IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 December 2022, accepted 27 December 2022, date of publication 29 December 2022, date of current version 9 January 2023.

Digital Object Identifier 10.1109/ACCESS.2022.3233321

RESEARCH ARTICLE

Applicable Image Security Based on Computational Genetic Approach and Self-Adaptive Substitution

NAWAL SHALTOUT[1], AHMED A. ABD EL-LATIF[2,3,*], (Senior Member, IEEE), WALEED M. AL-ADROUSY[1], AND SAMIR ELMOUGY[1]

[1]Department of Computer Science, Faculty of Computers and Information, Mansoura University, Mansoura 35516, Egypt
[2]EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[3]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt

Corresponding authors: Nawal Shaltout (nawalshaltout@mans.edu.eg) and Ahmed A. Abd El-Latif (aabdellatif@psu.edu.sa)

ABSTRACT With the emergence of new information technology fields and various usages of internet applications, securing massive amounts and multiple varieties of multimedia data has become a significant challenge. Hence, it is essential to investigate and develop new cryptographic algorithms to ensure the protection and privacy of multimedia data at rest and during transmission through the communication channel while attempting to overcome the limitations of traditional cryptographic methods. This paper suggests a novel image encryption and decryption technique based on a computational genetic approach and self-adaptive chaotic substitution. The proposed encryption method depends mainly on four steps: sequence generation, diffusion, confusion, and optimization. The USC-SIPI image dataset is being utilized to prove the correctness and effectiveness of our approach in defending against different attack types. Furthermore, the proposed technique could be capable of withstanding attacks while achieving an information entropy of 7.999, Number of Pixel Change Rate of 99.62%, and a Unified Average Change in Intensity of 33.54%, respectively. The results of security testing and analysis revealed that our image security method is strongly recommended for modern communications security applications.

INDEX TERMS Image security, chaotic systems, computational methods, genetic algorithm.

I. INTRODUCTION

With the development of the Internet and computer technology, people are using applications and systems in many aspects of their daily life. These applications and systems depend entirely on multimedia data (e.g., texts, images, videos, and audio). Multimedia data carries all kinds of information. This critical information may be private, medical, civil, military, industrial records, or secret messages and is primarily a target of many attacks. Illegal use of data can lead to major problems for users and organizations. Thus, multimedia data must be protected before transmission or distribution over networks.

Various digital images and information formats, like color, gray, binary, and medical images, have been used and transmitted in the last few years. Text data is not the same as digital image data. Although many encrypting algorithms have been created and widely applied using text or binary data, such as AES, RSA, or IDEA, it is difficult to apply them to secure multimedia data, especially digital images [1], [2]. Traditional algorithms are not directly used in image encryption due to digital image attributes such as increased redundancy, large volumes, and strong association of multimedia content [3], [4], [5], [6].

For example, a woman's dark hair image is encrypted directly using the AES algorithm [7]. An encrypted image is intelligible to some extent because the image's adjacent pixels have a close relationship. This relation cannot be removed by the AES algorithm [7]. Therefore, new multimedia data encryption techniques must be studied for efficient security technology in applicable data transmission scenarios. Accordingly, scientists have tended to improve the

The associate editor coordinating the review of this manuscript and approving it for publication was Shuangqing Wei.

traditional algorithms or invent new efficient methods for image encryption.

Several different types of multimedia encryption techniques based on various technologies have been suggested, including the following: 1- Chaos-Based Image Encryption (CBIE) system [7], [8] has two parts: a chaotic system and image encryption. One-dimensional and multidimensional maps are examples of chaotic systems. 2-Transformation methods include Zigzag Transformation (ZT) [9], [10] and Chaotic Matrix Transform (CMT) [11]. 3- Artificial Intelligence includes optimization and heuristic search algorithms (Genetic Algorithm (GA)). These methods are applied through different stages in our work.

Generally, CBIE has more robust advantages compared with traditional methods. CBIE involves two parts: the encryption process and the chaotic method. Confusion and diffusion are two steps in the encryption process. The confusion phase seeks to change the position of image pixels, whereas the diffusion stage aims to affect the image pixel values. Any image encryption algorithm follows these steps. It also needs pseudorandom sequences as a secret key to apply these steps. There are different mechanisms to generate sequences, such as chaotic system mechanisms. Chaotic system characteristics make it very suitable for image encryption techniques. Some of these characteristics are highly sensitive to fundamental values and parameters, no periodicity, pseudorandom behavior, ease of implementation, and the merging property [12], [13].

Most chaotic maps used in image cryptography can be categorized into One-Dimension (1D), Two-Dimension (2D), Three-Dimension (3D), or Multi-Dimension (MD).

One-Dimension (1D) chaotic maps have an uncomplicated structure that is considered simple to implement. There are three types of 1D chaotic maps: logistic, sine, and tent [13]. However, they also have three defects: 1) Their chaotic range is restricted, 2) they have few parameters, and 3) their results are predictable and cost little to compute.

Two-Dimension (2D) chaotic maps have two parameters. It can produce two sequences, such as the Henon map [14], the Baker map [15], and the Arnold cat map [15], [16].

Three-Dimension or MD Chaotic Maps simulate the evolution of two or more variables. MD chaotic maps have superior chaotic performance than 1-D chaotic maps and are more challenging to predict chaotic orbits.

Several MD chaotic systems have been presented using existing 1D chaotic systems (or maps), or novel chaotic maps are generated in the encryption stage.

As we discussed, many image encryption techniques were introduced to keep digital images secure. However, many of these techniques did not provide optimal results. This drawback motivates many researchers to integrate optimization algorithms with these common techniques. The most common optimization algorithms are GA, which is used for optimization and in confusion and diffusion operations.

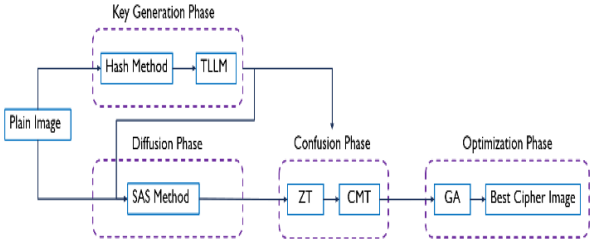


FIGURE 1. Architecture of suggested technique.

Consequently, we design a new applicable security mechanism for image encryption and decryption. The following points highlight its main contributions:

- The secret key is generated by combining Tent-Logistic [12] and Lorenz system (TLLM) [6].
- Develop encryption and decryption methods.
- CMT is used to overcome the defects of ZT.
- ZT and CMT are used to change image pixel position at the confusion stage.
- The proposed Self-Adaptive-Substitution (SAS) method is used to change image pixel values in the diffusion stage.
- GA is used to optimize encrypted images and to determine the best-encrypted image with a low coefficient correlation between image pixels.

The remaining portion of this paper is presented in the following sections. The second section discusses the background information on ZT, CMT, SAS, the GA operation, and related works. In Section 3, the suggested technique is introduced. Section 4 discusses the simulations and results, as well as comparisons to other works of literature. In Section 5, the conclusion and recommendations for further research are presented.

II. PRELIMINARIES AND LITERATURE REVIEWS

This section provides background information and literature reviews on different techniques and the essential components of our suggested method. These components involve chaotic systems such as tent-logistic and Lorenz maps, SAS, ZT, CMT, and GA. The architecture of the recommended technique is visualized in **Fig. (1),** which shows how these components are connected.

A. CHAOTIC MAPS

Chaotic maps produce random sequences. One of the most crucial chaotic map characteristics is a high sensitivity to the initial value. It indicates that if any small change is made to the parameters or the initial value, a new sequence is created, and a sharp change appears in the result. So, chaotic systems are more robust, nonpredictable, and effective. 1D maps and MD maps are the two types of chaotic maps. MD maps have been proposed using existing 1D chaotic maps or using 2D maps like the Henon map [13], [14], Arnold's cat map [15], [16], and Lorenz map [6], [29], [30], [31]. Based

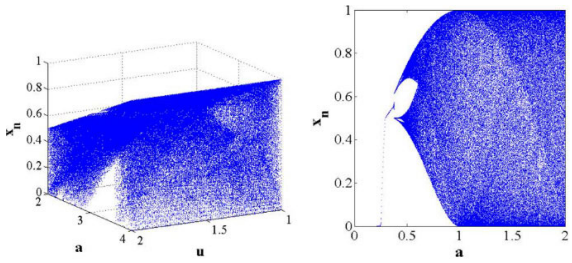


FIGURE 2. Bifurcation diagrams of tent-logistic [13].

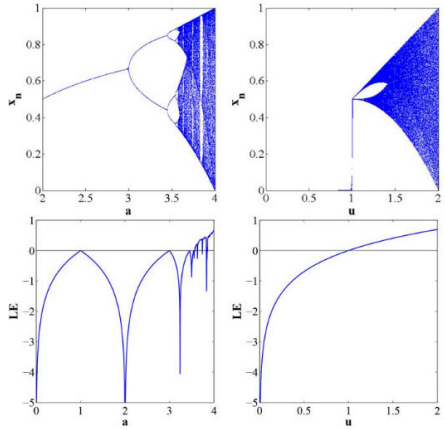


FIGURE 3. Lyapunov exponents of logistic map and bifurcation diagrams [13].

on a Tent-Logistic map [12] and a Lorenz map [6], [31], our suggested technique generates a novel hyperchaotic map (TLLM).

1) TENT-LOGISTIC MAP (TLM)

TLM comprises two 1D chaotic maps (logistic map and Tent map). Mathematically, TLM is stated as follows:

$$X_{n\pm1} = \begin{cases} auX_n\,(1-uX_n) & \text{for} X_n < 0.5 \\ au\,(1-X_n)\,(1-u\,(1-X_n)) & \text{for} X_n \geq 0.5 \end{cases} \tag{1}$$

where a and u are the logistic and tent map parameters, respectively. Parameter a has a range of [0,4], and the logistic map exhibits chaotic behavior when a ∈ [3.57, 4]. Also, u ∈ [0, 2] and the tent map behaves chaotically when u ∈ [1], [2], as shown in **Figs. (2),** and **(3).**

After combining tent and logistic maps, their performance is enhanced, and chaotic ranges become wider along with a and u parameters, as shown in **Fig. (3)** [12].

2) LORENZ MAP (LM)

The 3D Lorenz map has a complex structure in which it is defined as [6]:

$$\begin{aligned} \dot{X} &= a(y-x) \\ \dot{Y} &= (b-z)\,x - y \\ \dot{Z} &= xy - cz \end{aligned} \tag{2}$$

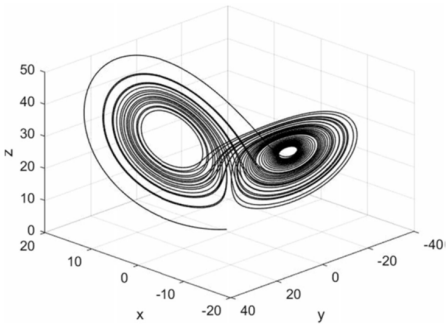


FIGURE 4. Chaotic attractor of Lorenz system [6].

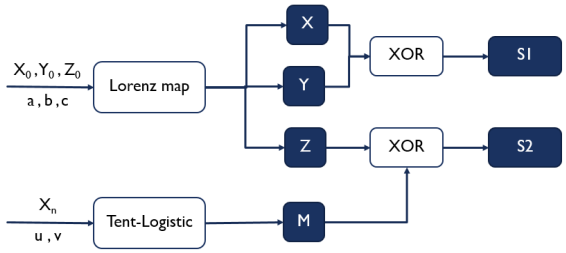


FIGURE 5. TLLM structure.

where the parameters are a, b, and c, and the initial values are x, y, and z. The Lorenz map has a dynamic behavior when a =10, b ∈ [28], [90], and c = 8/3, as shown in **Fig. (4)** [6].

3) NEW 2D DISCRETE CHAOTIC SEQUENCE

When image encryption only depends on ID chaotic maps, the key space is minimal and becomes easy to predict. Also, their chaotic ranges are limited. On the other hand, the original Lorenz system has limitations in terms of ergodicity, dimension, unpredictability, and complexity [21]. Hence, various studies have refined or modified the original Lorenz system to increase its performance [33], [34], [35].

To overcome these problems, TLM is combined with the Lorenz map, increasing the chaotic map's control parameters, which are obtained by preforming the XOR function between the 2D Tent-Logistic Map and the 3D Lorenz Map (TLLM). TLLM is described as shown in **Fig. (5).**

In Figure 5, X_0, Y_0, and Z_0 are initial values, and a, b, and c are the parameters of the Lorenz map. Also, X_n is the initial value, and u and v are the parameters of the Tent-Logistic map.

B. SELF-ADAPTIVE SUBSTITUTION (SAS)

SAS is an essential phase in the image encryption methodology. Furthermore, the primary purpose of the diffusion phase is to alter image pixel values. SAS involves two main methods: A) self-adaptive method. B) substitution method. The basic concept behind self-adaptive is to divide the image into four equal blocks.

First, the original image is checked if it is symmetric or not. If the image is symmetric, the image is split correctly. On the other hand, if the image is asymmetric, we resize it using the nearest interpolation method to make it symmetric. Second,

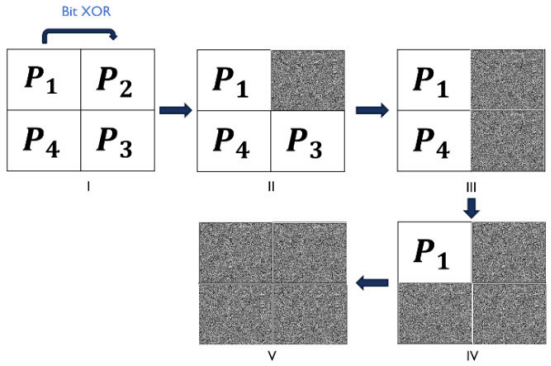


FIGURE 6. SAS method steps.

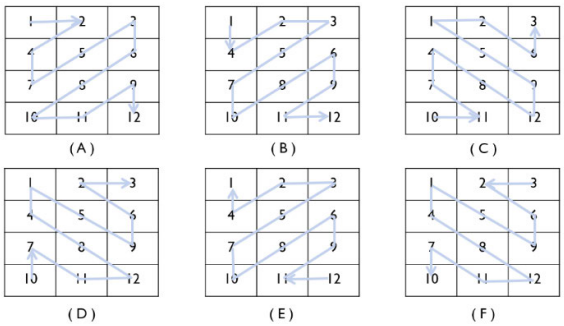


FIGURE 7. Zigzag models [10].

the image is divided into blocks. One block's pixels are used to encrypt another. Then, the encrypted block is utilized to encrypt another block, as shown in **Fig. (6).**

As shown in this figure, the output image is obtained, and it is unintelligible. Afterward, the substitution method diffuses the output image with a chaotic sequence. The substitution process given by Eq. **3** is executed for the cipher image C based on its two previous pixel values and chaotic sequence value. Suppose an output image is converted to 1-D array Q with size L, and Chaotic sequence S with size L is generated using TLLM. Then, for each pixel, the substitution procedure is as follows:

$$\begin{aligned}
&\textbf{if } \mathbf{m} == 1\\
&\mathbf{C(m)} = \mathbf{mod(S(1) + Q(1) + Q(L) + Q(L-1)}, 2^F);\\
&\textbf{elseif } \mathbf{m} == 2\\
&\mathbf{C(m)} = \mathbf{mod(S(2) + Q(2) + C(1) + Q(L)}, 2^F);\\
&\textbf{else}\\
&\mathbf{C(m)} = \mathbf{mod(S(m) + Q(m) + C(m-1) + C(m-2)}, 2^F).
\end{aligned} \tag{3}$$

where F is the intensity scale number in Q and m is the index of cipher image C. For example, if Q contains only binary data, then F equals 2.

C. ZIGZAG TRANSFORMATION (ZT)

ZT is often utilized to scramble the encrypted image pixels. It's a method of scanning image pixels in a zigzag pattern using a specific model. There are eight paths (4 paths with 2 directions each) of zigzag models [9], as shown in **Fig. (7)**, in which we focus on the model (A). According to this model, the image pixels are exchanged starting at the upper left corner of the matrix and ending with the right corner, as shown in **Fig. (8)**. ZT has two drawbacks:1) the periodicity of the transformation. 2) the position of some pixels remains the same [24], [25], [26].

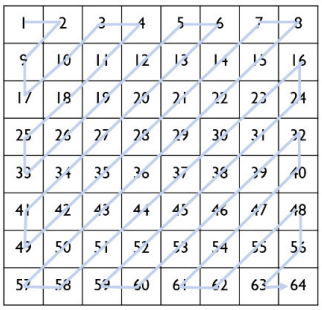


FIGURE 8. Zigzag Transformation [10].

Therefore, this paper improves ZT using the chaotic matrix transform to solve the drawbacks and executing CMT after ZT gives a better confusion effect than executing ZT only.

D. CHAOTIC MATRIX TRANSFORM (CMT)

Because of the high redundancy, large volumes, and strong association between pixels in digital images, new mechanisms for confusion are created to break and reduce these correlations. CMT is one of these mechanisms [11]. It takes a plain image and a chaotic sequence generated by TLLM as input and returns a scrambled matrix as an output. Let P be a plain image, S be a chaotic sequence of size M×N, and C is the scrambled image. CMT steps are as follows:

1- Obtain the sorted matrix, SS, by sorting each column within its values of S.

2- The index matrix I is generated by attaining the row number of each value in SS using Eq. **4**., as shown in **Fig. (9)**.

$$\begin{aligned}
&\mathbf{I(i,\ j) = k\ for\ SS(i,\ j) == S(k,\ j)}\\
&\mathbf{Where\ i,\ j,\ k\ are\ indexes,}\ 1 \le i, k \le M \ \mathbf{and}\ 1\\
&\le j \le N
\end{aligned} \tag{4}$$

3- The new positions for P pixels are defined by connecting pixels with locations in I into a circle. For example, a new pixel location (i,j) = C(I(i,j),j). Then, shift these pixels' m positions to left within circles. This step is defined using Eq. **5**.

$$\begin{aligned}
&C(I(i,j),j)\\
&\quad = P(I(i, mod(j+i-1, N)+1),\\
&\qquad mod(j+i-1, N)+1)
\end{aligned} \tag{5}$$

4- Finally, the scrambled image is obtained.

Therefore, CMT can change pixel positions in a plain image according to the chaotic sequence generated by TLLM.

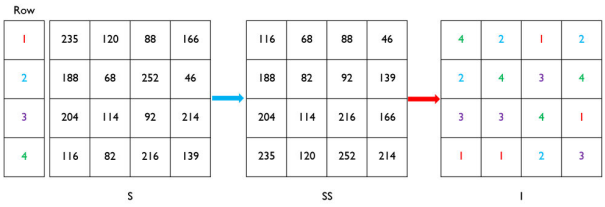


FIGURE 9. Index matrix generation [12].

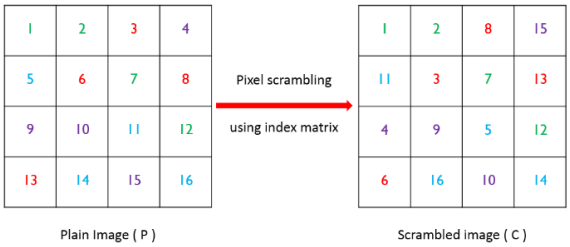


FIGURE 10. Pixel scrambling processes in CMT [12].

Furthermore, pixel positions are changed in both the horizontal direction and vertical direction, unlike other methods

Fig. (9)and **Fig. (10),** show an example of CMT. Fig 9 indicates the index matrix generation from the chaotic sequence. Additionally, Fig 10 specifies scrambled image generation according to the index matrix.

E. GENETIC ALGORITHM (GA)

GA is an effective evolutionary algorithm to solve search and optimization problems and seeks the optimal solution using selection, crossover, and mutation operations. It depends essentially on a population containing a collection of chromosomes. Each chromosome expresses a solution to the problem and consists of a set of genes. [23], [24].

This paper uses GA to obtain the best cipher image with a low correlation coefficient. The correlation coefficient is the most suitable method for selecting best scrambled image. That's because any image has highly correlated adjacent pixels. If the image still has a strong correlation between the pixels, this will make it easier to attack. So, we need to calculate the correlation between pixels and select the best scrambled image with minimum correlation. Therefore, we choose correlation coefficient method as a fitness function for GA.

Thus, the initial population consists of the collection of images. Each solution is an image represented as a one-dimensional array of pixels; each pixel in an image is a chromosome gene.

F. APPLICABLE SCENARIO OF THE PROPOSED CONFIDENTIALITY MECHANISM IN THE CLOUD ENVIRONMENT

Multimedia data is captured and generated from different platforms (e.g., medical devices, PC, mobiles, and finger scanners). The multimedia data is sent from the sender to the receiver through a cloud server, as shown in **Fig. (11)**.

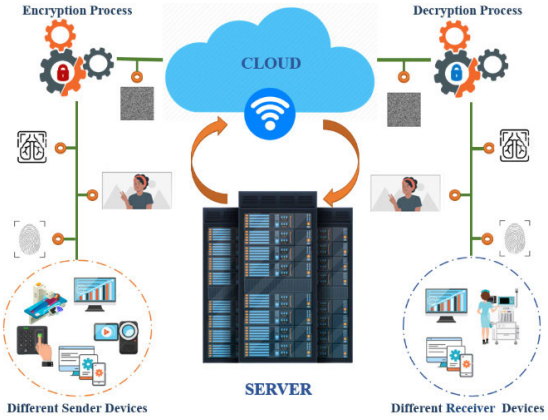


FIGURE 11. Proposed framework for secure data transfers.

We can observe from this figure that the original multimedia data is transformed into encrypted data with the encryption algorithm under the control of the secret key and is saved to the server. This data is also accessible from the server by the receiver. The encrypted data is then decrypted using the decryption algorithm under the control of the same secret key.

Some attacks may be performed to break the system or application and obtain the original multimedia data. So, we work on developing efficient encryption and decryption algorithms that are secure against attacks.

G. LITERATURE REVIEWS

We are going to highlight some of the previous encryption techniques. Zhou et al. [8] introduced an encryption method utilizing a logistic-tent map. This algorithm consists of 5 steps: 1- The random pixel enrollment. 2- Row separation. 3- 1D substitution. 4- Row combination. 5- Image rotation. Experimentation results demonstrated that this method shows effective diffusion property and confusion property. Zhou et al. [12] introduced a common chaotic framework by simulating the structure of cascade in electronic circuits known as the Cascade Chaotic System (CCS). In addition, they proposed a data encryption mechanism based on CCS. Also, they used a chaotic map created via CCS to develop a different Pseudorandom Number Generator (PRNG). The author shows that their suggested framework can provide high-level security for many forms of data while also resisting differential attacks. Hua et al. [11] presented a CMT-IEA image encryption method relying on CMT and 2D-SLMM. They pointed out that their proposed technique can resist attacks and provide high-security protection for various image types. Abbas [16] provided an encryption method for images using 3mixing matrix modification in Independent Component Analysis by the chaotic Arnold's cat map. He showed using his experimentation results that his proposed work enhanced the overall performance of securing encrypting of image. Ghebleh et al. [23] introduced an encryption mechanism by using the approximation of the least square and ID chaotic map. They stated that their proposed approach is an efficient security method and is better

than the compared techniques. Alain et al. [9] introduced a method for scrambling in the plain image. This method relies on pixels position scrambling and pixels value scrambling. The scrambling process is performed using ZT with a new modification. These modifications depend on image color space. The author confirms that the enhanced zigzag has superior performance based on their analysis of the results.

Xingyuan et al. [24] suggested an encryption mechanism that depends on the enhanced ZT and the LL chaotic system. The author shows that their mechanism is efficient and withstands common attacks. Ramasamy et al. [10] presented an encryption method using modified ZT and chaotic maps. Furthermore, they proposed enhancing the logistic chaotic map to a three-dimensional chaotic map. The author signifies that their algorithm is fast, strong, and simple. Zhang et al. [25] introduced an algorithm to encrypt images. This algorithm depends on the Self-confusion technique. Experiment results showed that this work has fast speed and strong security. Allawi [26] introduced a new RGB image scheme to protect images from unauthorized users. This scheme depends on a 1D logistic chaotic map and random number generator. The author indicated that this proposed scheme could resist attacks based on the results of experimentations. Xian et al. [27] introduced a technique to encrypt images. This technique relied on chaotic sub-block scrambling and chaotic digit selection diffusion. The author stated that their technique is more effective and has key sensitivity according to the results of their experimentation. Hanif et al. [28] introduced an approach to encrypting images using (MPWLCM) and (ILM) chaotic maps. Using their results of experimentations, the author indicated that their proposed approach has robust security and could resist varied attacks. Gao and Wang [29] introduced an encryption technique based on enhanced ZT. In order to confuse the image, The zigzag method began at a random point and crossed in both directions. Then, many coupling diffusion cycles were employed to change the pixel value. The authors specified that their method is highly secure and efficient and satisfies image encryption requirements. Qobbi et al. [30] suggested an encryption algorithm using DNA encoding, chaos, and genetic operations. Moreover, the authors revealed that their algorithm is not vulnerable to any known attacks, according to simulations done on many images of varying sizes.

As we discussed, many image encryption techniques were introduced to keep digital images secure. However, many of these techniques did not provide optimal results. This drawback motivates many researchers to integrate optimization algorithms with these common techniques. The most common optimization algorithms are GA. GA is used not only for optimization but also in confusion and diffusion operations. Niu et al. [7] developed an encryption method based mainly on chaotic systems and genetic operations. GA is utilized to enhance the performance of DNA encoding. Based on the outcomes of their experimentation, the authors indicated that their approach is more effective and has high-level security. Wong et al. [31] analyzed the image encryption technique security published by Biswas et al. This technique relies on chaotic maps (logistic tent) and genetic operations. Based on Chen's chaotic map, Logistic-Sine map, and GA, Ghazvini et al. [32] introduced a hyper encryption technique. According to the results, the authors indicated that their approach produces an efficient result on security. Murali et al. [33] introduced a domain-flexible encryption approach using the ortho polynomials transformation method, the chaos system, the genetic methods, and square wave diffusion. According to this technique, Important and irrelevant portions of the original image are separated. A genetic method is employed to encrypt the critical parts. In the domain of the orthogonal polynomial, the insignificant region is shuffled. Then, the square wave technology is utilized to diffuse the cipher image. Using the Lorenz system, quantum GA (QGA), and adaptive diffusion method, Man et al. [34] provided a technique for image encryption.

III. THE PROPOSED TECHNIQUE

This section discusses our suggested technique's two main approaches. Our suggested technique is built on encryption and decryption approaches.

A. ENCRYPTION APPROACH

The encryption technique involves four phases:

1- Sequence (key) generation.
2- Diffusion phase.
3- Confusion phase.
4- Optimization phase using GA.

In the first phase, two sequences (S1 and S2) are generated using the Lorenz map and the Tent-logistic map (TLLM). In the diffusion phase, S1 is used to apply the SAS method to a plain image. The diffused image is scrambled using the ZT method and CMT during the confusion phase. Also, the initial population is generated based on S2, ZT, and CMT. Finally, GA is performed to obtain the best cipher image. **Fig. (12)**represents a flowchart of the suggested technique. The four main steps are presented in the subsections below.

1) SEQUENCE GENERATION

The encryption process depends mainly on secret keys. The key space is the core of key generation. A decent key spacing must be large enough to provide the best protection against all kinds of attacks. The chaotic system has a large space range. So, we use the hyperchaotic system to generate secret keys in the proposed algorithm. These keys (sequences) are generated using equations Eq. (1) and Eq. (2). of TLLM, as shown in **Fig. (5)**. TLLM is used to create sequences for the diffusion phase, which changes the values of pixels, and the confusion phase, which changes the placements of pixels. The initial values for these sequences (S1, S2) are produced using the hash function SHA-256. SHA-256 produces sequence with length 256 bits (b1, b2 . . . b256). The sequence is divided into 6 parts, as shown in **Fig. (13)**. Each part is converted into a

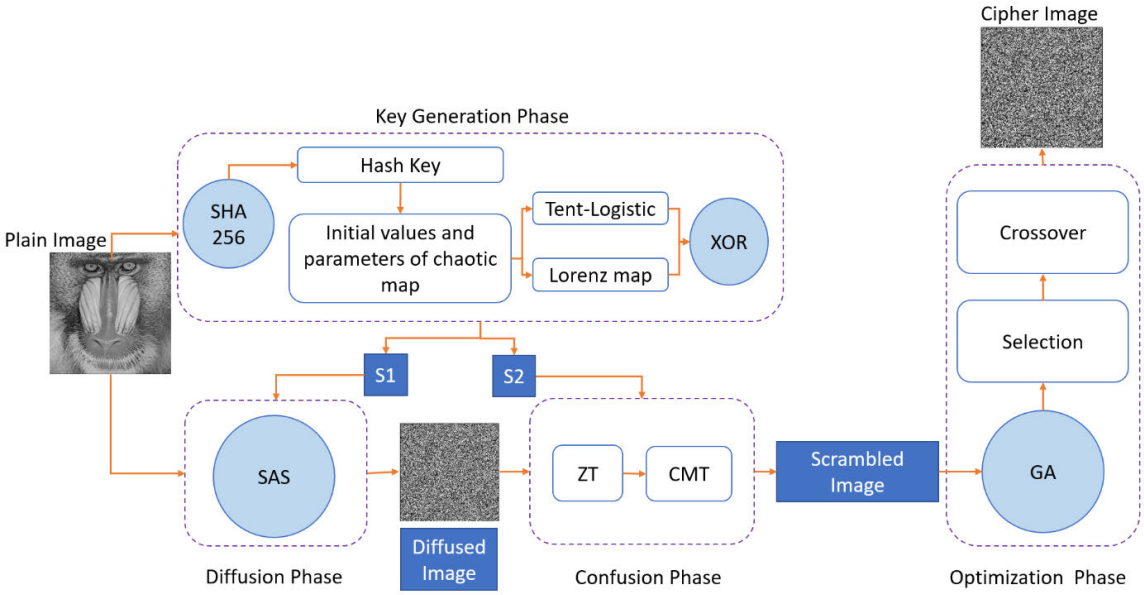


FIGURE 12. Flowchart of The Proposed Technique.

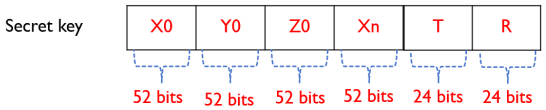


FIGURE 13. Secret key structure.

decimal number using Eq. (6) [11], [35].

$$\mathbf{X} = \frac{\sum_{i=1}^{32} b_i 2^{32-i}}{2^{32}} \tag{6}$$

$$\begin{cases} X_0 = (X_0 + R * T) mod 1 \\ Y_0 = (Y_0 + R * T) mod 1 \\ Z_0 = (Z_0 + R * T) mod 1 \\ X_n = (Z_0 + R * T) mod 1 \end{cases} \tag{7}$$

where b_i is the bit value, and R and T are coefficients derived from K. The initial values and parameters of TLLM are defined by Eq. (**7**). A TLLM method is shown in Algorithm **1.**

2) DIFFUSION PHASE

This phase aims to change pixel values of the plain image using SAS, which was explained previously. Self-adaptive diffusion involves two phases: 1- Self-adaptive XOR blocks. 2- Applying the substitution method with S1 generated from the previous phase on all blocks using Eq. (**3**). Algorithm **2** demonstrates the SAS procedure.

3) CONFUSION PHASE

The main target of this phase is to change the diffused image pixel positions and create the initial population of GA.

Algorithm 1 The Sequence Generation

Input: An original image **P** with **M**×**N** dimensions
Output: The sequences (**S1**, **S2**)

1. Apply **SHA-256 method** to the original image **P** to extract secret key **K** with 256 bits.
2. Divide **K** into **six**parts (X_0, Y_0, Z_0, X_n, **T, R**).
3. Transform each part into **decimal value** using Eq (6).
4. TWO groups of initial values (X_0, Y_0, Z_0) and (X_n) are obtained using Eq (7).
5. **Lorenz map** generates **3** sequences (**X, Y, Z**) using Eq (2) and initial values (X_0, Y_0, Z_0) in step 4.
6. **Tent-Logistic map** generates sequence **(S)** using Eq (1) and initial values (X_n)in step 4.
7. **S1** is generated by **XORing** sequence **X** and sequence **Y.**
8. **S2**is generated by**XORing**sequence**S**and sequence **Z.**

To make that, ZT and CMT are utilized. The image is shuffled using two main steps:

Step 1: Apply the ZT method to the diffused image, as shown in Fig. 9

Step 2: Apply CMT shown in **Fig. (10) and** presented in Algorithm 3 with sequence S2 generated in sequence generation step to ZT result to enhance the performance of ZT.

Step 3: Create the initial population for GA by repeating Steps 1 and 2 many times.

According to the previous steps, the initial population with encrypted images is obtained.

4) THE OPTIMIZATION PHASE

Until now, the plain image is encrypted, and the initial population is created. In this phase, we need to obtain the optimal

Algorithm 2 The Diffusion Phase

Input: An original image **P** with **M**×**N** dimensions and chaotic sequence **S**
Output: The diffused image **D**
IF ***P NOT*** *symmetric*
  P= resize (P, 'nearest')
1 Divide plain image **P** into **4** blocks (P_1, P_2, P_3, P_4) as shown in **Fig. (6),**
2 Define zero matrix **E** with the same size of **P**
3 Divide **E** into **4** blocks
4 **for** *j=1 to 3* **do**
5 Perform **XOR** operation between block $\boldsymbol{P_j}$ and block $\boldsymbol{P_{jC1}}$ and save the output into $\boldsymbol{E_{jC1}}$, block
6
end
7 Perform **XOR** operation between block $\boldsymbol{E_4}$ and block $\boldsymbol{P_1}$ and save the output into $\boldsymbol{E_1}$ block.
8 The diffused image **D** is obtained by applying substitution method with sequence **S** to **E** matrix using Eq (3)

Algorithm 3 CMT Method

Input: A diffused image **D** and chaotic sequence **S** with the dimensions **M**×**N**
Output: Scrambled image**C**
1 Each column of S is sorted to produce the sorted matrix SM
2 The index matrix **I** is generated by getting row number of each value in **SM** using Eq (4)
3 **for** *j=1 to M* **do**
4 Link pixels of **D** with positions in**I**.
5 Within circles, shift these related pixels **j** positions to the left **using Eq (5)**
6
end
7 The scrambled image**C** is obtained

cipher image. This optimization process is done using GA. Figure 14 shows the main steps of GA.

The initial population is created in the previous phase by applying ZT and CMT many times on the shuffled image. Then, GA follows these below steps:

Step 1: The correlation coefficient is used as the fitness function. It is calculated for each encrypted image in the population.

Therefore, the diagonal, vertical, and horizontal correlation coefficients are obtained by using Eq. **(8).** [32]:

$$r_{xy} = \frac{|cov(x,y)|}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{8}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{9}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{10}$$

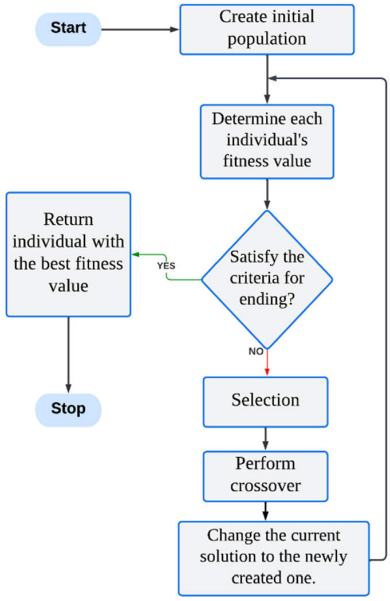


FIGURE 14. The block diagram for GA.

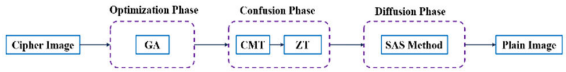


FIGURE 15. Decryption structure.

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{11}$$

where x and y are the image's two adjacent pixels values and, N is the total number of adjacent pairs of image pixels that are vertically, horizontally, or diagonally adjacent.

Step 2: Choose two parents with minimum fitness function from the current population.

Step 3: The new children are generated by applying a crossover operation on their parents. Then they added in the new population.

Step 4: Iterate Steps 2 and 3 until the last parent in the current population. After that, the new population is obtained.

Step 5: The current population is compared with the new population by selecting the best-generated images with the minimum fitness function.

Step 6: Repeat steps from 1 to 5 many times to generate a new population until reach to minimum fitness function. Then choose the best one. Finally, the last cipher image is picked as the best-encrypted image with the lowest correlation coefficient. The encryption algorithm is presented in Algorithm **4.**

5) THE DECRYPTION APPROACH

The decryption process is like the encryption process but in reversed order. We must use the same key in the encryption process to decrypt any cipher image. This process includes all encryption steps in reversed order, as shown in **Fig. (15)**.

In the decryption process, we first apply the GA crossover operation on the cipher image to extract the intermediate

Algorithm 4 The Encryption Process

Input: An original image P with the dimension M×N
Output: The encrypted image E

1. Generate two sequences S1, S2 using TLLM as shown in Algorithm **1**.
2. The diffused image D is generated by apply diffusion phase to the plain image P using sequence S1 as shown in Algorithm **2**.
3. Zigzag Matrix ZM is generated by applying zigzag transform method to the diffused image D
4. Applying CMT shown in Algorithm**3** with sequence S2 to ZT.
5. Creating the initial population POP with size L images for GA by repeating step 3 and step 4
6. **For** *i=1 to G*
   For *j=1:2 to L*
7. Calculate the correlation coefficient function to the j solution in POP
8. Select parents with the minimum correlation coefficient
9. Apply crossover operation to the selected parents to generate new children
   Add children in new population NPOP
   End
   For *j=1 to L*
   Calculate the fitness function to the j solution in the NPOP
   End
   The POP in position i is compared with NPOP
   Replace the previous population with the newly made.
10. **End**
11. Select the encrypted image from the best population as a best solution and the best encrypted image E

image. Then, the intermediate image is scrambled using the reverse of the CMT equation. Then the Zigzag method is performed in the reverse order. Finally, the reverse of the SAS method is applied to obtain the original image.

IV. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

In this section, the effectiveness of the suggested technique is demonstrated by analyzing its performance in terms of various validation metrics. Finally, the suggested technique is compared with some recent techniques. The following experiments are performed using symmetric images with size 512 × 512 in the USC-SIPI Image. Also, Asymmetric images with different sizes.

A. STATISTICAL ANALYSIS

This section depicts the experiments performed to evaluate our proposed technique. We have examined performance regarding frequently utilized tests and metrics in the proposed work.

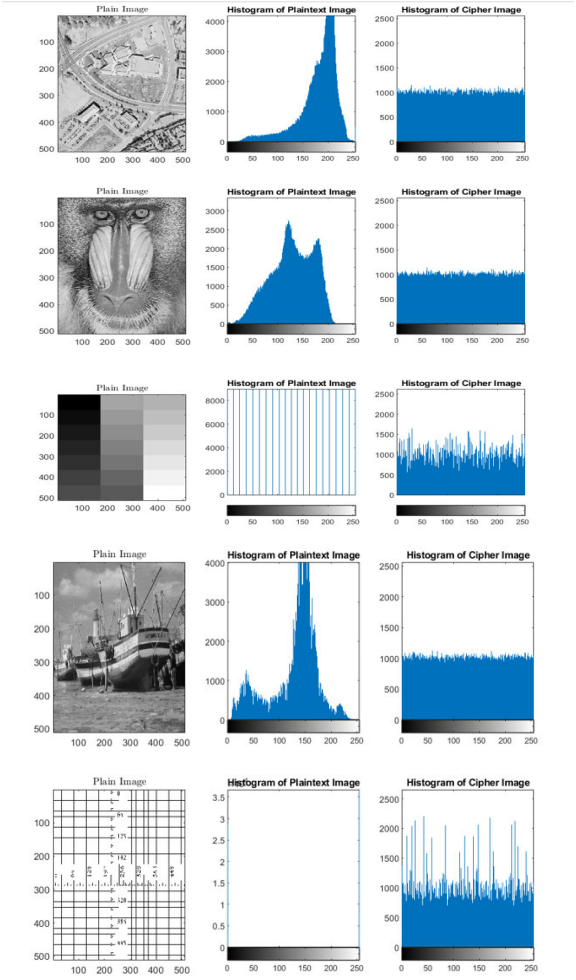


FIGURE 16. Images and cipher output histograms.

1) HISTOGRAM ANALYSIS

The histogram is the most statistical feature that shows how an image's pixels are distributed. Furthermore, the histogram represents the intensity value of the pixels in any image. The gray image consists of 256 different intensity values. The encrypted image histogram must be standardized to resist the various attacks. For presenting the test of our algorithm, 5 gray images are used. The result of our algorithm for these 5 gray images and their histogram is illustrated in Fig. **(16).** As illustrated in this figure, original image histograms contain sharp peaks, whereas cipher image histograms have a homogenous distribution. Thus, the attacker cannot extract any details from the images. As a result, the suggested technique is immune to statistical attacks.

2) CORRELATION ANALYSIS

Because nearby pixels are close together in the plain image, they have strong associations. As a result, correlation evaluation is vital for calculating the correlation coefficient among neighboring pixels and determining the method's

effectiveness. The proposed technique is powerful when the coefficient of correlation between pixels is low.

Equation (8) [34] is used to calculate the coefficient of correlation horizontally, vertically, and diagonally. Table **1** includes the correlation coefficient for a few original and cipher photo samples.

TABLE 1. Plain Image (PI) and Cipher Image (CI) correlation coefficients in the horizontal, vertical, and diagonal directions (CI).

									
Horizontal	PI	0.9719	0.8665	0.9831	0.9008	0.9381	0.4542	0.9965	0.8722
	CI	-0.0014	0.0013	-0.0061	0.0008	-0.0012	-0.0058	-0.0029	-0.0045
Vertical	PI	0.9850	0.7586	0.9900	0.8602	0.9713	0.4648	0.9998	0.8667
	CI	-.00013	-0.0037	0.0030	-0.0050	-0.0003	-0.0004	-0.0003	-0.0032
Diagonal	PI	0.9593	0.7261	0.9733	0.8031	0.9222	-0.0290	0.9964	0.7562
	CI	-0.0024	-0.0019	-0.0020	-0.0022	-0.0029	-0.0015	-0.0025	-0.0012

Therefore, the suggested technique must generate an encrypted image with a low pixel correlation coefficient.

As shown in Table **1**, In all three directions, the coefficient of correlation of nearby pixels in original images is high and close to one. However, the correlation of encrypted images is low and near zero. Therefore, the suggested technique is effective and robust against statistical attacks.

3) INFORMATION ENTROPY ANALYSIS

The entropy of an image is used to estimate its unpredictability. Entropy, in other words, measures the degree of information uncertainty and unpredictability. Hence, the greater entropy value demonstrates the increased amount of randomness in an image. Mathematically, entropy can be described as [14] and [34]:

$$\boldsymbol{H}(\mathbf{s}) = \sum_{i=0}^{\mathbf{i2}^{R}-\mathbf{1}} = \mathbf{P}(s_{\mathbf{i}}) \log_2 (\frac{\mathbf{1}}{\boldsymbol{P}(s_i)}) \tag{12}$$

where s_i is the pixel value, R represents the number of bits required to identify s_i, and P (s_i) denotes the likelihood of $s_i$appearing in a gray image.

Our proposed technique uses gray images in which each pixel is presented in 8 bits. So, R in the previous equation is equal to 8. Also, each pixel in the 8-bit gray image has 256 outcomes. Therefore, the probability of s_i is 1/256. Generally, a more considerable entropy value is equal to eight. However, it is approximately eight. Table **2** illustrates the entropy values for plain and cipher images.

TABLE 2. The proposed technique's information entropy for plain and encrypted images.

								
Plain Image	7.4451	7.3579	7.0480	6.9940	7.1914	0.5000	4.3923	1.5483
Cipher Image	7.9994	7.9993	7.9991	7.9990	7.9992	7.9547	7.9673	7.9973

As illustrated in this table, entropy values are pretty close to eight in the encrypted images. Hence, the suggested technique is more effective against an entropy attack and offers better randomness.

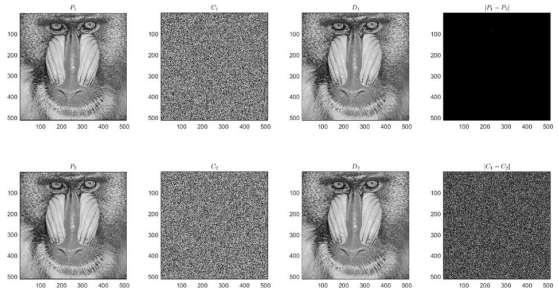


FIGURE 17. P1 Actual image – C1 Cipher image – D1 Deciphered image – P2 One-pixel modified actual image – C2 Modified image's cipher – D2 Decrypted modified cipher image.

B. DIFFERENTIAL ATTACKS

The ability to withstand differential attack is a critical criterion for determining the plain image's sensitivity. Attackers try to guess the secret key by making a tiny change to the plain image and comparing the modified encrypted image to the plain encrypted image. An encryption technique must ensure that even little changes in the plain image result in a significant difference in the encrypted image to fend off this attack. Hence, we need to measure the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) to estimate the magnitude of sensitivity to minor image modification.

Let P1 and P2 be two plain images with MN dimensions and only one distinct pixel, respectively. Let C1 and C2 represent the two encrypted images. Thus, the following equations are used to calculate NPCR and UACI:

$$\boldsymbol{D(i,j)} = \begin{cases} \mathbf{1} & \boldsymbol{C_1(i,j) = C_2(i,j)} \\ \mathbf{0} & \boldsymbol{C_1(i,j) = C_2(i,j)} \end{cases} \tag{13}$$

$$\boldsymbol{NPCR} = \frac{\sum_{i,j} \boldsymbol{D(i,j)}}{\boldsymbol{M \times N}} \times \mathbf{100\%} \tag{14}$$

$$\boldsymbol{UACI} = \frac{\mathbf{1}}{\boldsymbol{M \times N}} \left(\sum_{i,j} \frac{\boldsymbol{C_1(i,j) - C_2(i,j)}}{\mathbf{255}} \right) \times \mathbf{100\%} \tag{15}$$

In our experiment, the suggested technique is evaluated by changing one pixel randomly in a plain image. Fig. **(17)** illustrates the encrypted images of the Baboon.512 image and its modified image, which differs only by one pixel. Table **3** presents the NPCR and AUCI values of tested images with only one-pixel change.

TABLE 3. In terms of UACI and NPCR, evaluating the distinction between two encrypted images of the actual images with a one-pixel.

								
NPCR	99.6220	99.6223	99.6098	99.5968	99.6113	99.6025	99.6147	99.6048
UACI	33.5440	33.5434	33.4438	33.4764	33.4831	33.5696	33.3295	33.5367

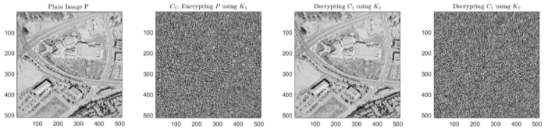


FIGURE 18. Results of key sensitivity for aerial image.

TABLE 4. PSNR and MSE evaluation of a sample of images.

PSNR	13.0701	27.0254	20.5418	3.4988	20.7415	10.6690
MSE	0.0493	0.0020	0.0088	0.4468	0.0084	0.0857

As shown in Table 3, The suggested technique achieves NPCR values of about 99.62% and UACI values of around 33.56 percent. Hence, the suggested technique can survive the differential attack.

C. KEY ANALYSIS

The key space and sensitivity are two important criteria used to measure the strength of our technique versus brute-force attacks.

1) KEY SPACE ANALYSIS

The encryption system must include a big space to survive brute-force attacks. A brute-force attack aims to anticipate the real key by searching all possible fake keys. In our proposed technique, the secret key is constructed from the plain image using SHA-256. Hence, the secret key is 256 bits. This key includes 4 initial values (X0, Z0, Y0, N0) and 5 parameters for TLLM. The computer accuracy of these parameters and initial values is 10^{-14} in key space analysis [34], [38]. Accordingly, the key space is calculated as follows: -

$$\left(10^{14}\right)^4 \times \left(10^{14}\right)^5 = 10^{126} \cong 2^{404}$$

Therefore, the suggested technique provides a huge key space that can withstand all types of brute-force attacks.

2) KEY SENSITIVITY ANALYSIS

Our proposed method uses two keys to encrypt and decrypt images. These keys are generated using TLLM. Generally, the tent-logistic and Lorenz maps are sensitive to their preliminary values and parameters. Therefore, if any slight modification is made in any key, this will obtain a new decrypted image different from the original image. We start with the primary key (K1) to test the sensitivity of our keys. Also, we make a one-bit change in K1 to obtain K2. As shown in Fig. **(18),**K1 is utilized to encrypt an original image (P) to Extract the encrypted image C1. Then, C1 is decoded using K1 and K2 to obtain the decrypted images.

As observed in Fig. **(18)**, the decryption method is done correctly, and the original image is reconstructed when we utilize the correct key (K1). But, when using K2, the decryption process fails to extract the plain image.

TABLE 5. NIST test results.

Test Items	P-value	Results
Frequency	0.067549	Pass
Block Frequency	0.211573	Pass
Cumulative Sums forward	0.100694	Pass
Cumulative Sums Reverse	0.538079	Pass
Runs	0. 867100	Pass
Longest Run	0.048225	Pass
Rank	0.156593	Pass
FFT	0.739918	Pass
Nonoverlapping Template	0.181676	Pass
Overlapping Template	0.050669	Pass
Universal	0.628686	Pass
Approximate Entropy	0.112811	Pass
Random Excursions	0.023921	Pass
Random Excursions Variant	0.241071	Pass
Serial	0.185585	Pass
Serial	0.869731	Pass
Linear Complexity	0.893122	Pass

Another way to measure the key sensitivity of our suggested technique is mainly based on the calculation of the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR).

MSE is utilized to evaluate the error between a decrypted image (D2) and a plain image. It is calculated by taking the

TABLE 6. Comparison the proposed technique with other techniques.

MEASURE	Image Name	Methods						
		Al-Hazaimeh et al. [6]	Niu et al. [7]	Qayyum et al. [38]	Ghazvini et al. [32]	Girdhar et al. [7]	Lyle et al. [42]	Proposed
KEY Space		2^{304}	2^{233}	2^{299}	2^{224}	2^{149}	2^{199}	$\mathbf{2^{404}}$
Entropy	Lena	7:99922	7.9976	7.9973	7.9991	-	7.9993	**7.9994**
	Bab	-	7.9973	7.9969	7.9987	7.998	7.9993	**7.9993**
	C.man	7.99715	-	7.9974	7.9991	-	7.9994	**7.9993**
	Boat	-	-	-	7.9993	7.997	7.9993	**7.9994**
UACI	Lena	33.241	33.51	33.49	33.35	-	33.4302	**33.5440**
	Bab	-	-	33.52	33.17	33.463	33.4435	**33.5434**
	C.man	33.3381	-	33.49	33.40	-	33.4209	**33.4451**
	Boat	-	-	-	33.31	33.482	33.4523	**33.4831**
NPCR	Lena	99.5888	99.61	99.61	99.57	-	99.6201	**99.6320**
	Bab	-	-	99.61	99.63	99.609	**99**.6040	**99.6372**
	C.man	99.5789	-	99.61	99.56	-	99.6025	**99.6298**
	Boat	-	-	-	99.59	99.61	99.6231	**99.6321**

difference between P and D2 as follows [34]:

$$\boldsymbol{MSE}\left(\boldsymbol{p_m},\boldsymbol{p_d}\right) = \frac{1}{\boldsymbol{M}\times\boldsymbol{N}}\sum_{i=1}^{\boldsymbol{M}}\sum_{j=1}^{\boldsymbol{N}}(\boldsymbol{p_m}(\boldsymbol{i},\boldsymbol{j}) - \boldsymbol{p_d}(\boldsymbol{i},\boldsymbol{j}))^2 \quad (16)$$

where $p_d(i,j)$ represents the grayscale pixel values of a decrypted image with MN dimensions and $p_m\,(i,j)$ signifies the grayscale pixel values of an original image. The PSNR is used to evaluate image quality. It's also used to calculate the conflict between the decrypted image D2 and the plain image P using the equation below

$$\boldsymbol{PSNR}\left(\boldsymbol{p_m},\boldsymbol{p_d}\right) = 20\log\left(\frac{\boldsymbol{255}}{\boldsymbol{MSE}}\right) \quad (17)$$

For optimal performance, PSNR and MSE should be high and low, respectively. Table **4** shows the results of PSNR and MSE. Hence, our proposed technique's encryption and decryption keys are extremely sensitive.

D. TIME COMPLEXITY

The core of our algorithm is to encrypt and decrypt gray images with size $M \times N$. The processing time of the proposed algorithm is distributed into 4 main stages.

The first stage is the chaotic sequence generation. The two sequences are generated using a 3D Lorenz map and a 2D tent-logistic map. The length of these sequences is equal to the size of the image (MN). Therefore, the complexity of this stage is $O\,(M \times N)$.

The second stage is the diffusion process which works on blocking the image and making substitutions for all pixels of the image. So, the complexity is $O\,(M \times N)$.

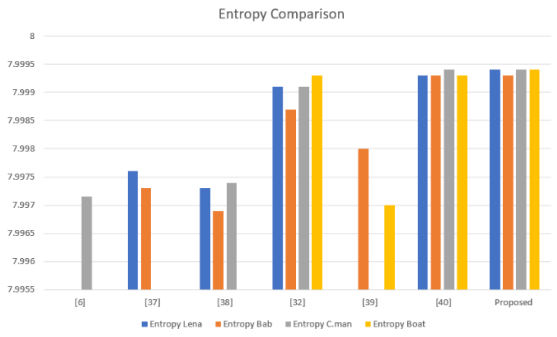
The third stage is the confusion process which contains ZT and CMT. ZT method works on creating a vector from image pixels in a zigzag form. So, the complexity of ZT is $O\,(M \times N)$. then CMT is performed with complexity $O\,(M \times N)$.

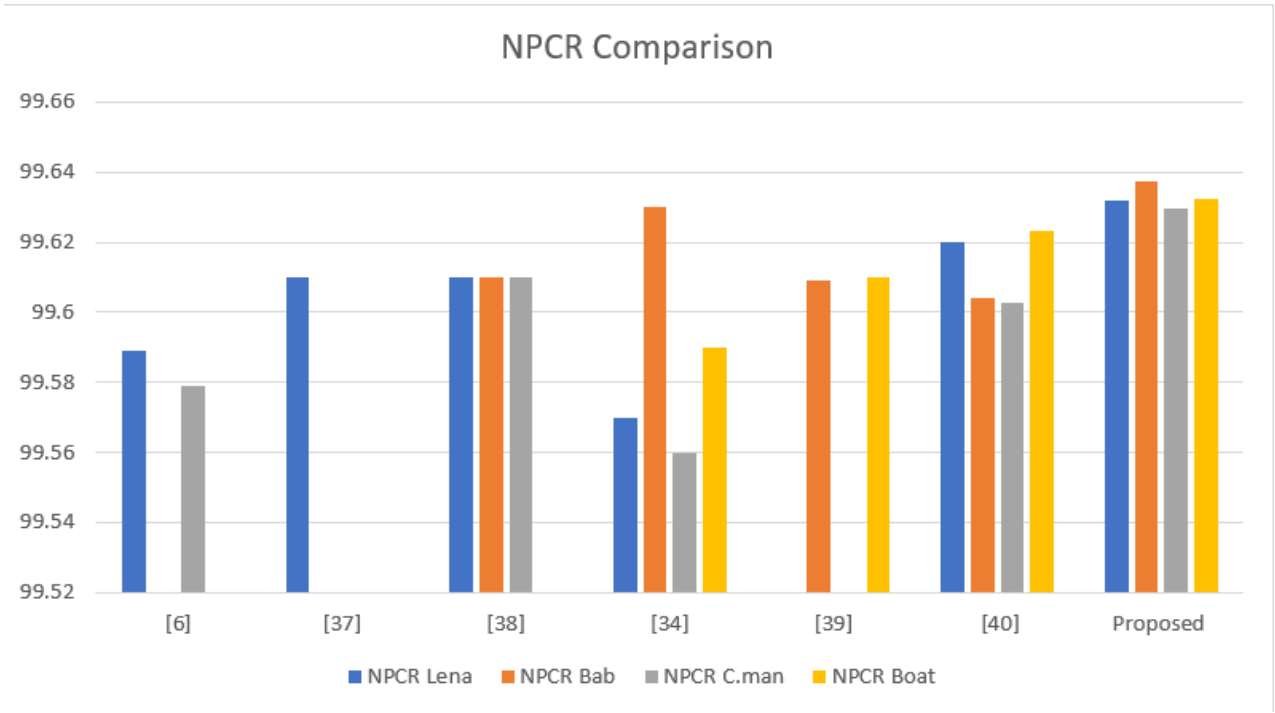
Finally, the optimization process is performed using GA. The time complexity of GA is mainly dependent on the number of generations G, the number of individuals (images) I, and the number of population P. So, the time complexity of GA is O (G∗I(O(selection)+O(crossover)) ∗P). Therefore, time complexity of the algorithm is mainly dependent on the size of the input image and the number of generations.

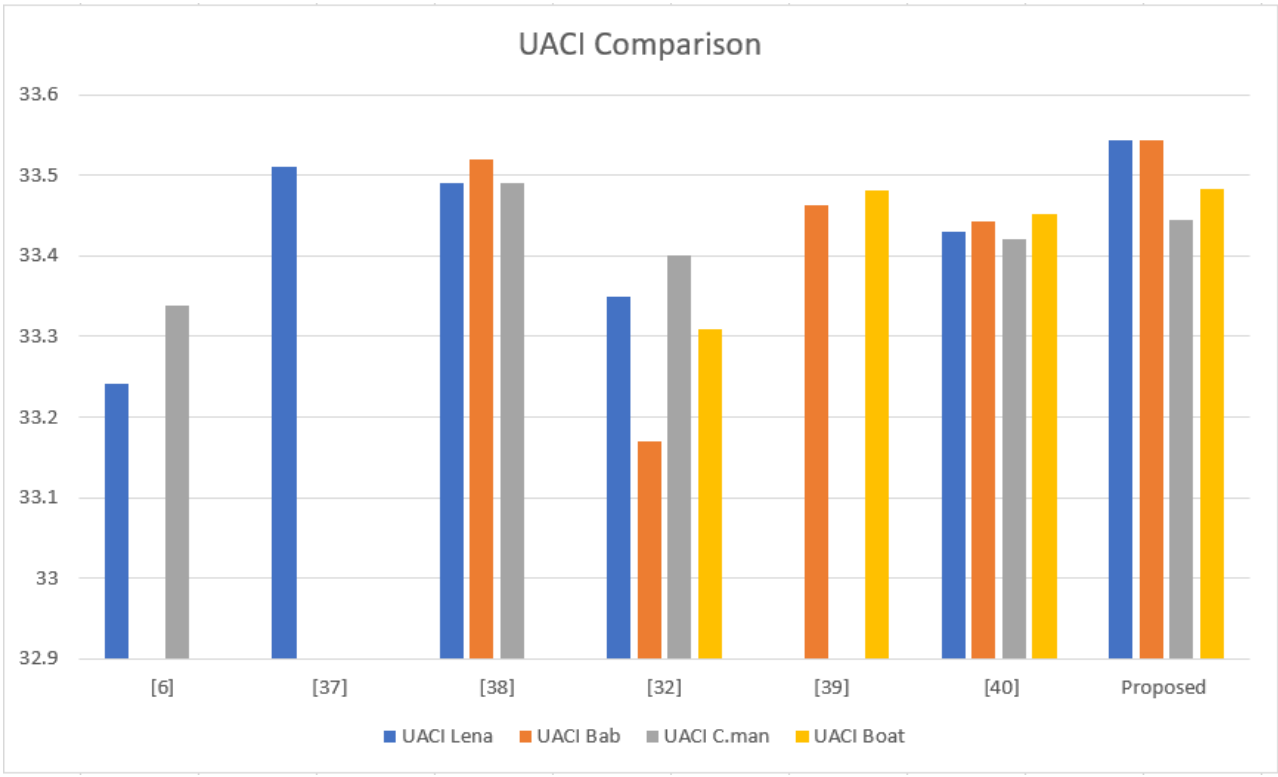
E. NIST TEST SUITE

NIST test suit is used to determine the randomness of the sequences. The NIST has 15 statistical tests, and each test has a randomness probability value (P-value). The TABLE 5 represents the NIST test of our sequences.

As can be seen in the previous table, the data sequences have passed all random tests. This proves that our algorithm has good randomness.







F. PERFORMANCE COMPARISON

The introduced technique's performance is compared with several related methods. Additionally, the same dataset is used in all these approaches, and we select common images for comparison. Table **5** shows the key space, Entropy, NPCR, and UACI results of our technique and other compared techniques. According to this table, our proposed technique performs best on all standards for all tested images. Also, it outperforms other compared techniques in terms of NPCR, UACI, and entropy. Thus, our proposed technique is more effective than other techniques. Below, we present comparison charts for entropy, UACI, and NPCR.

V. CONCLUSION

Ensuring the security and privacy of massive, unstructured volume of multimedia data is a serious issue. Accessing

multimedia data is an essential need of our daily life since information technology services, systems, and applications pervade every aspect of our lives, leaving these data vulnerable to severe cyber-attacks. This study presents a grayscale image encryption technique that relies on ZT, a chaotic system, and a GA. Based on the TLLM approach, The hash key is utilized to construct the default values of the chaotic sequences. The diffused image is realized using self-adaptive diffusion performed by the first sequence. In the confusion phase, two ordered functions (e.g., ZT and CMT) are employed to scramble the diffused image and generate the initial population for the GA. Finally, a GA is utilized to enhance and optimize the encryption process to find the best-encrypted image with a correlation coefficient close to zero. As a result, our technique produces a cipher image with high entropy, a few correlation pixels, and a histogram with a uniform distribution. Therefore, the proposed technique is capable of withstanding statistical attacks. Furthermore, the NPCR, UACI, and key analysis results show that our technique has a secure and vast key space, can withstand differential attacks, and satisfy the key sensitivity with an acceptable level. Unlike other methods, the proposed mechanism can prevent data loss during the recovery of the actual data, which is considered one of the greatest distinctive features of our mechanism.

In the future, we can utilize neural networks to get the preliminary values and parameters of chaotic maps. Additionally, a quantum system can be combined with a chaotic system to construct a more effective sequence. Also, other swarm optimization algorithms can be used instead of genetic algorithms to improve the encryption process.

REFERENCES

[1] S. Kandar, D. Chaudhuri, A. Bhattacharjee, and B. C. Dhara, "Image encryption using sequence generated by cyclic group," *J. Inf. Secur. Appl.*, vol. 44, pp. 117–129, Feb. 2019, doi: 10.1016/j.jisa.2018.12.003.

[2] J. Wang, X. Zhi, X. Chai, and Y. Lu, "Chaos-based image encryption strategy based on random number embedding and DNA-level self-adaptive permutation and diffusion," *Multimedia Tools Appl.*, vol. 80, no. 10, pp. 16087–16122, Apr. 2021, doi: 10.1007/s11042-020-10413-7.

[3] S. H. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, "A new modified version of advanced encryption standard based algorithm for image encryption," in *Proc. Int. Conf. Electron. Inf. Eng.*, Aug. 2010, pp. 141–145, doi: 10.1109/ICEIE.2010.5559902.

[4] X. Huang and G. Ye, "An efficient self-adaptive model for chaotic image encryption algorithm," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 12, pp. 4094–4104, 2014, doi: 10.1016/j.cnsns.2014.04.012.

[5] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Process., Image Commun.*, vol. 80, Feb. 2020, Art. no. 115670, doi: 10.1016/j.image.2019.115670.

[6] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Comput. Appl.*, vol. 31, no. 7, pp. 2395–2405, Jul. 2019, doi: 10.1007/s00521-017-3195-1.

[7] Y. Niu, Z. Zhou, and X. Zhang, "An image encryption approach based on chaotic maps and genetic operations," *Multimedia Tools Appl.*, vol. 79, nos. 35–36, pp. 25613–25633, Sep. 2020, doi: 10.1007/s11042-020-09237-2.

[8] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, no. 11, pp. 172–182, 2014, doi: 10.1016/j.sigpro.2013.10.034.

[9] M. A. Rakotomalala, T. E. Rakotondraina, and S. Rakotondramanana, "Contribution for improvement of image scrambling technique based on zigzag matrix reodering," *Int. J. Comput. Trends Technol.*, vol. 61, no. 1, pp. 10–17, Jul. 2018, doi: 10.14445/22312803/ijctt-v61p102.

[10] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map," *Entropy*, vol. 21, no. 7, p. 656, Jul. 2019, doi: 10.3390/e21070656.

[11] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015, doi: 10.1016/j.ins.2014.11.018.

[12] Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2012, Sep. 2015, doi: 10.1109/TCYB.2014.2363168.

[13] T. S. Ali and R. Ali, "A novel medical image signcryption scheme using TLTS and Henon chaotic map," *IEEE Access*, vol. 8, pp. 71974–71992, 2020, doi: 10.1109/ACCESS.2020.2987615.

[14] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, Arshad, F. Masood, F. Khan, and W. J. Buchanan, "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140876–140895, 2020, doi: 10.1109/ACCESS.2020.3012912.

[15] A. B. Joshi, D. Kumar, A. Gaffar, and D. C. Mishra, "Triple color image encryption based on 2D multiple parameter fractional discrete Fourier transform and 3D Arnold transform," *Opt. Lasers Eng.*, vol. 133, Oct. 2020, Art. no. 106139, doi: 10.1016/j.optlaseng.2020.106139.

[16] N. A. M. Abbas, "Image encryption based on independent component analysis and Arnold's cat map," *Egyptian Informat. J.*, vol. 17, pp. 139–146, Mar. 2016, doi: 10.1016/j.eij.2015.10.001.

[17] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, Nov. 2018, doi: 10.3390/e20120913.

[18] R. I. Abdelfatah, M. E. Nasr, and M. A. Alsharqawy, "Encryption for multimedia based on chaotic map: Several scenarios," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19717–19738, Jul. 2020, doi: 10.1007/s11042-020-08788-8.

[19] X. Liu, Y. Song, and G.-P. Jiang, "Hierarchical bit-level image encryption based on chaotic map and feistel network," *Int. J. Bifurcation Chaos*, vol. 29, no. 2, Feb. 2019, Art. no. 1950016, doi: 10.1142/S0218127419500160.

[20] A. Girdhar and V. Kumar, "A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 27017–27039, Oct. 2018, doi: 10.1007/s11042-018-5902-z.

[21] Q. Ran, L. Wang, J. Ma, L. Tan, and S. Yu, "A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections," *Quantum Inf. Process.*, vol. 17, no. 8, pp. 1–30, Aug. 2018, doi: 10.1007/s11128-018-1958-y.

[22] X. Wang and N. Guan, "A novel chaotic image encryption algorithm based on extended zigzag confusion and RNA operation," *Opt. Laser Technol.*, vol. 131, Nov. 2020, Art. no. 106366, doi: 10.1016/j.optlastec.2020.106366.

[23] A. Bal and N. Paul, "An efficient image encryption method based on genetic algorithm," *Int. J. Eng. Sci. Invention*, vol. 7, no. 4, pp. 64–70, Apr. 2018.

[24] P. A. Agbedemnab and M. Agebure, "An optimal digital image encryption system using the genetic algorithm," *Int. J. Eng. Sci. Comput.*, vol. 11, no. 4, pp. 1–5, May 2021.

[25] M. Ghebleh, A. Kanso, and D. Stevanović, "A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation," *Multimedia Tools Appl.*, vol. 77, no. 6, pp. 7305–7326, Mar. 2018, doi: 10.1007/s11042-017-4634-9.

[26] W. Xingyuan, Z. Junjian, and C. Guanghui, "An image encryption algorithm based on ZigZag transform and LL compound chaotic system," *Opt. Laser Technol.*, vol. 119, Nov. 2019, Art. no. 105581, doi: 10.1016/j.optlastec.2019.105581.

[27] Y. Zhang, "A fast image encryption algorithm based on convolution operation," *IETE J. Res.*, vol. 65, no. 1, pp. 4–18, 2017, doi: 10.1080/03772063.2017.1400406.

[28] S. T. Allawi, "Image encryption based on chaotic mapping and random numbers," *J. Eng. Appl. Sci.*, vol. 14, no. 19, pp. 6954–6958, Oct. 2019, doi: 10.36478/jeasci.2019.6954.6958.

[29] Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, "Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion," *Opt. Lasers Eng.*, vol. 134, Nov. 2020, Art. no. 106202, doi: 10.1016/j.optlaseng.2020.106202.
[30] M. Hanif, R. A. Naqvi, S. Abbas, M. A. Khan, and N. Iqbal, "A novel and efficient 3D multiple images encryption scheme based on chaotic systems and swapping operations," *IEEE Access*, vol. 8, pp. 123536–123555, 2020, doi: 10.1109/ACCESS.2020.3004536.
[31] H. Gao and X. Wang, "Chaotic image encryption algorithm based on zigzag transform with bidirectional crossover from random position," *IEEE Access*, vol. 9, pp. 105627–105640, 2021, doi: 10.1109/ACCESS.2021.3099214.
[32] Y. Qobbi, A. Jarjar, M. Essaid, and A. Benazzi, "Image encryption algorithm based on genetic operations and chaotic DNA encoding," *Soft Comput.*, vol. 26, no. 12, pp. 5823–5832, Jun. 2022, doi: 10.1007/s00500-021-06567-7.
[33] K.-W. Wong, W.-S. Yap, D. C.-K. Wong, R. C.-W. Phan, and B.-M. Goi, "Cryptanalysis of genetic algorithm-based encryption scheme," *Multimedia Tools Appl.*, vol. 79, nos. 35–36, pp. 25259–25276, Sep. 2020, doi: 10.1007/s11042-020-09191-z.
[34] M. Ghazvini, M. Mirzadi, and N. Parvar, "A modified method for image encryption based on chaotic map and genetic algorithm," *Multimedia Tools Appl.*, vol. 79, nos. 37–38, pp. 26927–26950, Oct. 2020, doi: 10.1007/s11042-020-09058-3.
[35] P. Murali, G. Niranjana, A. J. Paul, and J. S. Muthu, "Domain-flexible selective image encryption based on genetic operations and chaotic maps," *Vis. Comput.*, pp. 1–23, Feb. 2022, doi: 10.1007/s00371-021-02384-z.
[36] Z. Man, J. Li, X. Di, and Y. Mu, "Application of quantum genetic algorithm in high noise laser image security," *Optoelectronics Lett.*, vol. 18, no. 1, pp. 59–64, Jan. 2022, doi: 10.1007/s11801-022-1070-5.
[37] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, "An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata," *Neural Comput. Appl.*, vol. 32, no. 9, pp. 4961–4988, May 2020, doi: 10.1007/s00521-018-3913-3.
[38] S. F. Yousif, "Grayscale image confusion and diffusion based on multiple chaotic maps," in *Proc. 1st Int. Scientific Conf. Eng. Sci. 3rd Scientific Conf. Eng. Sci. (ISCES)*, Jan. 2018, pp. 114–119, doi: 10.1109/ISCES.2018.8340538.
[39] A. Girdhar, H. Kapur, and V. Kumar, "A novel grayscale image encryption approach based on chaotic maps and image blocks," *Appl. Phys. B*, vol. 127, no. 3, pp. 1–12, Mar. 2021, doi: 10.1007/s00340-021-07585-x.
[40] M. Lyle, P. Sarosh, and S. A. Parah, "Adaptive image encryption based on twin chaotic maps," *Multimedia Tools Appl.*, vol. 81, no. 6, pp. 8179–8198, Mar. 2022, doi: 10.1007/s11042-022-11917-0.

NAWAL SHALTOUT received the B.Sc. degree from the Computer Science Department, Faculty of Computer and Information Sciences, Mansoura University, Mansoura, Egypt, in 2013 and 2017, respectively.

Since 2017, she has been a Demonstrator with the Department of Computer Science, Faculty of Computer, and Information Sciences, Mansoura University. Her research interests include cryptography, image security, chaotic systems, software engineering, mobile development, and optimization algorithms.

AHMED A. ABD EL-LATIF (Senior Member, IEEE) received the B.Sc. degree (Hons.) in mathematics and computer science and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2005 and 2010, respectively, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology (HIT), Harbin, China, in 2013. He is currently an Associate Professor in computer science with Menoufia University, and the EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia. He is the author and coauthor of more than 200 papers, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. He received many awards, State Encouragement Award in Engineering Sciences 2016, Arab Republic of Egypt; the Best Ph.D. Student Award from the Harbin Institute of Technology, China, in 2013; and the Young Scientific Award, Menoufia University, in 2014. His research interests include multimedia content encryption, secure wireless communication, the IoT, applied cryptanalysis, perceptual cryptography, secret media sharing, information hiding, biometrics, forensic analysis in digital images, and quantum information processing. He is a member of ACM. He is a fellow of the Academy of Scientific Research and Technology, Egypt. He is the chair/the co-chair/the program chair of some Scopus/EI conferences. He is the Editor-in-Chief of *International Journal of Information Security and Privacy* and the Series Editor of *Advances in Cybersecurity Management* (https://www.routledge.com). He is also an academic editor/an associate editor for set of indexed journals (Scopus journal's quartile ranking). Currently, he had many books, more than ten books, in several publishers in Springer, IET, CRC press, IGI-Global, Wiley, and IEEE.

WALEED M. AL-ADROUSY was born in Macau, Saudi Arabia, in 1982. He received the B.Sc., M.Sc., and Ph.D. degrees in computer science from the Faculty of Computer and Information Sciences, Mansoura University, in 2004, 2010, and 2015, respectively.

He is currently an Egyptian Researcher. He worked as a Demonstrator, from 2004 to 2010, and a Teaching Assistant, from 2010 to 2015. Since 2015, he has been a Lecturer with the Faculty of Computer and Information Sciences, Mansoura University. His research interests include several scientific fields, such as social network analysis, recommender systems, distributed systems, game development, 3D modeling, simulation, mobile development, security, and software engineering.

SAMIR ELMOUGY received the Ph.D. degree in computer science from the School of Electrical Engineering and Computer Science, Oregon State University, USA. He is currently a Professor in computer science and the Vice Dean for Postgraduate Studies and Research at the Faculty of Computers and Information, Mansoura University, Egypt. From 2008 to 2014, he was an Assistant Professor at the Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He has published over 70 papers in refereed IEEE Transactions/Springer journals, IEEE conferences, and book chapters. Also, he participated in the reviewing process of many international refereed journals and conferences. His current research interests include artificial intelligence, the IoT, information theory, and software engineering.