodal cancelable biometric templates. *IEEE Transactions on Information Forensics and Security, 15*, 1945–1958.
8. Mohamed, H., Yashu, L., & Kuanquan, W. (2019). Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. *IEEE Access Journal, 7*, 26527–26542.
9. Eltaieb, R. A., et al. (2023). Efficient implementation of cancelable face recognition based on elliptic curve encryption. *Optical and Quantum Electronics, 55*(9), 841.
10. Masood, F., et al. (2022). A lightweight chaos-based medical image encryption scheme using random shuling and XOR operations. *Wireless Personal Communications Journal, 127*(3), 1405–1432.
11. El-Hameed, H. A. (2022). Cancelable biometric security system based on advanced chaotic maps. *The Visual Computer, 38*(6), 2171–2187.
12. Alarifi, A., Amoon, M., Aly, M. H., & El-Shafai, W. (2020). Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system. *IEEE Access, 8*, 221246–221268.
13. Kaur, H., & Khanna, P. (2018). Random distance method for generating unimodal and multimodal cancelable biometric features. *IEEE Transactions on Information Forensics and Security, 14*(3), 709–719.
14. Jin, Z., Hwang, J. Y., Lai, Y.-L., Kim, S., & Teoh, A. B. J. (2018). Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing. *IEEE Transactions on Information Forensics Security, 13*(2), 393–407.
15. Kaur, H., & Khanna, P. (2020). Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing. *Future Generation Computer Systems, 102*, 30–41.
16. Zhong, D., Shao, H., & Du, X. (2019). A hand-based multi-biometrics via deep hashing network and biometric graph matching. *IEEE Transactions on Information Forensics and Security, 14*(12), 3140–3150.
17. Murakami, T., et al. (2019). Cancelable permutation-based indexing for secure and efficient biometric identification. *IEEE Access, 14*(12), 45563–45582.
18. Hua, Z., Zhou, Y., & Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. *Information Sciences, 480*, 403–419.
19. Mursi, M. F. M., Hossam, E. H., Ahmed, F. E., El-samie, A., & Abd-El-aziemd, A. H. (2014). A new image encryption scheme based on multiple chaotic systems in different modes of operation. *Advances in Information Science and Applications, 2*, 487–496.
20. Patro, K. A. K., & Acharya, B. (2019). An efficient colour image encryption scheme based on 1D chaotic maps. *Journal of Information Security and Application, 46*, 23–41.
21. Xian, Y., & Wang, X. (2021). Fractal sorting matrix and its application on chaotic image encryption. *Information Sciences, 547*, 1154–1169.
22. Mursi, M. F., Ahmed, H. E. H., Abd El-Samie, F. E., & Abd El-Aziem, A. H. (2014). Image encryption based on development of Hénon chaotic maps using fractional fourier transform. *International Journal of Strategic Information Technology and Applications, 5*(3), 62–77.
23. Amira, G., Noha, O., & El-Khamy, S. E. (2021). New DNA coded fuzzy based (DNAFZ) S-boxes: Application to robust image encryption using hyper chaotic maps. *IEEE Access, 9*, 14284–14305.

24. Abdullah, Q., et al. (2020). Chaos-based confusion and diffusion of image pixels using dynamic substitution. *IEEE Access, 8*, 140876–140895.
25. Zaid, A., et al. (2022). Provably secure and fast color image encryption algorithm based on S-boxes and hyperchaotic map. *IEEE Access, 10*, 26257–26270.
26. Yiqun, Z., et al. (2022). Security enhancement in coherent OFDM optical transmission with chaotic three-dimensional constellation scrambling. *Journal of Lightwave Technology, 40*(12), 3749–3760.
27. Carlos E., Daniel P., Cecilio P. (2021) One-dimensional pseudo-chaotic sequences based on the discrete Arnold's Cat Map Over Z_3^m. IEEE Transactions on Circuits and Systems II: Express Briefs 68(1): 491-495.
28. Wenying, W., et al. (2021). Visual quality assessment for perceptually encrypted light field images. *IEEE Transactions on Circuits and Systems for Video Technology, 31*(7), 2522–2534.
29. Pauline, P., & William, P. (2021). CFB-then-ECB mode-based image encryption for an efficient correction of noisy encrypted images. *IEEE Transactions on Circuits and Systems for Video Technology, 31*(9), 3338–3351.
30. Janani, T., & Brindha, M. (2022). Secure similar image matching (SESIM): An improved privacy preserving image retrieval protocol over encrypted cloud database. *IEEE Transactions on Multimedia, 24*, 3794–3806.
31. Ahmed, S., et al. (2023). A cancelable biometric system based on deep style transfer and symmetry check for double-phase user authentication. *Symmetry, 15*(7), 1426.
32. Eltaieb, R. A., et al. (2023). Efficient implementation of cancelable face recognition based on elliptic curve cryptography. *Optical and Quantum Electronics, 55*, 841.
33. Fatma, M., et al. (2022). A cancelable biometric security framework based on RNA encryption and genetic algorithms. *IEEE Access, 10*, 55933–55957.
34. Soliman, N. F., et al. (2021). An efficient GCD-based cancelable biometric algorithm for single and multiple biometrics. *CMC-Computers Materials Continua, 69*(2), 1571–1595.
35. Hameed, El., et al. (2022). Cancelable biometric security system based on advanced chaotic maps. *The Visual Computer, 38*(6), 2171–2187.
36. Ibrahim, S., et al. (2020). Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption. *Multimedia Tools and Applications, 79*(10), 14053–14078.
37. Ratha, N. K., et al. (2007). Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 29*(4), 561–572.
38. Kaur, H., & Khanna, P. (2016). Biometric template protection using cancelable biometrics and visual cryptography technique. *Tools Applications, 75*(23), 16333–16361.

Dr. Ayman H. Abd El-aziem was born in Egypt, on December 5, 1977, He was graduated from military technical college (MTC), Egypt in 2002, received his PhD degree from Shubra faculty of engineering Benha University of in 2015 at Computer system engineering. He is currently lecture stuff member with department od Information System, faculty of infomatin science and computer science , October 6 university, He is co- other about 25 paper in international journal and, His areas of interest are: Chaos theory, Chaos encryption schemes, channel communications and image processing.at image enhancement, image encryption, Operation Research.

Ahmed Abdelhafeez was born in Egypt, on September 1st, 1973. He received his B.Sc. and M.Sc. (by research) degrees in Computer Engineering from Military Technical College and the Faculty of Engineering, Arab Academy for Science and Technology and Maritime Transport - Egypt. His M.Sc. work was on employing AI and machine learning techniques for detecting the effects of cancer on humans. He completed his Ph.D. in 2023 from the Faculty of Engineering, Ain Shams University. He is currently an Assistant Professor researcher at the Department of Artificial Intelligence at Ain Shams University, Cairo - Egypt. His research interests include the areas of artificial/computational intelligence, machine learning, ensemble learning, image processing (mostly medical), pattern recognition, statistical analysis, computational psychology, and evolutionary computation.

Dr. Tamer H.M. Soliman was born in Egypt in 1978. He received the M.Sc. degree in satellite communications from Alexandria University, Alexandria, Egypt, in 2010 and the Ph.D. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2016. Since 2017, he has been a part-time assistant professor at many universities. Since 2016, he has been the Scientific SE in the Area of Information and Communication Technologies and Radar Systems at the Egyptian Technical Research and Development Centre, Alexandria. He is the coordinator of several projects of the R&D Programs of the Radar and Communication Systems. He has authored or co-authored more than 20 papers published in technical journals and conference proceedings. His research interests include digital communications, radar systems, SE, coding, data security, and control.