Computer Modeling in Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.063405

ARTICLE

Chaos-Based Novel Watermarked Satellite Image Encryption Scheme

Mohamed Medani[1], Yahia Said[2], Nashwan Adnan Othman[3,4], Farrukh Yuldashev[5], Mohamed Kchaou[6], Faisal Khaled Aldawood[6] and Bacha Rehman[7,*]

[1]Applied College of Muhayil Aseer, King Khalid University, Abha, 62529, Saudi Arabia
[2]Center for Scientific Research and Entrepreneurship, Northern Border University, Arar, 73213, Saudi Arabia
[3]Department of Computer Engineering, College of Engineering, Knowledge University, Erbil, 44001, Iraq
[4]Department of Computer Engineering, Al-Kitab University, Altun Kupri, 36001, Iraq
[5]Department of Informatics and Its Teaching Methods, Tashkent State Pedagogical University, Tashkent, 100070, Uzbekistan
[6]Department of Industrial Engineering, College of Engineering, University of Bisha, Bisha, P.O. Box 001, Saudi Arabia
[7]Department of Computer Science, Solent University, Southampton, SO14 0YN, UK

*Corresponding Author: Bacha Rehman. Email: bacha.rehman@solent.ac.uk

Received: 14 January 2025; Accepted: 12 March 2025; Published: 11 April 2025

ABSTRACT: Satellite images are widely used for remote sensing and defence applications, however, they are subject to a variety of threats. To ensure the security and privacy of these images, they must be watermarked and encrypted before communication. Therefore, this paper proposes a novel watermarked satellite image encryption scheme based on chaos, Deoxyribonucleic Acid (DNA) sequence, and hash algorithm. The watermark image, DNA sequence, and plaintext image are passed through the Secure Hash Algorithm (SHA-512) to compute the initial condition (keys) for the Tangent-Delay Ellipse Reflecting Cavity Map (TD-ERCS), Henon, and Duffing chaotic maps, respectively. Through bitwise XOR and substitution, the TD-ERCS map encrypts the watermark image. The ciphered watermark image is embedded in the plaintext image. The embedded plaintext image is permuted row-wise and column-wise using the Henon chaotic map. The permuted image is then bitwise XORed with the values obtained from the Duffing map. For additional security, the XORed image is substituted through a dynamic S-Box. To evaluate the efficiency and performance of the proposed algorithm, several tests are performed which prove its resistance to various types of attacks such as brute-force and statistical attacks.

KEYWORDS: DNA sequence; TD-ERCS chaotic map; henon chaotic map; duffing chaotic system; SHA-512; encryption technique; watermark embedding

1 Introduction

With the technological evolution, satellites are used for various applications such as remote sensing, national security, weather forecasting, deep space research, and navigation purposes [1,2]. The most effective way of satellite communication is through digital images, and these images are exposed to various threats [3]. That is why these images need encryption and digital watermarking to ensure integrity and confidentiality [4]. Masking or concealing the information is encryption, while embedding some information in the digital media to protect it from manipulation and illegal copying is digital watermarking. A digital watermark may be visible or invisible, depending on the scenario. Encryption can be done using different cryptographic techniques. Cryptography deals with the security of information [5]. Confusion and diffusion are the two fundamental mechanisms involved in cryptography. From previous research, it is clear that confusion is

changing the values of the pixels dependent on a key, which is obtained via swapping/substituting one value for another [6]. Conventional encryption schemes such as the advanced encryption standard, Rivest-Shamir-Adleman, data encryption standard, and international data encryption algorithm are not suitable for image encryption because of the high correlation of image pixels. Using chaotic maps in cryptography is an emerging field that uses random sequences to encrypt digital images. In addition to being non-linear, these elementary chaotic maps exhibit a variety of strange attractors with variable initial keys, as well as inherent randomness [7]. To design a resilient cryptosystem, it is necessary to use each of these characteristics effectively. These initial conditions serve as secret keys that can only be accessed by authorized individuals. It is impossible to decrypt the system without knowing these keys. In this context, sensitivity to control parameters and initial conditions is critical since it stops unauthorized users and hackers from attempting to decrypt the secured content. Because of the high sensitivity, even minor modifications to the control parameters and initial conditions values result in drastically different weird random numbers, making decryption by hackers nearly impossible.

To consistently enhance the level of encryption security, researchers are persistently engaged in the pursuit of novel high-security techniques to contribute to the encryption process. Therefore, numerous encryption methods have been introduced and presented in the literature, including chaos-based encryption [8–10], visual image encryption [11,12], S-Box-based encryption [13–15], compression and encryption [16,17], and Deoxyribonucleic Acid (DNA) based encryption [18,19]. Authors in [8] use Joseph transforms and discrete Fourier transforms to significantly enhance the security of designed image encryption. In addition to space domain encryption, frequency domain encryption has also been performed. Logistic chaotic map is used for creating chaotic numbers, while Joseph traversals are used for permuting image pixels. As a consequence, it can be concluded that Joseph's traversal can improve the security of an image, and therefore, the proposed scheme can withstand common attacks. Conventional image encryption algorithms generate encrypted images that include noise-like attributes, drawing potential attackers' interest. Therefore, to address this issue, visual or meaningful image encryption algorithms are proposed. Su et al. compressed the plaintext image employing sensing, subsequently applying the Arnold transform to induce scrambling and generate a ciphertext image [11]. The ciphertext image is subsequently divided into segments and embedded into a carrier image utilizing shifting intensity levels through Singular Value Decomposition (SVD). To achieve enhanced security, a controllable quantum walk is utilized for the generation of pseudorandom sequences, that are then implemented to determine the embedded image's positioning within the carrier image and to construct the sensing matrix. In [12], an image encryption algorithm that initially undergoes Vector Quantization (VQ) encoding as a first step, followed by visual encryption by content transformation using Discrete Wavelet Transform (DWT) to produce the resulting meaningful image is developed.

The authors in [20] Multi-Image Encryption (MIE) and Back-Propagation (BP) neural network compression method capable of encrypting color and grayscale images of different sizes. Through the use of BP neural networks, the MI cube is first compressed, then scrambled and finally diffused. The authors in [21] utilized Computational Ghost Imaging (CGI) to design a dual-channel image encryption and authentication algorithm. The pseudo-random sequences are generated using a Logistic map and a 4D chaotic system. Khan et al. present a novel quantum image encryption scheme based on a chaotic confusion-diffusion architecture with two phases [22]. There are four separate confusion-diffusion modules integrated with the proposed architecture, which are capable of simultaneously performing a two-level encryption of both the position of the quantum encoding pixel as well as the intensity of the quantum encoding pixel. Ma et al. utilize Chen's system and Tabu Search (TS) to design an image encryption scheme that can resist plaintext attacks [23]. Chen's system key is computed by passing the plaintext image through a hash algorithm.

The block permutation technique is used to break the correlation between original adjacent pixels. Kong et al. developed two types of fractional-order memristors for encrypting images on a Field-Programmable Gate Array (FPGA) [24]. It exhibits high dynamic behavior such as extreme multistability, hyperchaos, overclocking, and multiscroll. Substitution boxes (S-Box) are used in image encryption applications for substituting plaintext pixels. Mainly S-Boxes are used for increasing image security via introducing non-linearity [25]. Zhu et al. proposed a robust methodology for constructing a strong and reliable S-Box to encrypt images [13]. The constructed S-Box is based on the utilization of a One-Dimensional (1D) piece-wise quadratic polynomial chaotic Map. Moreover, S-Box substitution and diffusion encryption techniques are combined with pixel segmentation encryption in this encryption algorithm. The authors in [14] proposed a novel approach for developing a chaos-based S-Box that can be incorporated into encryption algorithms. The algorithm's performance is assessed using various testing procedures.

Contribution

- The designed satellite image encryption scheme has both confusion and diffusion characteristics.
- The Key's dependence on both the watermark image and the plaintext image, as well as the DNA sequence, makes the scheme resilient to classical attacks.
- The ciphered watermark embedding provides an extra layer of security.

The rest of this article is arranged as follows: Section 2 provides an explanation of the preliminaries, and Section 3 provides a step-by-step description of the proposed watermarked satellite image encryption. Section 4 presents the experimental analysis of the designed scheme. Lastly, the conclusion is drawn in Section 5.

2 Preliminaries

The proposed scheme combines a secure hash algorithm (SHA-512) with multiple chaotic maps and DNA sequences. SHA-512, DNA sequences and chaotic maps are discussed in this section.

2.1 Henon Chaotic Map

Henon Chaotic Map is a two-dimensional dynamic system depicting chaotic behaviour in a discrete domain [26]. Mathematically Henon chaotic map can be written as [26]:

$$\begin{cases} x_{(n+1)} = -1(a.x_n^2 - y_n - 1) \\ y_{(n+1)} = b.x_n \end{cases} \tag{1}$$

The chaotic nature of this map is based on the values of its control parameters a and b and initial conditions x_0 and y_0. This chaotic behaviour is observed for the values $a = 1.4$ and $b = 0.3$, which are termed traditional values. The orbit may be chaotic, sporadic, or converge to an aperiodic orbit for values that differ from traditional values. Map sensitivity is demonstrated by iterating the map twice with $x_0 = 0.01$ and $x_0 = 0.01001$ or $x_0 = 0.01 \times 10^{-12}$. As can be seen from Fig. 1a,b, both sets of random numbers differ. Additionally, Fig. 2a illustrates 5000 random numbers generated through the Henon chaotic map. So, the chaotic system is extremely sensitive and produces different random numbers with small changes.

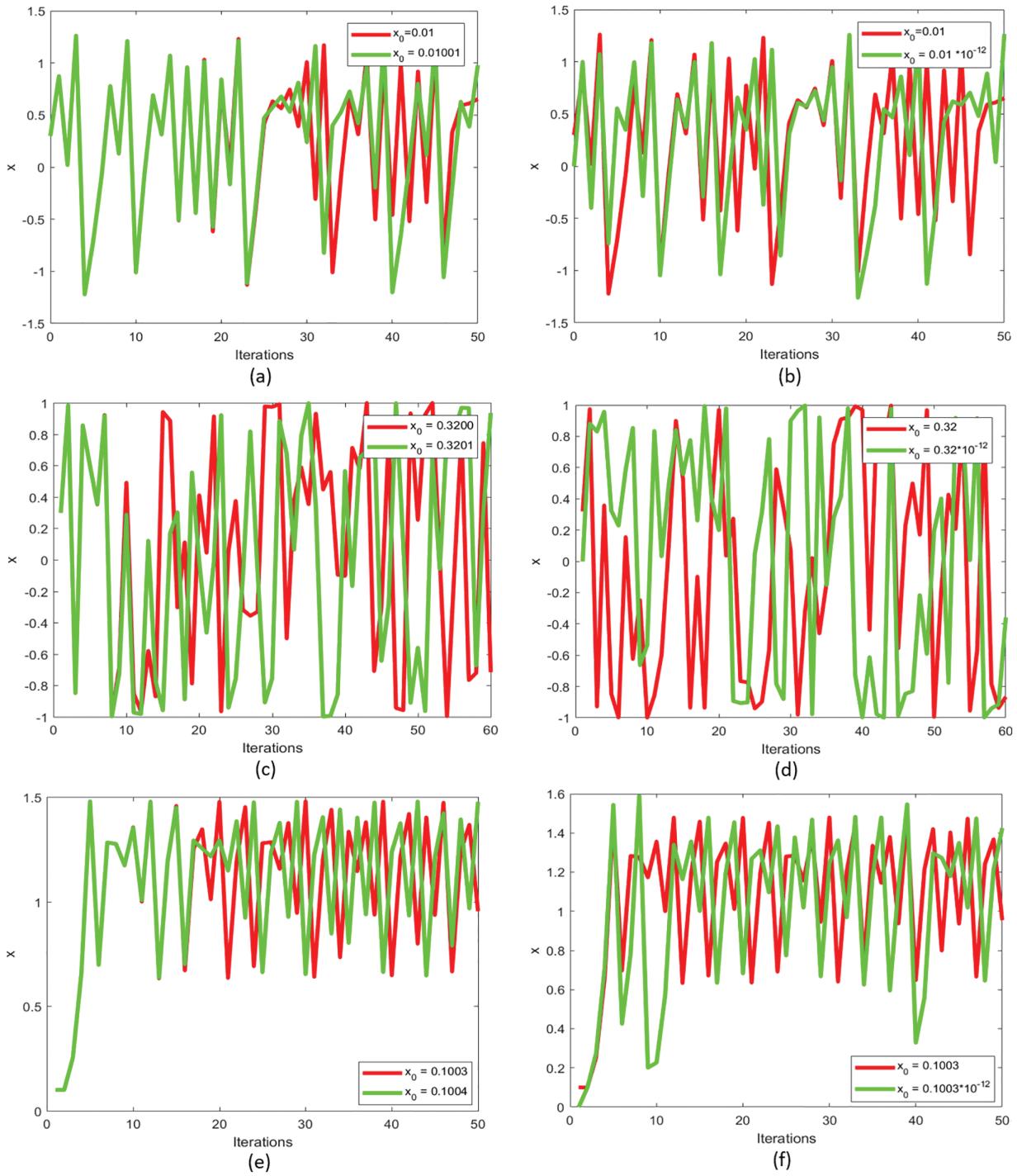

Figure 1: Sensitivity plots: (a, b) Henon map; (c, d) TD-ERCS map; and (e, f) Duffing map

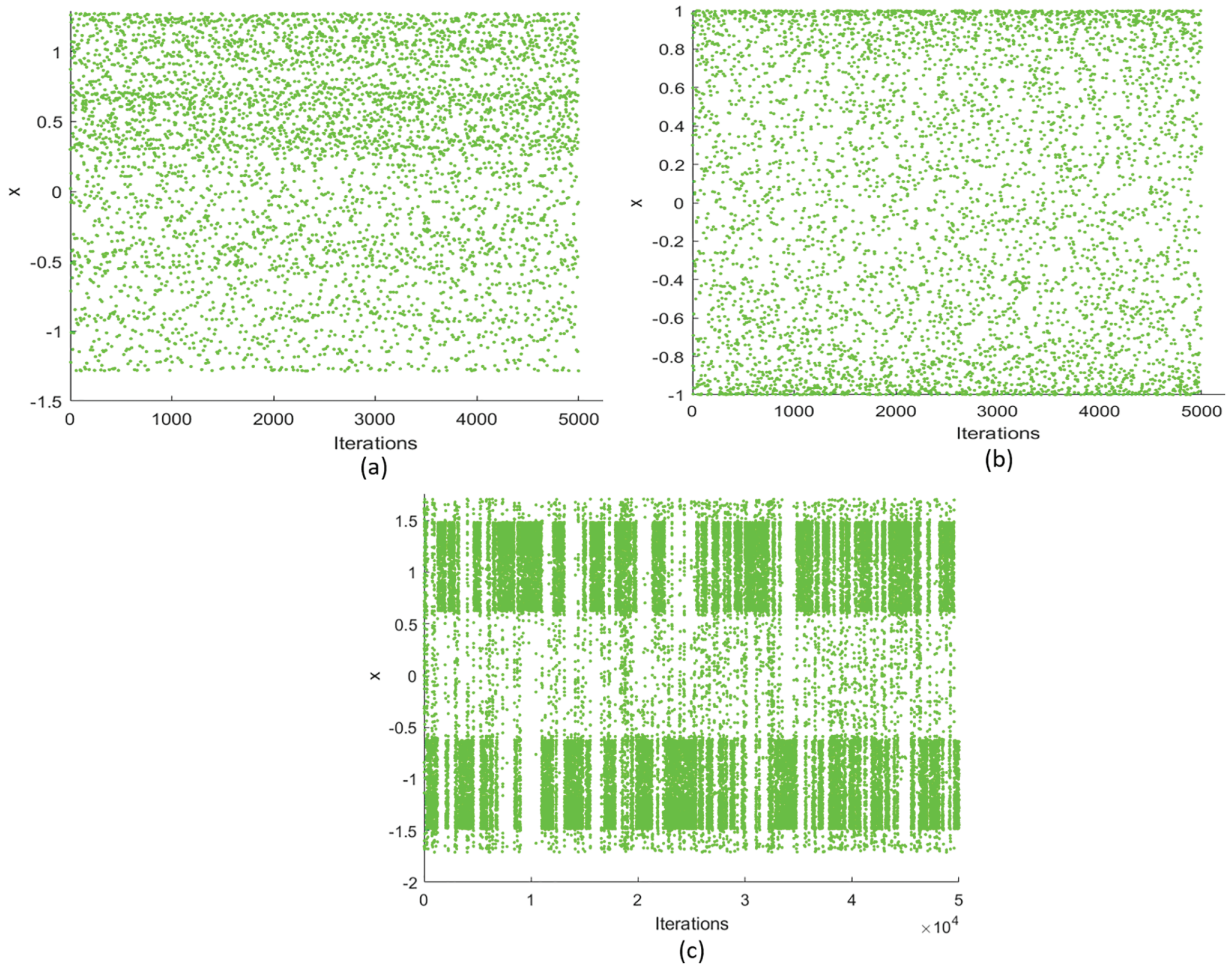

Figure 2: Random number plots: (a) Henon map; (b) TD-ERCS map; and (c) Duffing map

2.2 Tangent-Delay Ellipse Reflecting Cavity-Map

Li-Yuan et al. proposed TD-ERCS in 2004 [27]. It is a discreet chaotic map belonging to the class of two-dimensional chaotic maps. According to the authors in [28], TD-ERCS maps possess important properties, i.e., zero correlation in the total field, a Lyapunov exponent with a value greater than zero, and an unchangeable equiprobability distribution. Mathematically, the TD-ERCS map can be written as [29]:

$$
\begin{aligned}
x_n &= \frac{-\left[2k_{n-1}y_{n-1} + x_{n-1}\left(u^2 - k_{n-1}^2\right)\right]}{u^2 + k_{n-1}^2} \\
k_n &= \frac{2k'_{n-m} - k_{n-1} + k_{n-1}\left(k'_{n-1n}\right)^2}{1 + 2k_{n-1}k'_{n-m} - \left(k'_{n-m}\right)^2} \\
k'_{n-m} &= \begin{cases} -\dfrac{x_{n-1}}{y_{n-1}}\mu^2 & n < m \\ -\dfrac{x_{n-m}}{y_{n-m}}\mu^2 & n \geq m \end{cases} \\
y_n &= k_{n-1}x_n - k_{n-1}x_{n-1} + y_{n-1} \\
k'_0 &= -\frac{x_0}{y_0}\mu^2 \\
k_0 &= -\frac{\tan\alpha + k'_0}{1 - k'_0\tan\alpha}
\end{aligned}
\tag{2}
$$

whereas $(\mu, x_0, \alpha, n \text{ and } m)$ are TD-ERCS seed parameters and their values are $\mu \in (0,1]$, $x_0 \in [-1,1]$, $n = 1, 2, 3, \ldots$, $m = 2, 3, 4\ldots$ and $\alpha \in [0, \pi]$. The random number plot of the TD-ERCS map shows how it behaves and shapes under different parameters. With $x_0 = 0.3200$ and $x_0 = 0.3201$ or $x_0 = 0.32 \times 10^{-12}$, the map sensitivity is illustrated in Fig. 1c,d. Moreover, Fig. 2b shows 5000 random numbers generated through the TD-ERCS chaotic map. Fig. 1c,d shows that both the sets are random and the TD-ERCS chaotic map shows high sensitivity to a small change in the control parameters or initial conditions.

2.3 Duffing Map

A Holmes map or duffing chaotic map is a discrete-time chaotic system that maps points on a plane (x_n, y_n) to new points. It can be expressed mathematically as follows [30]:

$$
\begin{aligned}
x_{n+1} &= y_n \\
y_{n+1} &= -bx_n + ay_n - y_n^3
\end{aligned}
\tag{3}
$$

where x_0 and y_0 represent initial conditions of the map, whereas a and b are constant control parameters. This map shows chaotic behaviour for $a = 2.75$ and $b = 0.2$. Fig. 2c demonstrates 5000 random numbers generated through the Duffing map. For $x_0 = 0.1003$ and $x_0 = 0.1004$ or $x_0 = 0.1003 \times 10^{-12}$, Fig. 1e,f shows that both the sets are random and the duffing chaotic map is highly sensitive to minor variations in the initial parameters.

2.4 Deoxyribonucleic Acid DNA Sequence

The integral component of chromosomes is Deoxyribonucleic Acid (DNA). A DNA sequence is composed of Adenine (A), Thymine (T), Guanine (G), and Cytosine (C). Adenine, Thymine, Guanine, and Cytosine complement one another according to the Watson-Crick rule [31]. The nucleic acid database has the information of all the known nucleic acids. A permanent and unique ID number is assigned to every sequence known as the sequence code. More than 163 million unique DNA sequences are publicly available [32]. A DNA sequence can act as a natural password so it has its applications in image encryption. In this scheme, the DNA sequence code "NC012920" is used and is selected randomly from the publicly available DNA sequences.

2.5 Secure Hash Algorithm (SHA)

Secure Hash Algorithm abbreviated as SHA is a collection of cryptographic hash functions published by the National Institute of Standards and Technology as a recognized Federal Information Processing Standard (FIPS). Hash functions have their applications in generating pseudo-random numbers, speedy encryption, detection of a computer virus, verification of passwords and storage, etc. [33,34]. The SHA family consists of SHA-0, SHA-1, SHA-2, and SHA-3. SHA-2 is a family of SHA-256 and SHA-512, with the distinction of the word size only. The SHA-256 algorithm uses 32-byte words, while the SHA-512 algorithm uses 64-byte words. In the proposed algorithm SHA-512 is used. SHA-512 generates 512 bits or 128-character hash values.

3 The Proposed Scheme

All the images are grayscale, having pixel values between 0 and 255 for an 8-bit system. A flowchart depicting the proposed scheme is presented in Fig. 3. Each step of the scheme is described in detail as follows:

1. Let P be the plaintext image and W be the watermark image with dimensions $m \times n$, where m and n represent the image's rows and columns, respectively. For plaintext images P, $m = n = 1024$ and for watermark image W, the value is 256 for both m and n.

$$\begin{aligned} P &= plaintext\ image, \\ W &= Watermark\ image. \end{aligned} \tag{4}$$

2. The DNA sequence "NC012920", plaintext image P and watermark image W have been hashed using SHA-512 to generate α, β and γ, respectively.

$$\begin{aligned} \alpha &= SHA-512(NC012920), \\ \beta &= SHA-512(P), \\ \gamma &= SHA-512(R). \end{aligned} \tag{5}$$

3. The hash value α is utilized for the calculation of initial condition x_0 of TD-ERCS chaotic map and the map is iterated 256×256 times to get two vectors $\delta = \delta_1, \delta_2, \delta_3, ..., \delta_{256\times256}$ and $\varepsilon = \varepsilon_1, \varepsilon_2, \varepsilon_3, ..., \varepsilon_{256\times256}$.

$$\begin{aligned} \alpha_{decimal} &= bi2de(\alpha), \\ \alpha_0 &= \frac{\alpha_{decimal}}{2^{48}}. \end{aligned} \tag{6}$$

4. The vector δ is reshaped into a 256×256 matrix, multiplied with a larger number i.e., 10^{14} to increase its value, and then modified by applying 256 *Mod* operations so that all of the values are between zero and 255, and finally rounded to the nearest integer value by the floor function to obtain the matrix δ'. This can be summarized as:

$$\begin{aligned} \delta &= \begin{pmatrix} M_{11} & M_{12} & \dots & M_{1n} \\ M_{21} & M_{22} & \dots & M_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ M_{m1} & M_{m2} & \dots & M_{mn} \end{pmatrix}, \\ \delta' &= floor(Mod(10^{14} \times reshape(\beta, 256, 256)), 256). \end{aligned} \tag{7}$$

5. The δ' matrix and watermark image W are bitwise XORed to get matrix ζ.

$$\zeta = \delta' \oplus W. \tag{8}$$

6. A new vector A is generated by randomly selecting 256 values from the 256×256 ε vector. AsA values are arranged, the indices of the arranged values are stored in B which is a row matrix.

$$A = Random - vector_{1\times 256}. \tag{9}$$

7. The final ciphered watermarked image C_W is generated by reshaping the values stored in B into a 16×16 matrix (S-Box) and applying it to matrix ζ.

$$S - Box = \begin{pmatrix} B_{11} & B_{12} & \dots & B_{1n} \\ B_{21} & B_{22} & \dots & B_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ B_{m1} & B_{m2} & \dots & B_{mn} \end{pmatrix}, \tag{10}$$
$$C_W = S - Box(\zeta).$$

8. To embed the cipher watermark C_W, the pixel values are transformed into 8-bit binary and then separated into 4-bit groups: Most Significant Bits (MSBs) and Least Significant Bits (LSBs). LSBs and MSBs of four-bit binary values are transformed into decimal values and stored in MSB-matrix, and LSB-matrix, respectively. On the plaintext image P, the Lifting Wavelet Transform (LWT) is applied to produce LL, LH, HL, and HH matrices of size $(m/2) \times (n/2)$. Specifically, m and n represent the rows and columns of the plaintext image P. An embedded image E can be obtained by replacing plaintext image P's HL and HH matrices with MSB- and LSB-matrices of cipher watermark image C_w and applying inverse Lifting Wavelet Transform (ILWT).

$$\begin{aligned} &C_W(binary) = de2bi(C_W), \\ &LSB - matrix = C_W(binary)(1:4), \\ &MSB - matrix = C_W(binary)(5:8), \\ &[LL, LH, HL, HH] = lwt2(P), \\ &[LL, LH, HL, HH] = [LL, LH, LSB - matrix, MSB - matrix], \\ &E = ilwt2([LL, LH, LSB - matrix, MSB - matrix]). \end{aligned} \tag{11}$$

9. Since embedded image E has values greater than 255 and less than 0, a scaling function (min-max normalization) is applied to limit these values between 0 and 255.
10. The hash β is divided into two groups of 64 characters for computing the initial conditions x_0 and y_0 of the Henon chaotic map.

$$\begin{aligned} &[\beta_1\beta_2] = Split(\beta), \\ &x_{decimal} = bi2de(\beta_1), \\ &x_0 = \frac{x_{decimal}}{2^{48}}. \end{aligned} \tag{12}$$

$$\begin{aligned} &y_{decimal} = bi2de(\beta_2), \\ &y_0 = \frac{y_{decimal}}{2^{48}}. \end{aligned} \tag{13}$$

11. The Henon chaotic map is iterated 1024 times to generate two sets of random values that are $\omega = \omega_1, \omega_2, \omega_3, \dots, \omega_{1024}$ and $\psi = \psi_1, \psi_2, \psi_3, \dots, \psi_{1024}$.

12. Using ω and ψ, the embedded image E is permuted row- and column-wise to get the shuffled image S.

$$\begin{aligned} Row - per &= \omega(E), \\ S &= \psi(Row - per). \end{aligned} \tag{14}$$

13. The hash γ is utilized to calculate the initial conditions of the duffing chaotic map. The first 64 characters are used to calculate x_0 and the remaining are used to compute y_0.

$$\begin{aligned} [\gamma_1\gamma_2] &= Split(\gamma), \\ x_{decimal} &= bi2de(\gamma_1), \\ x_0 &= \frac{x_{decimal}}{2^{48}}. \end{aligned} \tag{15}$$

$$\begin{aligned} y_{decimal} &= bi2de(\gamma_2), \\ y_0 &= \frac{y_{decimal}}{2^{48}}. \end{aligned} \tag{16}$$

14. The duffing map is iterated 1024×1024 to generate $\sigma = \sigma_1, \sigma_2, \sigma_3, ..., \sigma_{1024\times1024}$ and $\tau = \tau_1, \tau_2, \tau_3, ..., \tau_{1024\times1024}$ vectors.
15. The same functions are applied on vector σ as in step (4) except that it is reshaped into 1024×1024 matrix to get matrix ρ.
16. The shuffled image S and ρ are bit wise XORed to obtain λ.

$$\lambda = S \oplus \rho. \tag{17}$$

17. Another 16×16 random S-Box is generated from the vector τ, the same way as in step (7), and applied on the matrix λ to get the final ciphertext image C.

$$\begin{aligned} S - Box &= \begin{pmatrix} \tau_{11} & \tau_{12} & \dots & \tau_{1n} \\ \tau_{21} & \tau_{22} & \dots & \tau_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{m1} & \tau_{m2} & \dots & \tau_{mn} \end{pmatrix}, \\ C &= S - Box(\rho). \end{aligned} \tag{18}$$

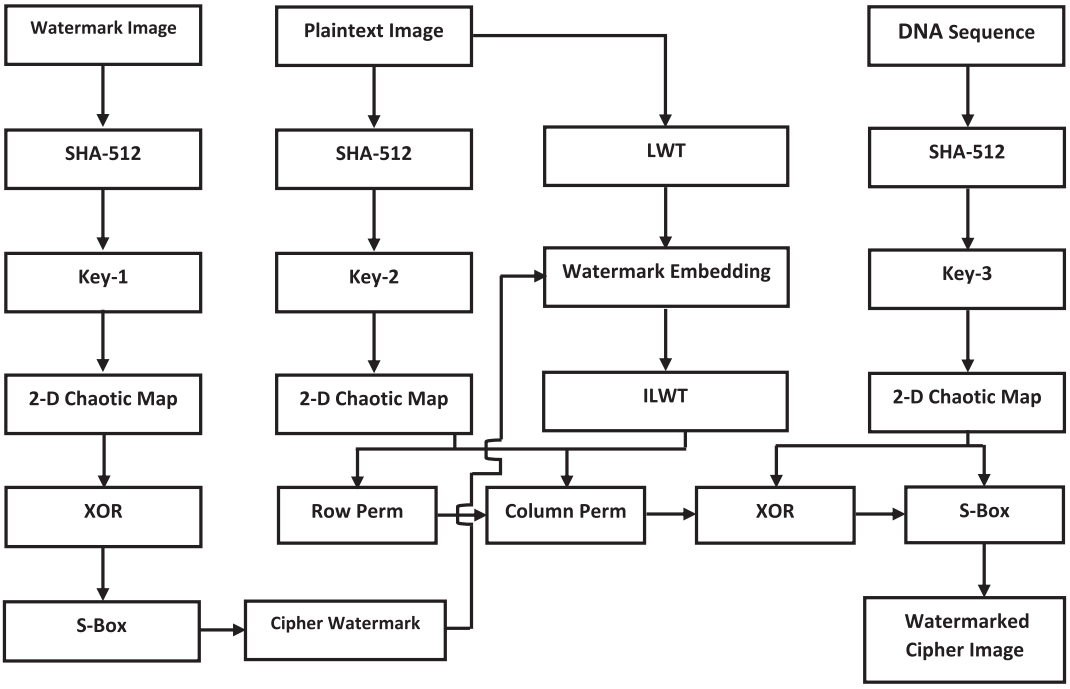

Figure 3: Flowchart detailing the outlined scheme

4 Results

Numerous security metrics are used to test the efficacy of the designed algorithm. Tests are conducted on a system with Microsoft Windows 10 operating system, 4 GB memory, 1 GHz CPU, and MATLAB 2018a. A Baboon image of size 256 × 256 is used as a watermark image, and six satellite images of size 1024 × 1024 are used as plaintext images. Fig. 4 illustrates plaintext original images and their respective histograms, while Fig. 5 shows ciphertext images along with their histograms.

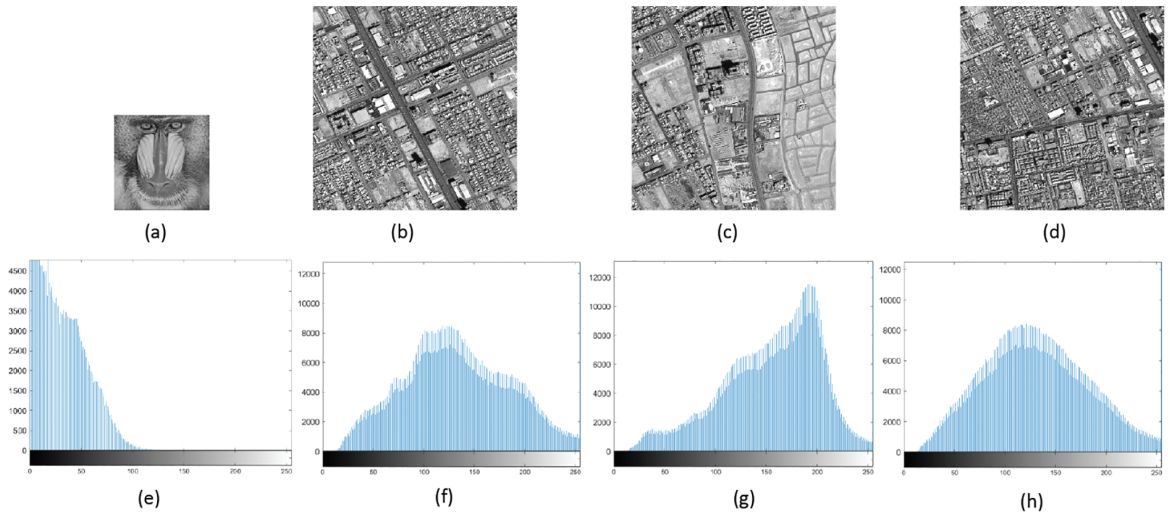

Figure 4: (Continued)

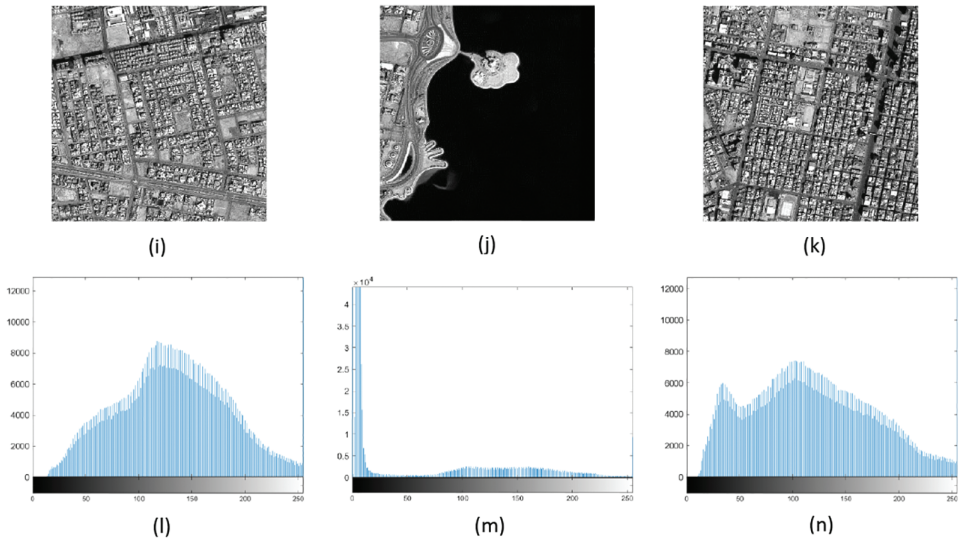

Figure 4: Results: (a, b, c, d, i, j, and k) are the plaintext Baboon watermark image, Satellite images 1, 2, 3, 4, 5, and 6, while (b, c, d, e, f, g, h, l, m, and n) are the histograms

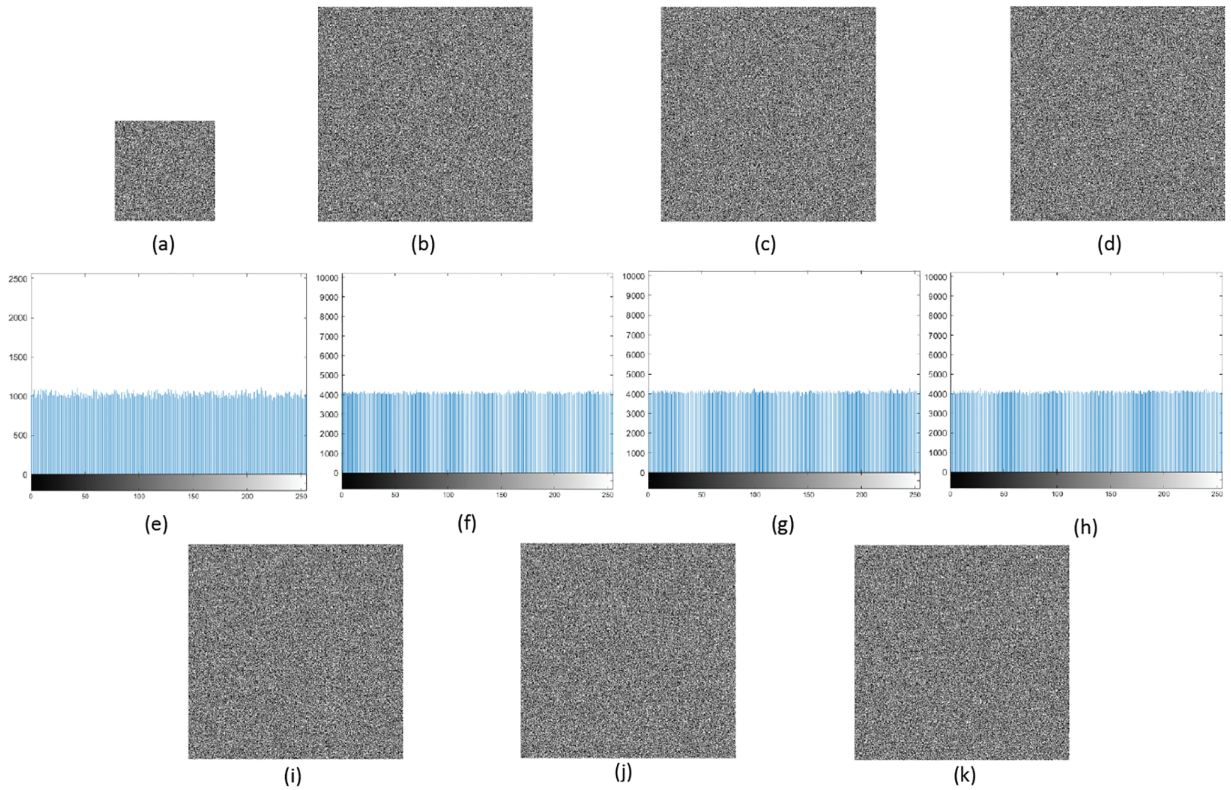

Figure 5: (Continued)

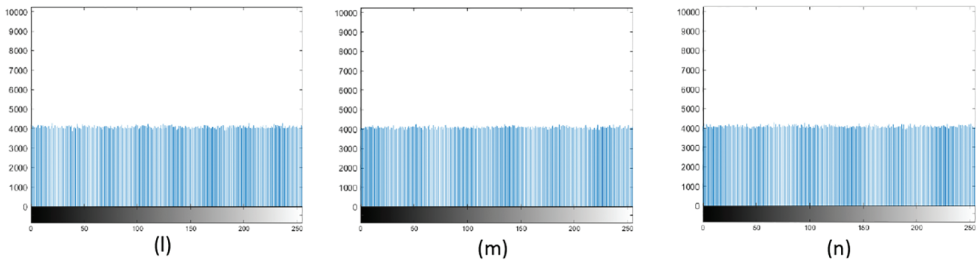

Figure 5: Results: (a, b, c, d, i, j, and k) are the ciphertext Baboon watermark image, Satellite images 1, 2, 3, 4, 5, and 6, while (b, c, d, e, f, g, h, l, m, and n) are the histograms

4.1 Statistical Attack Analysis

4.1.1 Correlation Analysis

The correlation test determines how similar the two variables are. An encryption scheme's effectiveness (quality) can be evaluated using this test. Let u and v symbolize a pair of neighbouring grayscale pixels in each plaintext and ciphertext image. It can be mathematically calculated as [35]:

$$C(u,v) = \frac{\frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))(v_i - E(v))}{\sigma_u \times \sigma_v} \tag{19}$$

where

$$\sigma_u = \sqrt{Var(u)}$$

$$\sigma_v = \sqrt{Var(v)}$$

$$Var(u) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))^2$$

$$Var(v) = \frac{1}{N}\sum_{i=1}^{N}(v_i - E(v))^2$$

The notation $C(u,v)$ computes the covariance of the grayscale values of the two plaintext and encrypted image pixels, u and v. Similarly, $Var(u)$, σ_u, and E calculate the variance, standard deviation, and expected operator, respectively. The N computes the total number of pixels. The correlation coefficient is calculated for neighbouring pixels in vertical, horizontal, and diagonal orientations across the image, utilizing 5000 random pixels. Table 1 contains the calculated correlation coefficient values. The correlation coefficients are nearly zero for the encrypted images, whereas they are almost equal to one for the plain images. Moreover, comparable distributions of pixels for satellite plaintext image 1 and the corresponding ciphertext image in the coordinate system are shown in Fig. 6. The correlation coefficient values presented in Table 1 and the evenly distributed correlation plots depicted in Fig. 6 validate the effectiveness and reliability of the proposed algorithm. Considering the favourable correlation properties and uniform distribution of the ciphertexts, these results suggest that the proposed algorithm has good resilience to statistical attacks.

Table 1: Calculated values for the correlation coefficient

Image	Direction	Plaintext	Ciphertext
Satellite image 1	Hor	0.9173	−0.0598
	Ver	0.8868	0.0386
	Dia	0.7851	0.0239
Satellite image 2	Hor	0.9526	−0.0339
	Ver	0.9329	0.0582
	Dia	0.8817	−0.0033
Satellite image 3	Hor	0.9268	−0.0229
	Ver	0.8988	−0.0070
	Dia	0.8211	0.0429
Satellite image 4	Hor	0.8971	−0.0401
	Ver	0.8826	−0.0223
	Dia	0.8125	−0.0405
Satellite image 5	Hor	0.9922	0.0193
	Ver	0.9869	−0.0021
	Dia	0.9849	0.0431
Satellite image 6	Hor	0.9080	0.0143
	Ver	0.9121	0.0483
	Dia	0.8552	−0.0240
[36]	Hor	–	−0.0016
	Ver	–	−0.0003
	Dia	–	−0.0025
[37]	Hor	–	0.0043
	Ver	–	−0.0024
	Dia	–	−0.0014

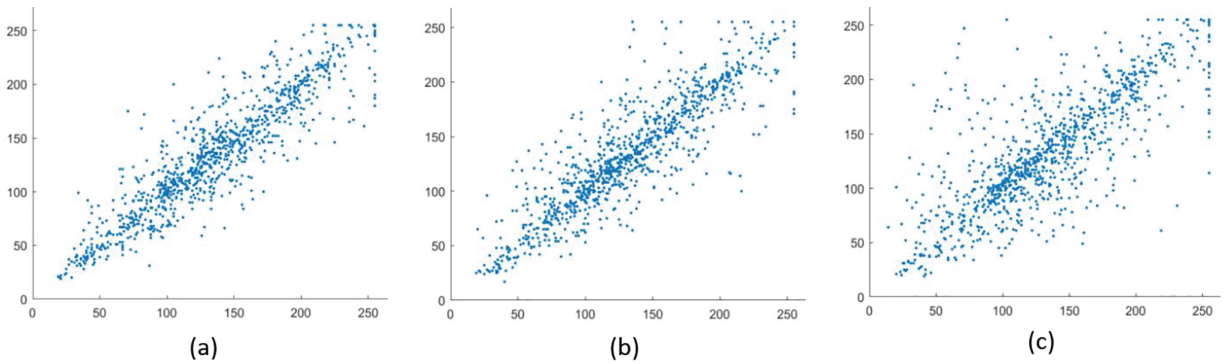

Figure 6: (Continued)

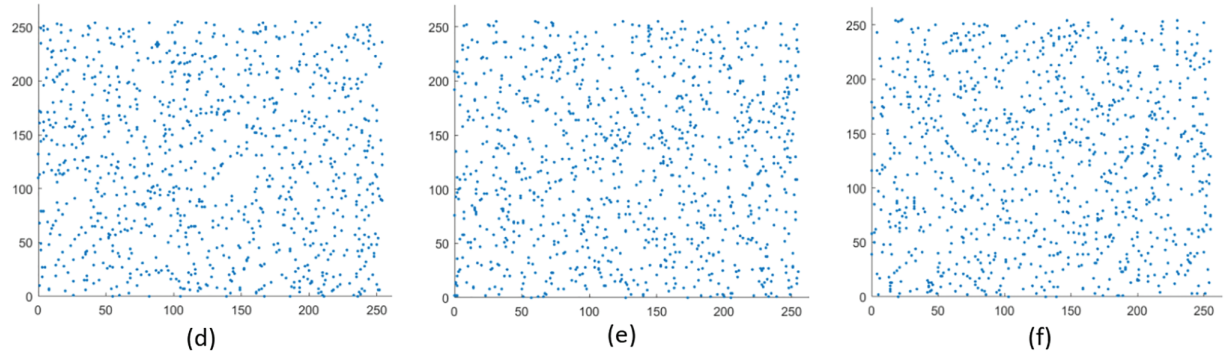

Figure 6: Correlation plots of Sattelite image1: The (a), (b), and (c) are plaintext plots while (d), (e), and (f) are ciphertext plots in horizontal, vertical, and diagonal directions, respectively

4.1.2 Histogram Analysis

A histogram of an image illustrates the dispersion of pixel values using significant statistical features. Histogram analysis is used to find the statistical strength of an image encryption scheme. An efficient encryption algorithm generates an encrypted image with a flat histogram without sharp peaks. The histograms of plaintext and ciphertext watermark Baboon image and six satellite images are generated and displayed in Figs. 4 and 5, respectively. The sharp peaks in histograms are easily visible in Fig. 4 (e, f, g, h, l, m, and n) while Fig. 5 (e, f, g, h, l, m, and n) confirms that the encrypted images histograms are almost flat and uniformly distributed. Accordingly, the proposed scheme conceals all aspects of plaintext images and can withstand statistical attacks.

4.2 Key Analysis

A key analysis in chaotic image encryption involves examining and evaluating the cryptographic keys used to encrypt the images. A key space analysis and a key sensitivity analysis are therefore conducted and explained in more detail.

4.2.1 Key Space Analysis

In this analysis, a cryptosystem's resistance to brute-force attacks is calculated. Key space generally means the size of the keys employed in the system. An efficient cryptosystem must have a large key space capable of resisting brute-force attacks. For a cryptosystem, the key space should be greater than 2^{100} [38]. Three chaotic maps are used in the proposed scheme, each with two initial conditions and two control parameters. Therefore, the key space for the proposed scheme can be computed as follows [17]:

$$Keyspace = (10^{15} \times 10^{15} \times 10^{15} \times 10^{15}) \tag{20}$$

$$Keyspace = (10^{60})^3 = 10^{180} \tag{21}$$

$$Keyspace \approx 2^{598} \tag{22}$$

Thus, one can conclude that with the available computational power, the computed key space is fairly large enough to withstand any brute-force attack.

4.2.2 Key Sensitivity Analysis

This analysis is used to assess the effects of modifications to a system's key variables or input parameters on its output. An image encryption process must undergo sensitivity analysis to be evaluated for security and resilience. Thus, the designed image encryption system must have greater sensitivity so that even a small modification in one of the encryption keys during the encryption and decryption process must produce a dissimilar ciphertext image. For the demonstration of the proposed scheme key sensitivity, let's change the initial condition x_0 from 0.3200 to 0.3201 or 0.3200×10^{-12} for the TD-ERCS map. A small modification by changing x_0 to 0.3201 or 0.3200×10^{-12} produces very different random numbers from those generated when x_0 was 0.3200. One can also confirm the sensitivity of the utilized maps from Fig. 1. The plots in Fig. 7 illustrate decrypted images with the original key, changed key, and differential image. Consequently, it may be concluded from the differential image that the images produced using the same and changed keys differ from one another and include no recognizable information about the original plaintext image. Therefore, one can conclude that the proposed image encryption has extraordinary sensitivity to the slightest modification in one of the initial conditions or control parameters.

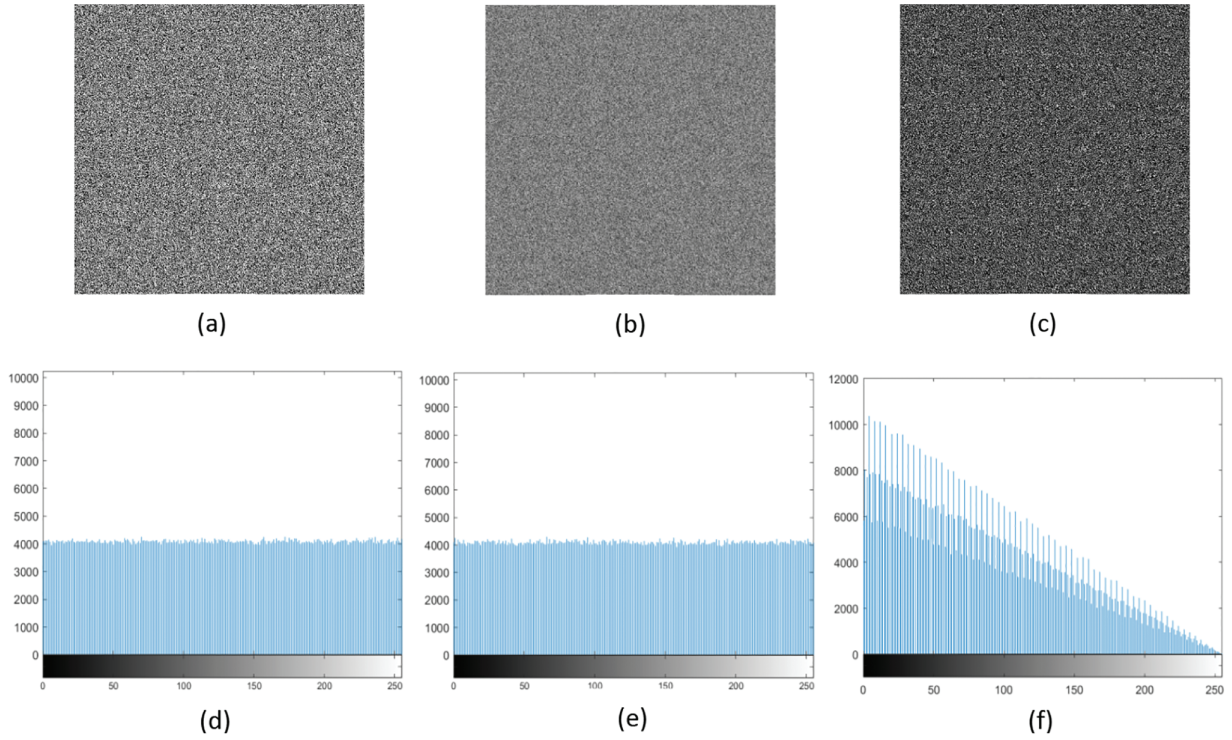

Figure 7: Key sensitivity plots: (a) First ciphertext; (b) second ciphertext with changed key; (c) differential image; (d) histogram of (a); (e) histogram of (b); (f) histogram of (c)

4.3 Entropy Analysis

Entropy is a quantitative metric and can be used to assess the level of unpredictability or randomness present in a given dataset or image. Entropy analysis is an essential tool for evaluating how well an encryption technique hides the underlying image data and how resistant it is to brute-force attacks when it comes to image encryption. Strong image encryption techniques require ciphertext images to have a high entropy value, giving them the impression of randomness. On the other hand, if the encryption method is not up

to par, the ciphertext image could show recognizable structures or patterns that could be used as a means of recovering the original image data. Shannon entropy $E(i)$ is a mathematical measure used to accurately measure the entropy of an image and is computed as follows [39]:

$$E(i) = -\sum_{i=0}^{255}(E(i) \times \log_2(E(i))) \tag{23}$$

Table 2 displays the results of the proposed scheme entropy evaluation. These high entropy values of the proposed image encryption system have thus made it resistant to possible brute-force attacks.

Table 2: Computed entropy values

Image type	Plaintext	Ciphertext
Satellite image 1	7.6414	7.9998
Satellite image 2	7.5128	7.9987
Satellite image 3	7.6350	7.9989
Satellite image 4	7.6154	7.9976
Satellite image 5	5.3267	7.9986
Satellite image 6	7.7010	7.9992
[36]	–	7.9998
[37]	–	7.9989

4.4 Differential Attack Analysis

An image encryption method can undergo evaluation through a differential attack to assess its resilience against changes in the pixel values of the plaintext image. The attacker compares two output images to determine the difference between them, so if the difference is significant, then the designed scheme is resilient to differential attack [39]. There are two tests for the evaluation of differential attack: Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI). The UACI test evaluates how much the pixel intensities differ between two images that have undergone encryption, rather than focusing on how often the number of pixels changes in the encrypted image when a single pixel in the original image is altered. NPCR measures how frequently the number of pixels changes when one pixel is changed in the plaintext. Mathematically NPCR and UACI can be computed as [39]:

$$NPCR = \frac{\sum_{x,y} \triangle(x,y)}{M \times N} \times 100, \tag{24}$$

$$UACI = \frac{1}{M \times N} \times \sum_{x,y} \frac{|C^*(x,y) - C(x,y)|}{255}, \tag{25}$$

where

$$\triangle(x,y) = \begin{cases} 0 & \text{if } C^*(x,y) = C(x,y), \\ 1 & \text{if } C^*(x,y) \neq C(x,y). \end{cases}$$

The variable C^* is the ciphertext image generated by altering a single pixel of the original image. The computed NPCR and UACI values are tabulated in Table 3. The values of UACI (greater than 33%) and NPCR (greater than 99%) indicate that the developed algorithm has a higher level of differential attack resistance.

Table 3: Computed NPCR and UACI values

Image type	NPCR	UACI
Satellite image 1	99.6653%	33.5328%
Satellite image 2	99.5948%	33.4387%
Satellite image 3	99.6359%	33.4432%
Satellite image 4	99.5833%	33.3367%
Satellite image 5	99.5921%	33.3861%
Satellite image 6	99.6435%	33.4176%
[36]	99.6300%	33.4400%
[37]	99.6161%	33.8537%

4.5 Visual Strength Analysis

4.5.1 Energy

Analyzing the energy distribution of an image can provide insight into the encryption method's effectiveness and security. In a digital image, each pixel's intensity or magnitude determines the energy distribution. Therefore, this test identifies the uniformity and predictability of energy distribution in ciphertext images. Mathematically energy can be represented as follows [17]:

$$E = \sum_{i,j} Q(i,j)^2. \tag{26}$$

where i and j represent the position of the pixel. Table 4 shows the calculated energy test values. Thus, ciphertext images with low energy values indicate high encryption quality.

Table 4: Computed values of energy, contrast, and homogeneity

	Energy		Contrast		Homogeneity	
Image type	**Plaintext**	**Ciphertext**	**Plaintext**	**Ciphertext**	**Plaintext**	**Ciphertext**
Satellite image 1	0.0666	0.0156	0.6302	10.5154	0.7901	0.3887
Satellite image 2	0.1067	0.0156	0.3871	10.5268	0.8536	0.3894
Satellite image 3	0.0711	0.0156	0.5702	10.4879	0.7981	0.3896
Satellite image 4	0.0718	0.0156	0.6172	10.5268	0.7997	0.3895
Satellite image 5	0.5050	0.0156	0.1228	10.4914	0.9529	0.3896
Satellite image 6	0.0594	0.0156	0.7115	10.5070	0.7859	0.3886

4.5.2 Contrast

In image encryption, contrast analysis determines how well images retain contrast. Across different regions of an image, this analysis determines if an image encryption algorithm maintains relative variations in pixel intensities and contrast levels. Mathematically, it is calculated as [17]:

$$C = \sum_{i,j} (|i-j|)^2 Q(i,j). \tag{27}$$

where i and j represent the pixel position. The computed contrast test values are tabulated in Table 4. Thus, it can be concluded that the ciphertext image with larger contrast values indicates a large variation in the generated ciphertext image, hence the proposed scheme is highly effective.

4.5.3 Homogeneity

Pixel homogeneity is a measure of consistency or uniformity of pixel values. An image is often evaluated by comparing the intensity of pixels within it, especially in examining textures and patterns. A small value is an indication of more variation or heterogeneity in the image, while a larger value indicates a more uniform distribution of pixel intensities. Mathematically, homogeneity can be interpreted as [17]:

$$H = \sum_{i,j} \frac{Q(i,j)}{1 + |i - j|}. \tag{28}$$

where i and j represent the pixel position. For the designed image encryption scheme, the calculated homogeneity values are tabulated in Table 4. The ciphertext image with higher homogeneity values indicates a more uniform distribution of pixel intensities and high-quality encryption.

4.6 Robustness Analysis

4.6.1 Occlusion Attack Analyis

Communication over a transmission medium can result in the loss of some part of an image or a change by an attacker. The encryption scheme must have enough robustness to decrypt images that have experienced lossy changes. A cropping attack is illustrated in Fig. 8 by removing 50 × 50 pixels from the ciphertext image to see how well the designed image encryption withstands a cropping attack. The decryption is carried out on the occluded image and the results are illustrated in Fig. 8. It is interesting to note that the recovered image successfully preserves the original data, illustrating the encryption scheme's effectiveness and robustness against occlusion attacks. As a result of this observation, the encryption technique proves to be resilient in maintaining data integrity during transmission, regardless of notable modifications.

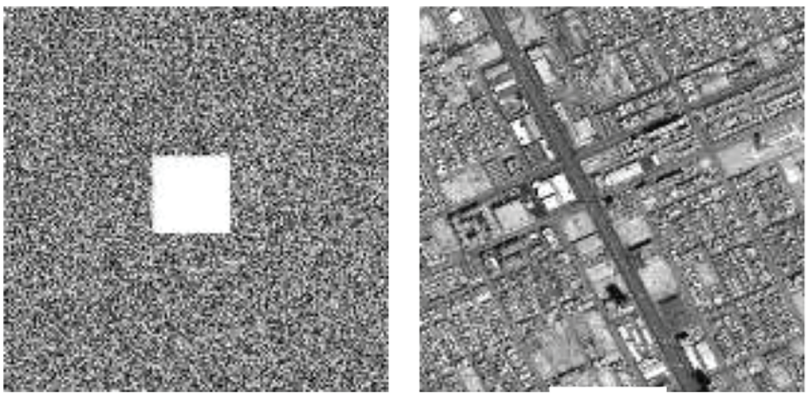

Figure 8: Occlusion attack: (a) occluded encrypted image; (b) decrypted image

4.6.2 Noise Attack Analysis

Noise interference can affect ciphertext images during transmission and storage. A strong encryption scheme must therefore be immune to noise interference. We evaluated the anti-noise performance of the designed algorithm on one of the encrypted satellite images by adding salt and pepper noise. A noisy satellite image is decrypted, and the result is shown in Fig. 9. Hence, the decrypted image preserves the original data, illustrating how robust the encryption scheme is.

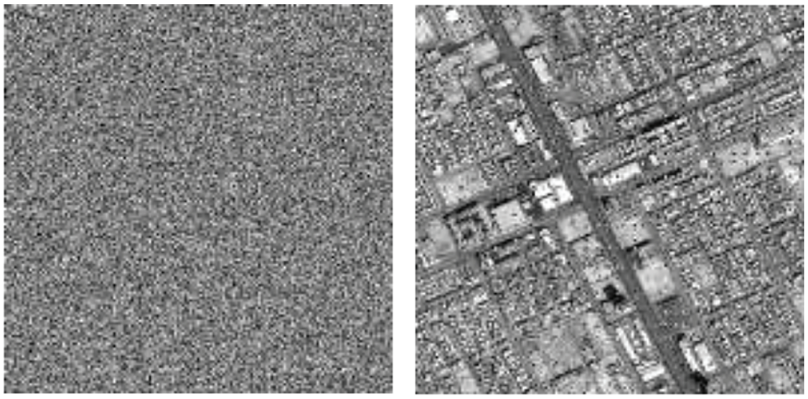

Figure 9: Noise attack: (a) polluted encrypted image; (b) decrypted image

4.6.3 Classical Attack Analysis

This section examines a wide range of attack methodologies at the ciphered image, including known-plaintext, chosen-plaintext, ciphertext-only, and chosen-ciphertext attacks. Three different chaotic maps are employed to produce confusing and diffuse vectors and matrices. SHA-512 hashes of watermark images, plaintext images, and DNA sequences are used to compute the keys (initial conditions and control parameters) of chaotic maps. The Watermark image is then encrypted using the TD-ERCS map and embedded in the plaintext image. The embedded plaintext image is permuted row- and column-wise using the Henon map. Following the permutation, the values from the duffing map are XORed with the permuted image. The XORed image security is further enhanced by applying a dynamic S-Box. A single-pixel change in the plaintext image, watermark image or DNA sequence will alter the resulting keystream, resulting in a completely different ciphertext image. As a result of the reliance on watermark images, plaintext images, and DNA sequences, as well as confusion and diffusion properties, the developed image encryption can resist classical attacks.

4.7 Computational Complexity Analysis

Tests are conducted on a system with the Microsoft Windows 10 operating system, 4 GB memory, 1 GHz CPU, and MATLAB2018a. In addition to the watermark image of 256 × 256, six satellite images of 1024 × 1024 are used as plaintext images. There are three main parts to the proposed scheme: (a) Encryption of watermark images, (b) Embedding, and (c) Final encryption. Watermark image encryption takes 0.2021 seconds, the embedding phase takes 3.7445 s while the final encryption takes 0.6277 s. Thus, to produce the final ciphertext image, the proposed scheme takes 4.5743 s. In [36], the satellite image encryption scheme takes 8 s for encryption or decryption. The satellite image encryption scheme presented in [37] encrypts an

image in 0.983 s. The proposed watermarked satellite image encryption takes more time due to the watermark embedding phase.

5 Conclusion

A novel satellite watermarked image encryption scheme is proposed. The initial conditions (key) for TD-ERCS, Henon, and Duffing chaotic maps are generated by applying the hash algorithm SHA-512 to watermark images, DNA sequences, and plaintext images, respectively. The Watermark image is encrypted using TD-ERCS and embedded in plaintext. The embedded plaintext image is permuted row-wise and column-wise using the Henon map and then XORed with the random matrix of the same size generated through the Duffing map. A dynamic S-Box was generated and applied to the XORed image to enhance security. To verify the robustness and superiority of the proposed watermarked image encryption scheme, a thorough security analysis is performed. To confirm the robustness and strength of the proposed satellite watermarked image encryption scheme, statistical analyses (correlation and histogram), key analyses (key space and key sensitivity), entropy analyses, differential attack analyses (NPCR and UACI), visual strength analyses (energy, contrast, and homogeneity), robustness analyses (cropping, noise, and classical attacks) are carried out which lead one to the conclusion that the suggested strategy is immune to any prospective attacks. Moreover, a possible limitation of the scheme could be the computational complexity. As the size of images increases, the overall encryption process could take more time.

Acknowledgement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through the large group research project under grant number *RGP*2/461/45. The authors are thankful to the Deanship of Graduate Studies and Scientific Research at the University of Bisha for supporting this work through the Fast–Track Research Support Program. The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, Saudi Arabia for funding this research work through the project number $NBU - FFR - 2025 - 3030 - 05$.

Funding Statement: This study is supported by the Deanship of Scientific Research at King Khalid University for funding this work through the large group research project under grant number *RGP*2/461/45 and the Deanship of Scientific Research at Northern Border University, Arar, Saudi Arabia for funding this research work through the project number $NBU - FFR - 2025 - 3030 - 05$.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Mohamed Medani, Yahia Said, Nashwan Adnan Othman, Mohamed Kchaou; data collection: Mohamed Medani, Yahia Said, Farrukh Yuldashev, Faisal Khaled Aldawood; analysis and interpretation of results: Bacha Rehman, Nashwan Adnan Othman, Farrukh Yuldashev, Mohamed Kchaou; draft manuscript preparation: Mohamed Medani, Yahia Said, Faisal Khaled Aldawood, Bacha Rehman. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: All data generated or analyzed during this study are included in this published article.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Xi Y, Li T, Wang H, Li Y, Tarkoma S, Hui P. Beyond the first law of geography: learning representations of satellite imagery by leveraging point-of-interests. In: Proceedings of the ACM Web Conference 2022; 2022; Lyon, France. p. 3308–16.

2. Zhang H, Xu Y, Luo R, Mao Y. Fast GNSS acquisition algorithm based on SFFT with high noise immunity. China Commun. 2023;20(5):70–83. doi:10.23919/JCC.2023.00.006.
3. Banu R, Vladimirova T. Fault-tolerant encryption for space applications. IEEE Transact Aeros Electr Syst. 2009;45(1):266–79. doi:10.1109/TAES.2009.4805278.
4. Singh AK, Thakur S, Jolfaei A, Srivastava G, Elhoseny M, Mohan A. Joint encryption and compression-based watermarking technique for security of digital documents. ACM Transact Inte Technol. 2021;21(1):1–20. doi:10.1145/3414474.
5. Abikoye O, Adewole K, Oladipupo A. Efficient data hiding system using cryptography and steganography. Int J Appl Inform Syst. 2012;4(11):6–11. doi:10.5120/ijais12-450763.
6. Shannon CE. Communication theory of secrecy systems. The Bell Syst Techn J. 1949;28(4):656–715. doi:10.1002/j.1538-7305.1949.tb00928.x.
7. Zhang B, Liu L. Chaos-based image encryption: review, application, and challenges. Mathematics. 2023;11(11):2585. doi:10.3390/math11112585.
8. Wang M, Fu X, Yan X, Teng L. A new chaos-based image encryption algorithm based on discrete fourier transform and improved joseph traversal. Mathematics. 2024;12(5):638. doi:10.3390/math12050638.
9. Zhou S, Wei Y, Zhang Y, Iu HHC, Zhang H. Image encryption algorithm based on the dynamic RNA computing and a new chaotic map. Integration. 2025;101(1):102336. doi:10.1016/j.vlsi.2024.102336.
10. Khan MS, Ahmad J, Al-Dubai A, Pitropakis N, Driss M, Buchanan WJ. A Novel Cosine-modulated-polynomial chaotic map to strengthen image encryption algorithms in IoT environments. Procedia Comput Sci. 2024;246:4214–23. doi:10.1016/j.procs.2024.09.261.
11. Su Y, Wang X. A robust visual image encryption scheme based on controlled quantum walks. Phy A: Statist Mech Applicat. 2022;587:126529. doi:10.1016/j.physa.2021.126529.
12. Zheng S, Liu C, Feng Z, Chen R, Liu X. Visual image encryption scheme based on vector quantization and content transform. Multim Tools Applicat. 2022;81(9):12815–32. doi:10.1007/s11042-022-12583-y.
13. Zhu S, Deng X, Zhang W, Zhu C. Secure image encryption scheme based on a new robust chaotic map and strong S-box. Mathem Comput Simulat. 2023;207(8):322–46. doi:10.1016/j.matcom.2022.12.025.
14. Çavuşoğlu Ü, Kaçar S, Pehlivan I, Zengin A. Secure image encryption algorithm design using a novel chaos based S-Box. Chaos Solit Fract. 2017;95(11):92–101. doi:10.1016/j.chaos.2016.12.018.
15. Khan JS, Kayhan SK, Ahmed SS, Ahmad J, Siddiqa HA, Ahmed F, et al. Dynamic S-box and PWLCM-based robust watermarking scheme. Wireless Pers Commun. 2022;125(1):513–30. doi:10.1007/s11277-022-09562-9.
16. Kadhim Q, Al-Jawher WAM. A new multiple-chaos image encryption algorithm based on block compressive sensing, swin transformer, and wild horse optimization. Multidiscip Sci J. 2025;7(1):2025012–2. doi:10.31893/multiscience.2025012.
17. Khan JS, Kayhan SK. Chaos and compressive sensing based novel image encryption scheme. J Inf Secur Appl. 2021;58(4):102711. doi:10.1016/j.jisa.2020.102711.
18. Zou C, Wang X, Zhou C, Xu S, Huang C. A novel image encryption algorithm based on DNA strand exchange and diffusion. Appl Math Comput. 2022;430(2):127291. doi:10.1016/j.amc.2022.127291.
19. Rahul B, Kuppusamy K, Senthilrajan A. Dynamic DNA cryptography-based Image Encryption Scheme using Multiple Chaotic Maps and SHA-256 hash function. Optik. 2023;289:171253. doi:10.1016/j.ijleo.2023.171253.
20. Gao X, Mou J, Banerjee S, Zhang Y. Color-gray multi-image hybrid compression-encryption scheme based on BP neural network and knight tour. IEEE Transact Cybernet. 2023;53(8):5037–47. doi:10.1109/TCYB.2023.3267785.
21. Guo Z, Chen SH, Zhou L, Gong LH. Optical image encryption and authentication scheme with computational ghost imaging. Appl Mathem Model. 2024;131(6):49–66. doi:10.1016/j.apm.2024.04.012.
22. Khan MS, Ahmad J, Al-Dubai A, Pitropakis N, Ghaleb B, Ullah A, et al. Chaotic quantum encryption to secure image data in post quantum consumer technology. IEEE Trans Consum Electron. 2024;70(4):7087–101. doi:10.1109/TCE.2024.3415411.
23. Ma X, Wang Z, Wang C. An image encryption algorithm based on Tabu Search and hyperchaos. Int J Bifurcat Chaos. 2024;34(14):2450170. doi:10.1142/S0218127424501700.

24. Kong X, Yu F, Yao W, Cai S, Zhang J, Lin H. Memristor-induced hyperchaos, multiscroll and extreme multistability in fractional-order HNN: image encryption and FPGA implementation. Neural Netw. 2024;171(1):85–103. doi:10.1016/j.neunet.2023.12.008.
25. Alexan W, Chen YL, Por LY, Gabr M. Hyperchaotic maps and the single neuron model: a novel framework for chaos-based image encryption. Symmetry. 2023;15(5):1081. doi:10.3390/sym15051081.
26. Hénon M. A two-dimensional mapping with a strange attractor. In: The theory of chaotic attractors. New York, NY, USA: Springer; 1976. p. 94–102.
27. Sheng LY, Sun KH, Li CB. Study of a discrete chaotic system based on tangent-delay for elliptic reflecting cavity and its properties. Acta Physica Sinica. 2004;53(9):2871–6. doi:10.7498/aps.53.2871.
28. Sheng LY, Cao LL, Sun KH, Wen J. Pseudo-random number generator based on TD-ERCS chaos and its statistic characteristics analysis. Acta Physica Sinica. 2005;54(9):4031–7. doi:10.7498/aps.54.4031.
29. Zhang K, Fang J-B. Color image encryption algorithm based on TD-ERCS system and wavelet neural network. Math Probl Eng. 2015;2015(11):1–10. doi:10.1155/2015/501054.
30. Dhopavkar TA, Nayak SK, Roy S. IETD: a novel image encryption technique using Tinkerbell map and Duffing map for IoT applications. Multim Tools Applicat. 2022;81(30):43189–228. doi:10.1007/s11042-022-13162-x.
31. Movafegh Ghadirli H, Nodehi A, Enayatifar R. Color image DNA encryption using mRNA properties and non-adjacent coupled map lattices. Multim Tools Applicat. 2021;80(6):8445–69. doi:10.1007/s11042-020-10014-4.
32. Khan JS, Ahmad J, Ahmed SS, Siddiqa HA, Abbasi SF, Kayhan SK. DNA key based visual chaotic image encryption. J Intell Fuzzy Syst. 2019;37(2):2549–61. doi:10.3233/JIFS-182778.
33. Menezes AJ, Katz J, Van Oorschot PC, Vanstone SA. Handbook of applied cryptography. Boca Raton, FL, USA: CRC Press; 1996.
34. Stallings W. Cryptography and Network Security. Upper Saddle River, NJ, USA: Prentice-Hall. Inc.; 1999.
35. Khan JS, Ahmad J. Chaos based efficient selective image encryption. Multidimens Syst Signal Process. 2019;30(2):943–61. doi:10.1007/s11045-018-0589-x.
36. Kumar A, Dua M. Novel pseudo random key & cosine transformed chaotic maps based satellite image encryption. Multim Tools Applicat. 2021;80(18):27785–805. doi:10.1007/s11042-021-10970-5.
37. Zhao L, Zhao L, Cui F, Sun T. Satellite image encryption based on RNA and 7D complex chaotic system. Visual Comput. 2024;40(8):5659–79. doi:10.1007/s00371-023-03128-x.
38. Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. Internat J Bifurcat Chaos. 2006;16(08):2129–51. doi:10.1142/S0218127406015970.
39. Ullah A, Shah AA, Khan JS, Sajjad M, Boulila W, Akgul A, et al. An efficient lightweight image encryption scheme using multichaos. Secur Commun Netw. 2022;2022(4):680357. doi:10.1155/2022/5680357.