AIMS Mathematics, 9(11): 31217–31238.
DOI: 10.3934/math.20241505
Received: 21 August 2024
Revised: 05 October 2024
Accepted: 09 October 2024
Published: 01 November 2024

https://www.aimspress.com/journal/Math

Research article

Securing air defense visual information with hyperchaotic Folded Towel Map-Based encryption

Shamsa Kanwal[1,*], Saba Inam[1], Fahima Hajjej [2] and Ala Saleh Alluhaidan[2]

[1]Department of Mathematical Sciences, Fatima Jinnah Women University, the Mall, Rawalpindi, Pakistan
[2]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

*** Correspondence: Email:** shamsa.kanwal@fjwu.edu.pk; Tel: +92-333-148-0866.

Abstract: In modern air defense systems, safeguarding sensitive information is crucial to prevent unauthorized access and cyber-attacks. Here, we present an innovative image encryption approach, leveraging chaotic logistic maps and hyperchaotic Folded Towel Map sequence generation. The proposed image encryption is a multi-layered procedure intended to secure image transmission. It initiates with permutation, where a chaotic logistic map generates pseudo-random sequences to scramble pixel positions. Next, key mixing creates complexity, randomness, and nonlinearity using an invertible key matrix. Finally, the diffusion phase employs hyperchaotic maps to produce a new sequence XORed with the pixels through a bitwise operation, further encrypting the image. This three-stage process efficiently protects images from unauthorized access, ensuring secure transmission. The proposed method enhances security by leveraging non-linearity, sensitivity, and robust mixing, properties making it highly resistant to cryptographic attacks. The experimental results showed robust encryption performance as established by metrics such as an entropy value of 7.9991, a UACI of 33.21%, and an NPCR of 99.61%. The proposed encryption approach outperformed existing methods in securing image transmission and storage, offering a reliable solution for protecting air defense communication strategic data.

Keywords: image encryption; chaotic logistic map; hyperchaotic Folded Towel Map; data security
Mathematics Subject Classification: 94A60, 68P25

1. Introduction

The widespread accessibility and quick dissemination of digital images in today's digital environment have become crucial to our daily existence. Image encryption safeguards the confidentiality, integrity, and privacy of sensitive visual data. It is the sensitizing aspect of modern data security. Emphasize encryption's importance in a number of industries, like as the military, banking, healthcare, media, and intellectual property security. Preserving the security of digital images during storage, transfer, and recovery becomes especially important due to the growing risk of unauthorized access, cyber-intrusions, and data leaks.

Due to advancements in technology, image encryption has become essential; image encryption is a procedure of safeguarding images by modifying their content in such a way that unsanctioned individuals or entities cannot effortlessly understand or access the original information. Defending the accuracy and secrecy of visual data is the aim of image encryption. For image encryption, numerous techniques are used such as Symmetric key and Asymmetric key encryption, chaotic systems and maps, visual cryptography and steganography, etc. [1].

Privacy and protecting data from unauthorized users have become a major concern in the modern day. Nowadays, building encryption is an elementary area of study. The major impartial of image encryption is to generate excellent finest cipher images or to modify images into obscure form to prevent data or information from tampering while preventing the information and quality of original image [2].

With the advancement in technology, and spiral noteworthiness of images in solicitation such as medical imaging, communication in military forte, and many more, it set off vitally important to protect intuitive information contained by images from unauthorized users. The leakage of significant information and confidential data can raise military, permissive, and national security issues. To safeguard data from tampering, encryption techniques are employed, which play an important role in certifying the confidentiality and integrity of sensitive and confidential data [3].

Drones, frequently referred to as unmanned airships (UAVs), are implemented in real-time scenarios such as cargo delivery, communication, and rescue missions. They mostly take images. Since UAVs have enough storage, storing a large number of images at once is not practicable, so UAVs have to send the images immediately; UAVs send the images in the absence of any security protocols leads to data fabrication, addition of noise, etc. UAVs are most of the time utilized independently, however currently, they are desegregated with other UAVs to communicate. In the course of transference and mediation of data among UAVs, the assaulter may launch their UAVs to steal private or confidential information [4].

The technique of capturing images from satellites, planes, unmanned aerial vehicles, and other flying objects has been referred to as aerial photography. It broadly utilized remote sensing technology, permitting the accession of high-resolution images of the earth's surface from an overhead view. There are many applications of Ariel photography in real estate management, urban planning, road network detection disaster evaluation, etc. Ariel images accommodate significant data concerning national security that needed a protective pathway; therefore these images require security or a protective environment [5].

Satellite imagery, refers to the images of the earth's surface apprehended by the satellites, imparts information about numerous geographic locations, land covers, and terrain used for generating maps, assists in observing environmental changes, urban planning, agriculture, and forestry also helpful in scientific research. Satellite images accommodate sensitive and confidential information about military installations, natural resources, and groundwork layout, access to such data by assaulter leads to espionage, terrorism, and unsanctioned scrutiny. Transference of unencrypted satellite images over

ill-protected communication networks uplifts the risk of tampering and data interception [6]. Encryption processes that involve edge detection, 3D bit-level scrambling, and dynamic diffusion techniques effectively protect the private images.

The air defense system frequently involves Radar system that gives vital information about the location, speed, direction, and altitude of latent threats; radar stations involve the transference of visual data such as images and videos. To encrypt visual data combination of permutation and diffusion techniques builds on a chaos map to accomplish high-level security. Rearrangement of the values of pixels is inferred by permutation approach, while dispersion of the impact of a single pixel throughout the image is implied by diffusion. Combining frequently updated encryption coefficients with a substitution box (S_box) [7].

Different encryption techniques are proposed to enhance the security of image transfer over networks such as a study introduces the Sin-Arcsin-Arnold Multi-Dynamic Coupled Map Lattice (SAMCML) model, which utilizes the chaotic properties to design a robust encryption scheme. By applying random changes, DNA encoding and SHA-512 for key generation, the algorithm generates secure ciphertext images [8].

With the quick evolution of satellite and network communication technologies, there is a huge need for protective storage and transference of satellite visual data. Moreover, the chaos built encryption method is utilized for satellite imagery. Chaos-built encryption methods produce complex deportment of a chaotic system. The initiate encryption techniques used countless chaotic maps incorporating Logistic Map, Henon Map, Tent Map, Cubic Map, Sine Map, and Chebyshev Map; these maps generate complexity in the encryption technique. The initiate encryption method contains the following abilities, large key space, complexity, pixel pixel-disturbing uniformity in contrast with traditional encryption techniques like AES and DES [9–11]. RSA and ECA algorithms are used in the re_encryption process also fog computing is utilized for image preservation [12,13].

Researchers have explored various chaotic maps and memristor-based systems to design advanced encryption schemes with improved robustness and performance. For instance, the research in [14] constructed a multiscroll memristive Hopfield neural network (HNN) by proposing Sigmoid functions into the memristor. The memristor, known for its synapse-like properties, make it idea for constructing dynamic systems like Hopfield network. Another study introduces a discrete memristive hyperchaotic system that covers the common issues such as low Lyapunov exponents and discontinuous chaotic ranges. The researchers derived four hyperchaotic maps that generate a cube attractor, significantly enhancing the complexity of the original system [15].

Other researchers proposed a new medical image ciphering technique by using Compressive sensing techniques along with a memristive hyperchaotic system. Unlike traditional methods, this approach focused on efficient handling of large volumes of medical images [16]. The use of chaotic properties in discrete memristor (DM) model was presented where an oscillatory term was introduced, which resulted in four hyperchaotic maps with hidden attractors and diverse dynamical behavior. These maps were successfully applied to pseudo random number generation ensuring high randomness in their outputs [17].

Our proposed method is developed by utilizing a chaotic logistic map, an influential mathematical model that manifests multiplex and undividable behavior, and a Hyperchaotic system, an adjunct of a chaotic system that manifests considerable intricacy in its behavior. The method of encryption integrates the Hyperchaotic folded towel maps and chaotic logistic maps to accomplish an exceptional level of security and privacy in image encryption. Image is used as a key in which 4×4 invertible

matrices are taken.

The logistic map is utilized for the permutation aspect of encryption procedure, to produce confusion in images by reordering the pixels of images. Then, the hyperchaotic folded towel map is utilized for the diffusion aspect in the encryption procedure, to make that swap to discrete pixels of images influence the whole image in a complex way.

The use of folded towel map ensures complex and unpredictable behavior due to the two positive Lyapunov exponents. Moreover, the integration of logistic map with folded towel map enhances both the confusion and diffusion steps. Besides this, the algorithm ensures the decryption is efficient by using the self-reversible chaotic maps. However, some limitations exists. The integration of the hyperchaotic map increases the complexity in the encryption process and hardware implementation. Since the system is highly sensitive to initial conditions, it can lead to performance issues if not managed properly.

The remaining manuscript is arranged in the following manner: Section 2 details some mathematical preliminaries. In Section 3, the suggested scheme is presented while section 4 gives the details about its implementation and evaluation. In section 5, we conclude the entire study.

2. Mathematical preliminaries

The proposed research paper comprises the following mathematical concepts:

- Chaotic maps reference the sort of mathematical functions that indicate chaotic behaviors. Chaotic maps exhibits some key properties, including dependence on initial conditions, nonlinearity, and topological mixing property.
- The logistic map serves as an uncomplicated yet effective chaotic map. It operates in a chaotic regime yielding a non-periodic sequence. The mathematical expression is defined in Eq (1)

$$x_{n+1} = b\, x_n(1 - x_n). \tag{1}$$

Here, b represents the bifurcation parameter that regulates the chaotic dynamics. To keep the output x_n within the range [0, 1], parameter b must lie within [0, 4].

- The folded towel map was introduced by Rossler in 1979 as an invertible map with hyperchaotic properties. It is three-dimensional system, known by its complex and chaotic behavior, making it perfect for encryption applications. The map's chaotic dynamics arise from its sensitivity to initial conditions and non-linearity present in its structure. Eq (2) is the mathematical representation of the folded towel map.

$$\left.\begin{aligned} x_{n+1} &= \mathrm{a}x_n\ (1-x_n) - 0.05\ (y_n+0.35)\ (1-2z_n), \\ y_{n+1} &= 0.1((y_n+0.35)\ (1+2z_n) - 1)\ (1-1.9x_n), \\ z_{n+1} &= 3.78z_n\ (1-z_n) + \mathrm{b}y_n. \end{aligned}\right] \tag{2}$$

The folded towel map, has hyperchaotic attributes as it is three dimensional and it contains two positive and one negative Lyapunov exponent, which signify the degree of separation between nearby trajectories in phase space. A system with at least two positive Lyapunov exponents indicates that it is hyperchaotic leading to more complex and unpredictable dynamics compared to a purely chaotic system. Moreover, its invertibility enhances security with an extra layer as the

decryption process can precisely reverse the encryption process without the loss of information. Figure 1 shows the folded towel map and Figure 2 shows the Lyapunov diagram [18].

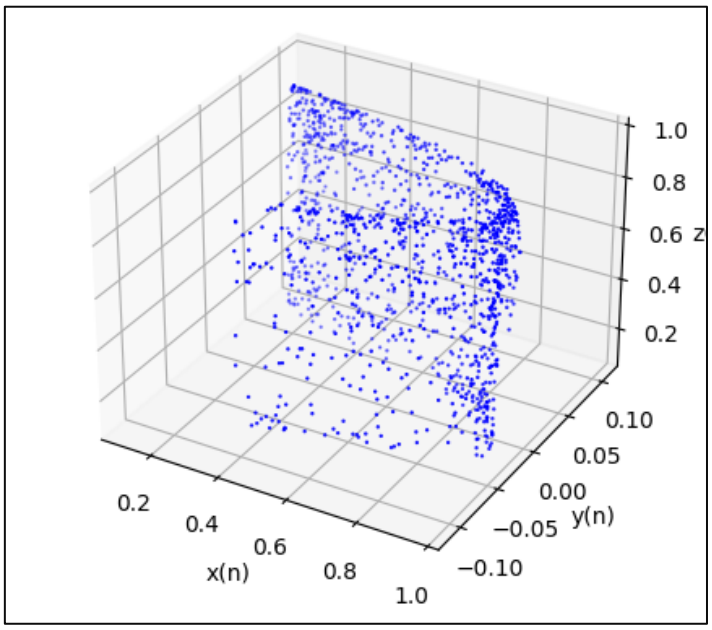

Figure 1. Folded Towel Map.

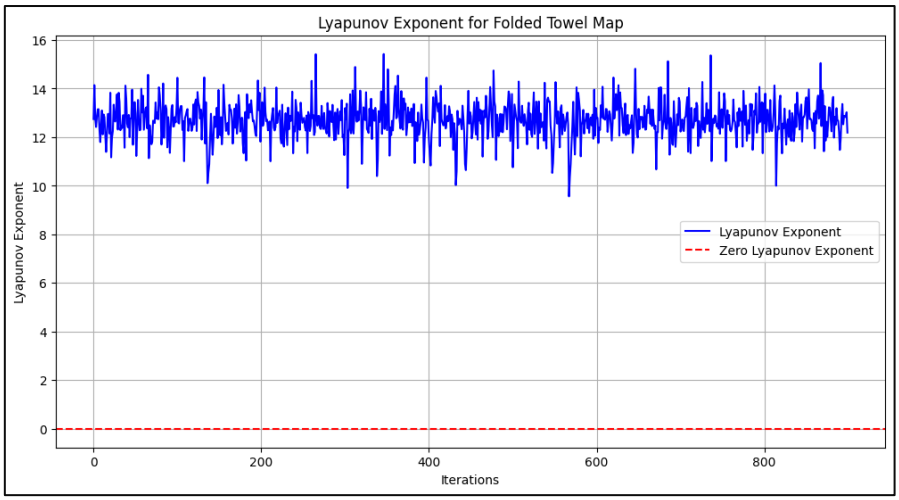

Figure 2. Folded Towel Map Lyapunov diagram.

3. Proposed encryption and decryption algorithm

Initially, an unintelligible image is generated by encrypting a plain image. Then, the decryption technique is utilized to retrieve the plain image. Image encryption junctures comprise; a permutation juncture: In it, Logistic maps are utilized to create pseudo-random sequences that are utilized for substitution and permutation operations. The sequence created by the logistic map works as a lead for

scrambling the pixel values of images. In the permutation phase, the position of image element rearrangement remains chaotic throughout the entire picture, leading to unaccompanied disorder; the image element values and picture turn indistinct. Key mixing juncture: This stage involves dividing the permuted pixel values by the key invertible matrix, which imparts complexity, randomness, and nonlinearity into encrypted images. Diffusion phase: The Hyperchaotic folded towel map created a new sequence XORed with prompt arouses outcomes. XOR is a bitwise operation that incorporates bits from two origins. The process diagram of our implied encryption technique is shown in Figure 3.

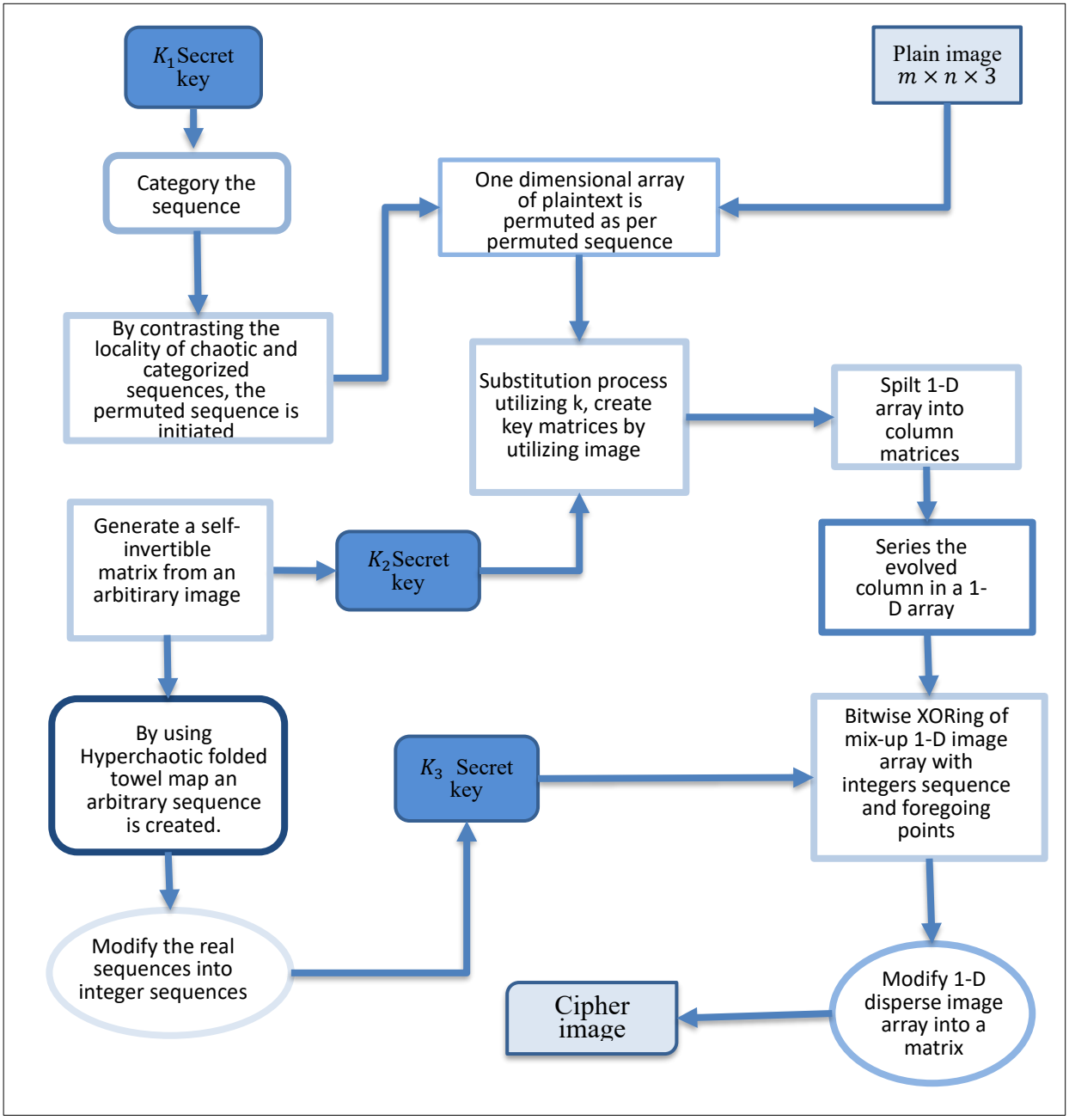

Figure 3. Process diagram of proposed scheme.

3.1 Encryption process

The initiated encryption schemes are comprised of three phases, which include; permutation, substitution, and diffusion phases. A chaotic system is an appeal for the initiated schemes to acquire productive outcomes.

3.1.1 Permutation phase

In order to add complication and non-linearity to the relationship among the original image's pixels, the permutation phase necessitates moving the location or spot of pixel values. Initially, a logistic map is used in this phase; the permutation of pixel locations or spots is accomplished by utilizing a logistic map with the key K_1. The logistic map employs the key K_1 as a parameter; the key K_1 is essential for controlling the pixel permutation sequence. By utilizing the key K_1 logistic map is recapitulated to create a chaotic sequence of values. After that, the chaotic sequence is organized in ascending order, which assists in putting the values for the remoter process together. Then, compare the sorted sequence and original sequence to regulate the permutation of pixel location. At the final stage; by utilizing the permuted sequence, a 1-D array of original images is produced.

Algorithm 1: Permutation of pixels

Input: Colored Plain image I, K_1 = (a ,$X(0)$) CLM
Output: Image array (W) with permuted pixels
Step 1: To generate a 1D array *P*, the original image matrix *I* must be transformed into a 1D array with size $M= m \times n \times 3$, where m is rows and n is columns of the original plain image *I*
Step 2: Utilizing CLM with the key K_1, create the chaotic sequence $X = \{x_1, x_2, \dots, x_M\}$ henceforth we sort the derived sequence in ascending order $Y = \{y_1, y_2, \dots, y_M\}$
Step 3: Determine the permutation vector J and make an inventory on the spots of sequence terms of X in Y and change the position is $J= \{j_1, j_2, \dots, j_n\}$
Step 4: J is employed to permute the array P in order to generate W

3.1.2 Substitution phase

This stage incorporates the implementation of a technique known as substitution technique, in which an arbitrary image is converted into a matrix format, used to generate the secret key, and finally used to request the replacement of the substitution technique. By converting the image into a matrix, a secret key K_2 is generated by taking a 4x4 invertible matrix to achieve the substitution algorithm.

Algorithm 2: Substitution with the image as a key

Input: Permuted array W, K_2 =image, such that *gcd (k, 256) =1***,** where ***k*** is arbitrarily integer.
Output: An array $\boldsymbol{E}$ of order M.
Step 1: Determine a matrix (self-invertible) from an arbitrary image. Confiscate any arbitrary pixel values originating from pixel values correlate with the matrix of the arbitrary image to construct a matrix of *4x4* order K_{11} *(mod256)* as $K_{11} = \begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} \\ k_{21} & k_{22} & k_{23} & k_{24} \\ k_{31} & k_{32} & k_{33} & k_{34} \\ k_{41} & k_{42} & k_{43} & k_{44} \end{bmatrix}$. Proceeds the arbitrarily integer $k \in (1, 256)$, in order that *gcd(k, 256) = 1*. Computing $K_{12} = k\ (I_3 - K_{11})\ mod256$, $K_{21} = K^{-1}(I_3 + K_{11})\ mod256$, and $K_{22} = -K_{11} mod256$ as I_3 (identity matrix). Configuration an *8×8* matrix (self-invertible) $K_P = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}$.
Step 2: Constructing sub-matrices Q_i. Transform 1D array W into submatrices with order *8 × 1*. Also, the i^{th} matrix is Q_i, where $i = 1,2, \ldots, \left(\frac{M}{8}\right)$. Key mixing is executed with the assistance of substitution technique $C_i = K_P \times Q_i\ (mod256)$. Connect all C_i in the form of a 1D array again as $E = \{C_1 \| C_2 \| \ldots \| C_{\left(\frac{M}{8}\right)}\}$.

3.1.3 Diffusion phase

The final stage of image encryption implies pixel diffusion. The pixel values are changed sequentially by the generated sequence by recapitulating a Hyperchaotic folded towel map by utilizing a specific key K_3. Subsequently, the sequence's values are altered to an integer sequence, which dissipates the image's pixel values collectively with a bit-wise *XOR* operation on an array with one dimension. The cipher image is obtained by rearranging the evolving one-dimensional grid into a matrix of order *P×Q×3*.

Algorithm 3: Pixel diffusion

Input: The array E, secret key $K_3 = (\varphi\ (0), \beta)$, Hyperchaotic folded towel map.
Output: Cipher image CP.
Step 1: Create a sequence $R = \{r_1, r_2, .., r_M\}$ along the key K_3 and Hyperchaotic folded towel map.
Step 2: By utilizing the given equation, modify sequence *R* into the sequence of integers.
PD *= floor (mod (*$R_i \times 10^{14}, 256$)).
Step 3: Apply *XOR of* each element of E with an element of PD at the correlate with the locations and fore-going ciphered pixel as $C_i = PD_i \oplus E_i \oplus C_{i-1}, i = 1,2, \ldots, M$.
Step 4: Modify the array C_i in the matrix configuration CP of the size $M = m \times n \times 3$. Encrypted image is acquired by modifying the matrix in Step (4).

3.2 Decryption process

The reverse encryption algorithm will be chosen during the imaging decryption process in order to retrieve the plain image. The decryption steps involve three stages; initially, XOR operation with the sequence created utilizing key K_2 is eradicated; the reverse process of encryption is followed.

Then, the Hill cipher is put in an application with an invertible matrix brought out from the image utilizing key K_2. Last in the encryption process, random sequence and inverse permutation were built by utilizing key K_1; thus, to reverse the process, we build the random sequence and put in an application the reverse permutation. After reversing all the encryption processes, we modify or reshape the array back into image dimensions, and the colored plain image is prosperously acquired.

Algorithm 4: Image Decryption

Input: Cipher image CP, secret keys K_1, K_2, K_3, CLM, and Hyperchaotic Folded Towel Map.
Output: Plain colored image I.
Step 1: The cipher image matrix CP is put down in an array of size $M = m \times n \times 3$.
Step 2: As in step 1 and step 2 (Algorithm 3), the recipient creates a sequence R of size M by secret key K_3 and Hyperchaotic Folded Towel map.
Step 3: In Step 2, each element of the decrypted image *CP* passes via the subsequent formula:

$$Dj = CPj \oplus PDj \oplus Dj - 1, j = 1, 2, \ldots, M$$

Step 4: Recipient construct matrix (self-invertible) K_P by utilizing key K_2 as in Algorithm 2.
Step 5: Modify one-dimensional array D into submatrices *(order 8 × 1)*DQj.
Step 6: Altered the key mixing by utilizing the formula.

$$Tj = K_P \times DQj\ (mod 256), j = 1, 2, \ldots, M.$$

Step 7: Transform all $Tj's$ in the configuration of a one-dimensional array DM.
Step 8: By recapitulating the CLM and utilizing the shared secret key K_1, acquire a sequence X and obtain Y by classifying X in ascending order.
Step 9: Acquired the permutation array by inverse transform position J^{-1}.
Step 10: Use $(J)^{-1}$ on DM to get P.
Step 11: Alter P in a matrix form of order $M = m \times n \times 3$ and transform to image I.

4. Implementation and evaluation of proposed algorithms

The proposed image encryption approach utilized a combination of techniques. In our proposed work, Matlab 2016a is used to execute the suggested system. The following is the detail of different parameters:

- **Choice of dataset**: The sample images of airplane and satellite images are acquired from the USC-SIPI (University of Southern California - Signal and Image Processing Institute) database.
- **Algorithms**: Pixel permutation requires repositioning the pixels of the image in a particular pattern. Substitution technique utilizing a key K_1 through in the company of image for mixing. Pixel diffusion implies outspreading the impact of each pixel all over the image.
- **Image preference for testing**: For the motive of testing, standard images of airplanes and satellite are chosen.
- **Encryption parameters**: We perform the encryption of a plain-color image P with arbitrary dimensions P=M × N using n encryption rounds and external-one time keys: $K_1 = (a, X(0))$, a self-invertible key matrix generated by $K_2 = \text{image, such that } gcd\ (k, 256) = 1$ and $K_3 = (\varphi\ (0), \beta)$. These keys are generated for each encryption ensuring robust protection against key leakage attacks and enhancing the security of the encryption process [19].
- **Proceed time for encryption**: For airplanes, the image proceed time is 0.129444 seconds, for the satellite image proceed time, it is 0.119113 seconds, and for the satellite image of water bodies, the proceed time is 0.1167 seconds.

The productiveness of our proposed encryption technique is assessed by contrasting it with another technique found in the literature. Numerous kinds of tests were conducted to check the security, productiveness, computational efficacious, and quality of encrypted images. Visual representation in Figures 4–6 exhibit an example of an image's input and output utilizing the initiated technique. The test images used were of size 256×256 and 1200×1200.

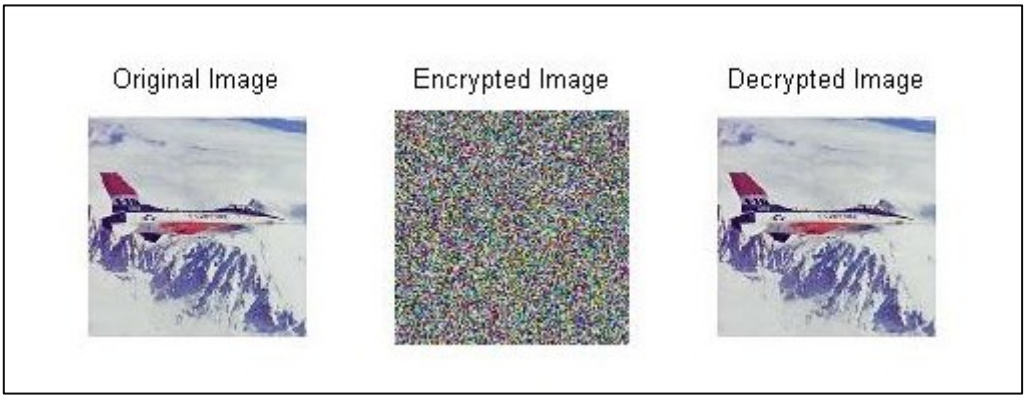

Figure 4. Plain, Cipher, and decrypted images of an airplane size 256×256.

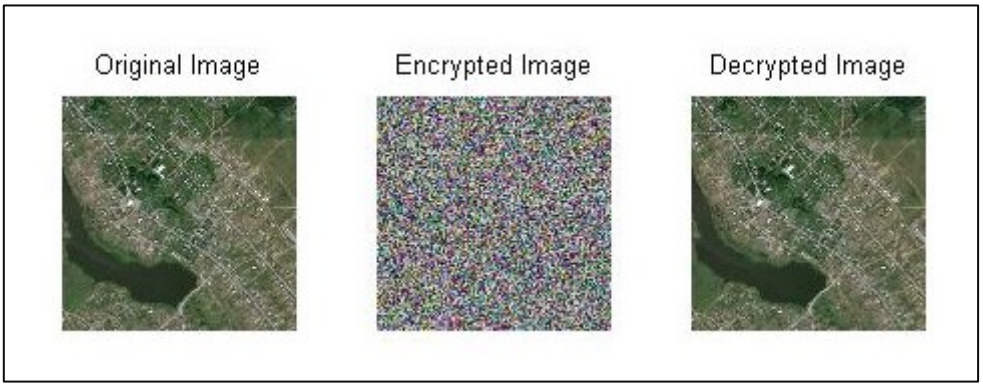

Figure 5. Plain, Cipher, and decrypted images of a satellite size 256×256.

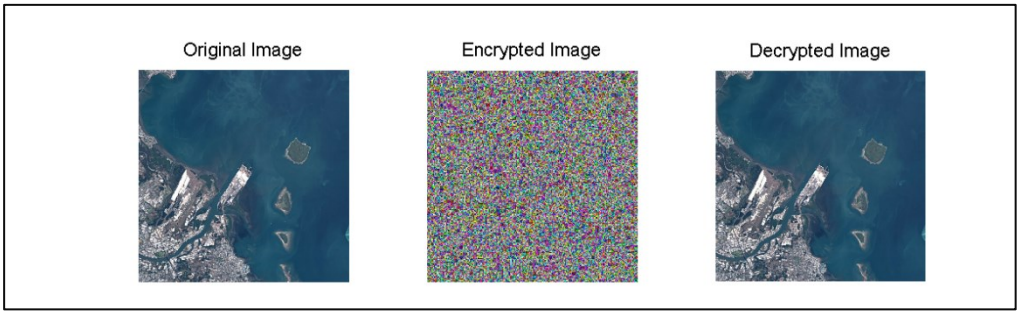

Figure 6. Plain, Cipher, and decrypted images of satellite image of water bodies size 1200×1200.

4.1 Security analysis

Security key analysis requires evaluation and flexibility of an encryption algorithm to ambush the point at recuperation of the encryption key. An effective encryption method should be resistant to all kinds of assaults, including statistical, differential, and exhaustive attacks [20]. In this module, we inspect the initiated technique or method's security from a variety of angles, for instance; Mean Square Error analysis (MSE) assesses the contortion instituted by the encryption process. Lower MSE value represents better protection of original signals throughout the time of encryption process, Peak Signal to Noise Ratio analysis (PSNR), is utilized for computing the quality of an image or signal contrast to the original image [21–24]. A higher value of PSNR represents the finer quality of the image. key sensitivity analysis determines how the infinitesimal changes in the encryption key influence the evolve cipher text, Pixel Correlation analysis assesses if in case there exists statistical correspondence betwixt adjacent pixels in the encrypted data, and information entropy analysis determines the unpredictability in encrypted data. Figures 9–13 compares the values of proposed scheme with existing literature [25–27].

4.2 Statistical analysis of histograms

Histogram analysis is used for evaluating the security of encryption techniques. The original image's histogram distributes pixel power across levels; multiple histograms are available for each RGB image. As the original images comprise of multiple extents, they evolve into a non-uniform histogram. On the other hand, a secure encryption scheme generates an encrypted image with a flat histogram, which equally represents each intensity level in the image. A flat histogram in the encrypted image can be utilized to mask statistical patterns next to the original image, rendering it difficult for hackers to obtain any kind of information. Thus, the existence of a uniform and histogram in a cipher image is evidence of an effective encryption technique, as uniformity in histogram produces uncertainty and randomness, making it challenging for attackers to attack. Figure 7 displays the histogram of the original image, and Figure 8 shows the histogram of the cipher image, also it is apparent that the cipher image's histogram is fairly uniform.

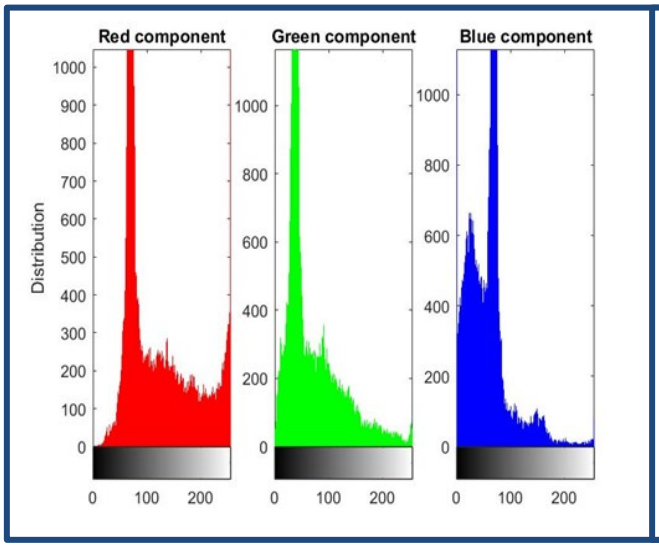

Figure 7. Histogram of original image Airplane.

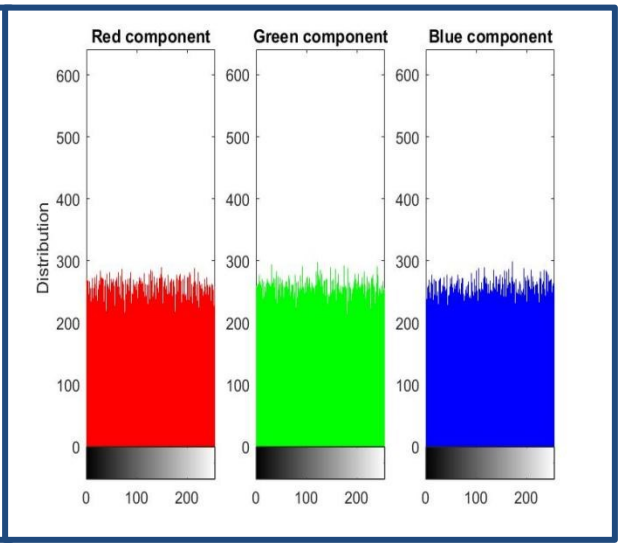

Figure 8. Histogram of encrypted image Airplane.

4.3 Correlation analysis of adjacent pixels

The correlation computes adjoining pixel values in the image. Although the intrinsic correlation between adjacent pixels in original images poses a security issue, the correlation of adjoining pixel values in the original image is analyzed to measure the connection between surrounding pixels. A higher value of correlation represents a stronger similarity between the neighboring pixels. It displays the productiveness of the encryption process in deranging the correlations that exist in the plain image. To eliminate the correlations images are encoded, as in cipher images the adjacent pixels seem statistically independent. The correlation is calculated using the Eq 3.

$$Cr = \frac{n(\sum_{i=1}^{m} p_i q_i - \sum_{i=1}^{m} p_i \sum_{i=1}^{m} q_i)}{(n\sum_{i=1}^{m}(p_i)^2 - (\sum_{i=1}^{m} p_i)^2)(n\sum_{i=1}^{m} q_i)^2 - (\sum_{i=1}^{m} q_i)^2)}. \tag{3}$$

Here p_i and q_i are the values of two adjacent pixels, m, and n is the total pixel values used to calculate the coefficient. Figure 9 shows the correlation of the adjacent pixel of the original image of the vegetable. Figure 10 displays the correlation of the cipher image of the vegetable. Table 1 illustrates the pixels RGB component allocation of the original and ciphered Airplane image.

Table 1. Correlation coefficient values of Airplane encrypted and ciphered image

Color	**Red**		**Green**		**Blue**	
	Original	Enc	Original	Enc	Original	Enc
Horizontal	0.9901	-0.0052	0.9852	0.0023	0.9779	0.0022
Vertical	0.9911	-0.0018	0.9869	0.0037	0.9834	0.0027
Diagonal	0.9815	-0.0043	0.9724	-0.0002	0.9628	0.0079

4.4 Chi-Square test analysis

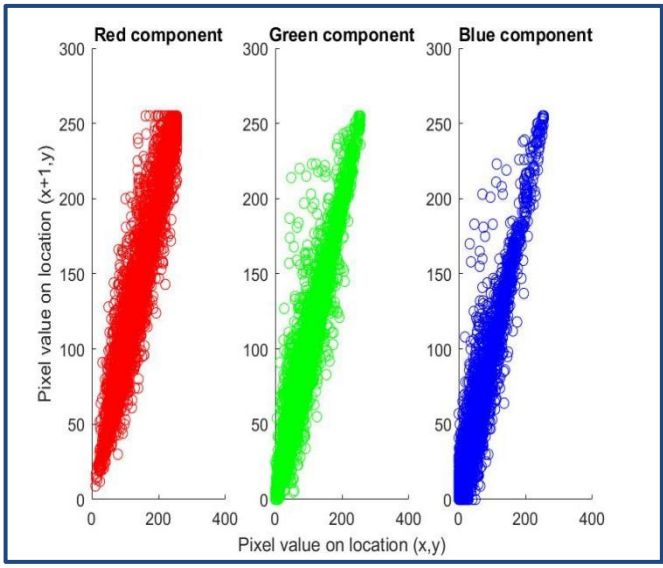

Figure 9. Correlation analysis of original image airplane.

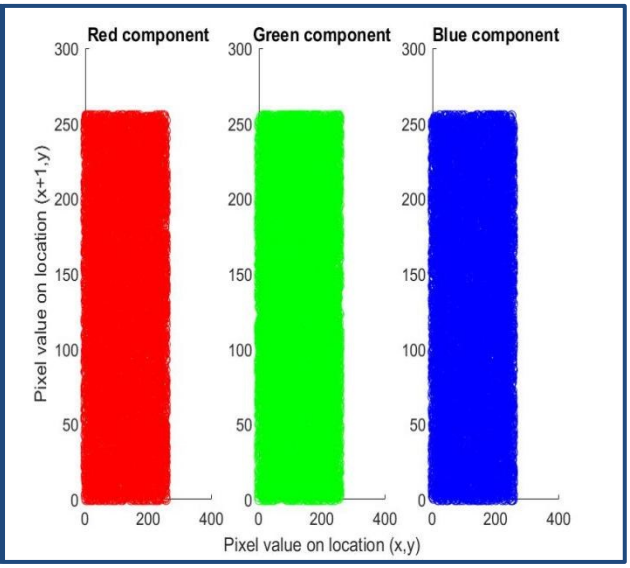

Figure 10. Correlation analysis of encrypted image airplane.

Chi Square analysis is the statistical method utilized to assess the degree of concurrence between discerned and anticipated frequencies of unconditional data. Chi-square test analysis is utilized to evaluate the consistency in the histogram of encrypted images. A low Chi-Square value indicates the high consistency in cipher images. The given Eq 4 provides estimation;

$$X_q{}^2 = \sum_{j=0}^{225} \frac{(M_j - N_j)^2}{N_j}, \tag{4}$$

where, M_j is the observed frequency of j and the expected frequency of j is N_j; the expected frequency is represented as

$$N_j = \frac{image\ size}{256}.$$

The proposed encryption scheme Refs [16] techniques' histograms of ciphered images display grayscale uniformity. It is manifested that our proposed scheme for the vegetable image has a significantly lower Chi-Square value when contrasted to the methods in the references [22], which indicates its effectiveness and competence. Table 2 displays the results of Chi-Square analysis.

Table 2. Testing outcomes of Chi-Square test analysis.

Image encryption algorithm.	**Testing scheme**
Ref [15]	267.7480
Proposed Scheme	
Airplane	230.3229
Satellite	270.2604

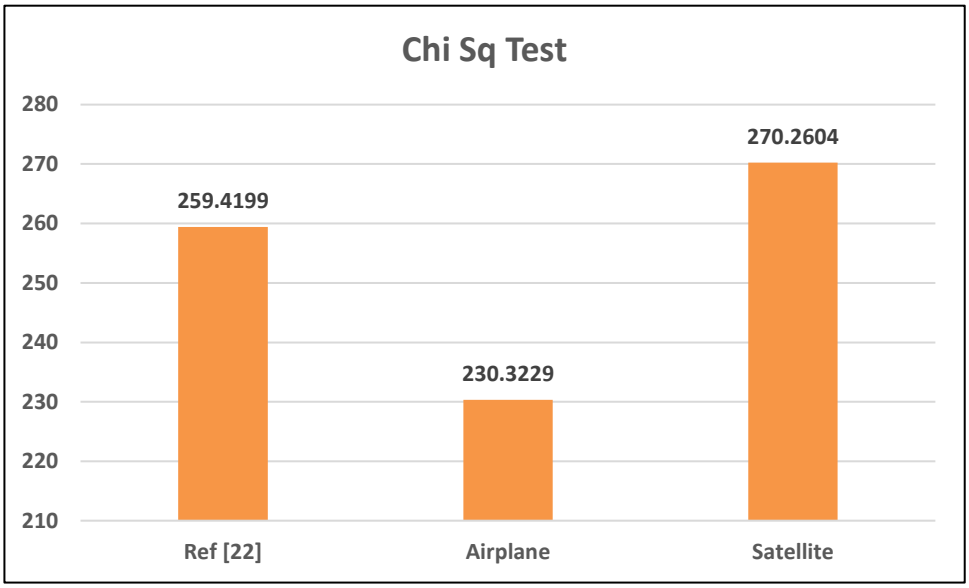

Figure 11. Chi Square values compared**.**

4.5 Entropy analysis

Entropy constitutes the distribution of randomness in a system. The entropy estimation formula is represented by the stipulated Eq 5.

$$\sum_{i=0}^{m-1} Q(m_i) log_2 \frac{1}{Q(m_i)}. \tag{5}$$

Suppose that m is the information source, where Q_{mi} represents the probability of the symbol. After encryption, the encrypted image's information entropy should be close to 8 [21]. The probability of information disclosure by the cryptosystem decreases as it approaches 8.

Equation (5) is used to compute the information entropy of the encrypted images. Table 3 illustrates the entropy values, and it is clear that they are around the optimal value of 8.

Table 3. Shows comparisons of entropies values.

Image encryption algorithms	Entropy values
Ref[16]	**7.9990**
Ref[17]	**7.9970**
Proposed algorithm	
Airplane	**7.9991**
Satellite	**7.9991**

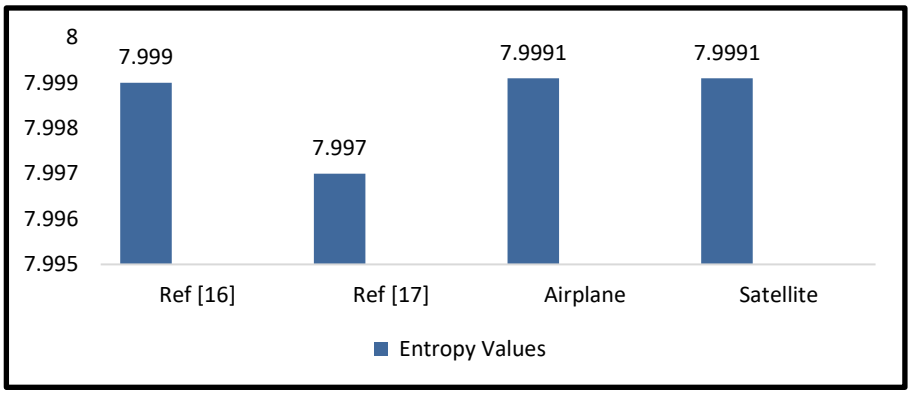

Figure 12. Entropy values compared with the literature.

4.6 Differential attacks

These attacks fall under the category of cryptanalytic attacks that exploit variations in ciphertext arising from minor changes in the plaintext. To prevent such attacks, encryption algorithms are developed. To evaluate the effectiveness of our encryption scheme against differential attacks, we calculate the Number of Pixel Change Rate (NPCR), which measures the percentage of pixels that change between the original and modified images. A higher NPCR value indicates that the proposed encryption scheme offers strong resistance to differential attacks. Additionally, we assess the Unified Average Changing Intensity (UACI), which reflects the average intensity change of pixels between the original and modified images; a lower UACI value signifies that the alterations are less noticeable. The NPCR and UACI values can be determined using the formulas presented in Eqs 6 and 7. The ideal NPCR and UACI values are approximately 99.6094070% and 33.4635070%, respectively [28].

$$NPCR = \frac{\sum_{i=0}^{m}\sum_{j=0}^{n} E(i,j)}{I_s} \times 100, \tag{6}$$

$$UACI = \frac{1}{I_s}\left[\sum_{i=0}^{m}\sum_{j=0}^{n} \frac{|Y(i.j) - Y'(i,j)|}{256}\right] \times 100, \tag{7}$$

and,

$$E(i,j) = \begin{cases} 1, & E_1(i,j) \neq E_2(i,j) \\ 0, & E_1(i,j) = E_2(i,j) \end{cases}.$$

Table 4. Comparison of NPCR and UACI values Airplane.

Image encryption algorithm	NPCR	UACI
Ref [16]	99.59360	32.175
Ref [20]	99.60	33.41
Standard Value	99.61	33.46
Proposed Scheme	99.61	33.206

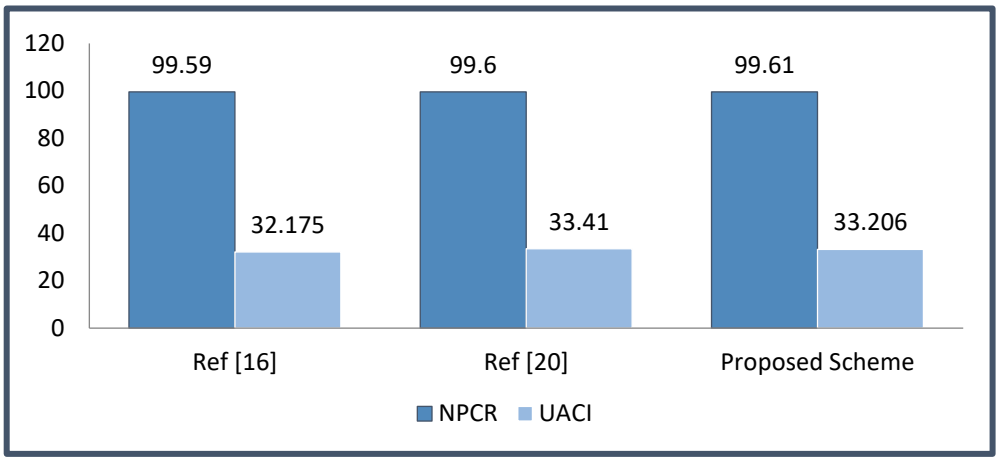

Figure 13. NPCR and UACI values compared with previous literature.

4.7 Mean square analysis

Mean square analysis is the analytical approach through the computation of Mean Square Error (MSE) utilized to assess the precision and discrepancy betwixt two data sets. MSE frequently utilizes metrics in image processing to assess variance between two images. A higher value of MSE displays considerable variance between the plain and cipher images. The calculations of MSE values are evaluated by using the formula given in the Eq 8;

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (x(i,j) - y(i,j))^2, \tag{8}$$

where m and n show the number of rows and columns. X displays the original image and Y displays the encrypted image, respectively. Table 5 represents the MSE of the initiated encryption technique for the image and contrasts it with a few other methods. The outcomes represent that the initiated scheme has a higher MSE value than the propositions made in Refs. We come to the termination that, when contrast to the schemes expressed in the references [23,24], there are a vital alterations between the plain image and the ciphered image in the initiated scheme.

4.8 Peak signal to noise ratio (PSNR) analysis

To calculate the image quality or signal contrast to the original image, PSNR is used. It assesses the ratio of the signal's peak power to the noise resulting from compression or other actions. The highest potential image quality is offered by a greater PSNR value. Moreover, a low PSNR value indicates a notable distinction between the encrypted and plain image. It goes over using the Eq 9;

$$PSNR = 10.log \frac{255^2}{MSE}. \tag{9}$$

Table 5. Shows PSNR and MSE values.

Image Encryption Scheme	MSE	PSNR
Ref [15]	7764.3	8.2440
Ref [16]	8888.88	8.64233
Proposed Scheme	11048.7162	7.6977

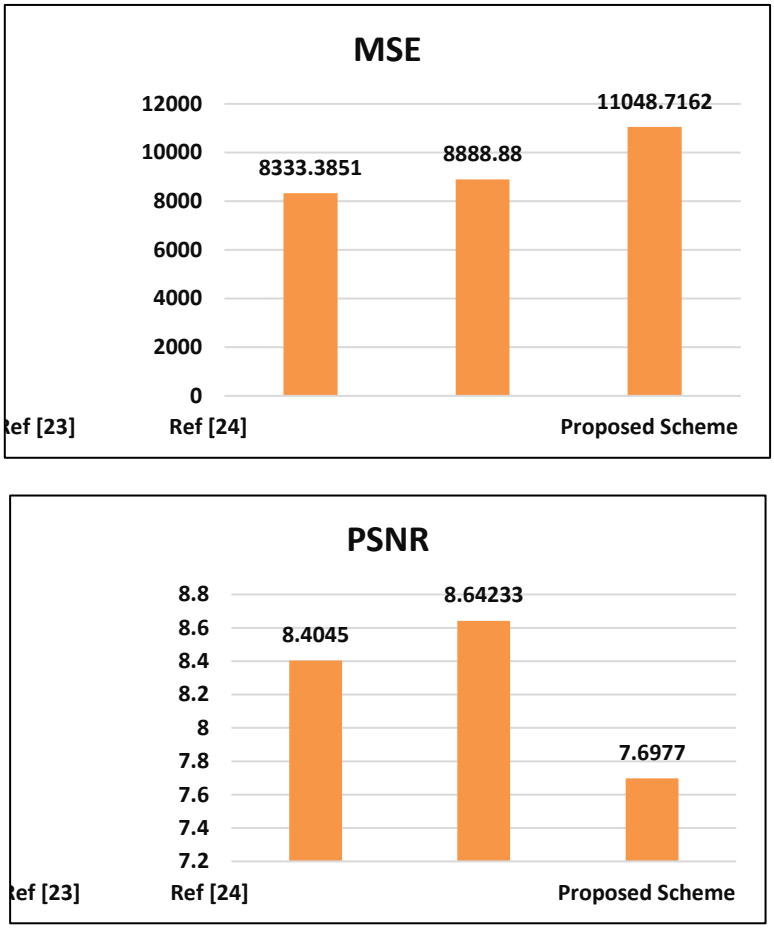

Figure 14. Comparison of MSE and PSNR values.

4.9 Structural similarityindex measure (SSIM)

SSIM is utilized in image processing that determines the structural similarity between original and encrypted images. Its formula is given in Eq (10). In terms of luminance, contrast, and structure, it computes the score between -1 and 1, where 1 represents the ideal similarity and -1 represents no similarity at all.

$$SSIM = \frac{(2\mu_{x_1}\mu_{x_2}+r_1)(2\delta x_1 x_2+r_2)}{(\mu_{x_1}{}^2\mu_{x_2}{}^2+r_1)(\delta_{x_1}{}^2\delta_{x_2}{}^2+r_2)}, \tag{10}$$

where x_1 and x_2 represent two images, $2\delta x_1 x_2$ indicates the covariance of x_1 and x_2, $\delta_{x_1}{}^2$ represents the variance of x_1, $\delta_{x_2}{}^2$ expresses the variance of x_2, μ_{x_1}represents the mean value of

x, μ_{x_2} expresses the mean value of x_2, and r_1 and r_2 are constants to ensure the stability of images [20].

Table 6. The value of SSIM.

Image Encryption Algorithm	SSIM
Ref [21]	0.0083
Ref [22]	0.0061
Proposed Scheme	0.0055

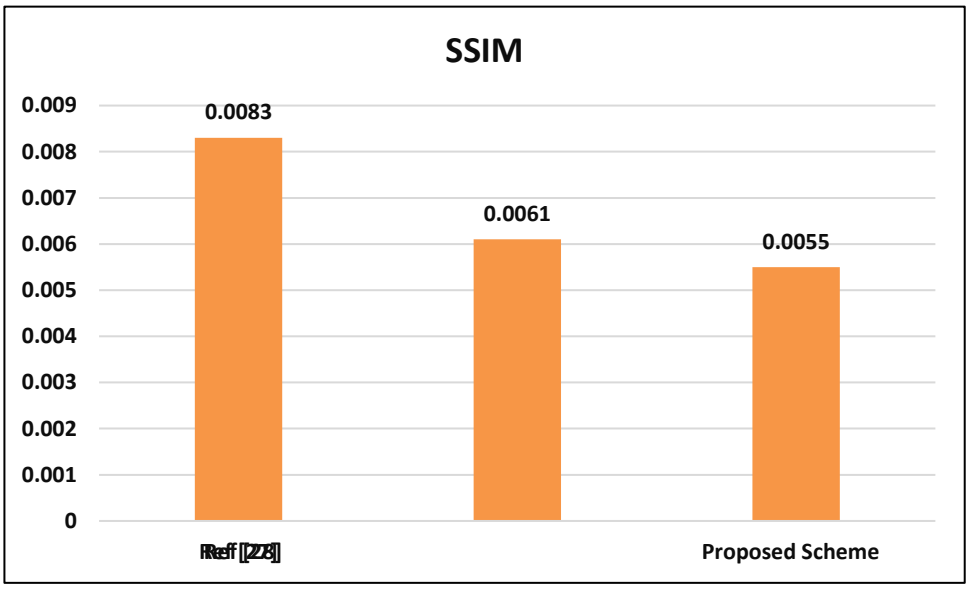

Figure 15. Comparison of SSIM values.

4.10 Key sensitivity analysis

Our proposed encryption technique depends steadily on the secrecy and probity of its secret key for encryption and decryption techniques. The secret key plays a vital role in building any encryption scheme or method; these are utilized to modify the original image into the encrypted image. Without the accurate key, it is not possible to decrypt the cipher image. Thus, in our proposed approach, a 0.0000000000000001 change or modification to the first key K_1 = (a, X (0)), results in an entirely different outcome. We will be unable to recover the original image utilizing that key after decryption. Our proposed method or approach is tremendously sensitive to input parameters or keys.

4.11 Key space analysis

Key space analysis is administered to decide the security durability of the proposed encryption technique as opposed to brute-force attacks. It determines the size of possible secret keys utilized in the encryption technique. The purpose of the analysis is to make sure that the size of the key is adequate such that the key space is greater than 10^3 so that an algorithm can withstand brute-force attacks. Our

proposed encryption scheme contains three distinct keys. The keys K_1 and K_3 comprise of logistic maps and Hyperchaotic folded towel maps. Additionally, the key K_2 is confiscated from the image, so there are a lot of probabilities for selecting the invertible matrices. The size of the key K_2 is also infinite. The entire number of chances to choose the keys could be $(10^{15})^2 \times (10^{15})^2 = (10)^{60} \approx (2)^{240}$. Also, exhaustive attacks become impossible when the key space is adequately large, as it requires an unworkable quantity of computation resources.

4.12 Robustness analysis of noise and data loss

As digital images are transmitted or stored, they can be affected by noise or data loss. A robust image encryption algorithm should handle these issues and allow proper decryption [29]. We test the robustness of encryption against salt and pepper noise (SPN) by adding varying levels of noise to the encrypted image. Despite the noise, the decrypted images remain identifiable, showing the algorithm's resistance to noise. Figure 16 shows the depicted cipher image of satellite, the noise levels are $0.05, 0.1$ and 1×10^{-4}, respectively. It can be seen that even with some data missing, the decrypted image could be partially recovered, demonstrating resilience against data loss.

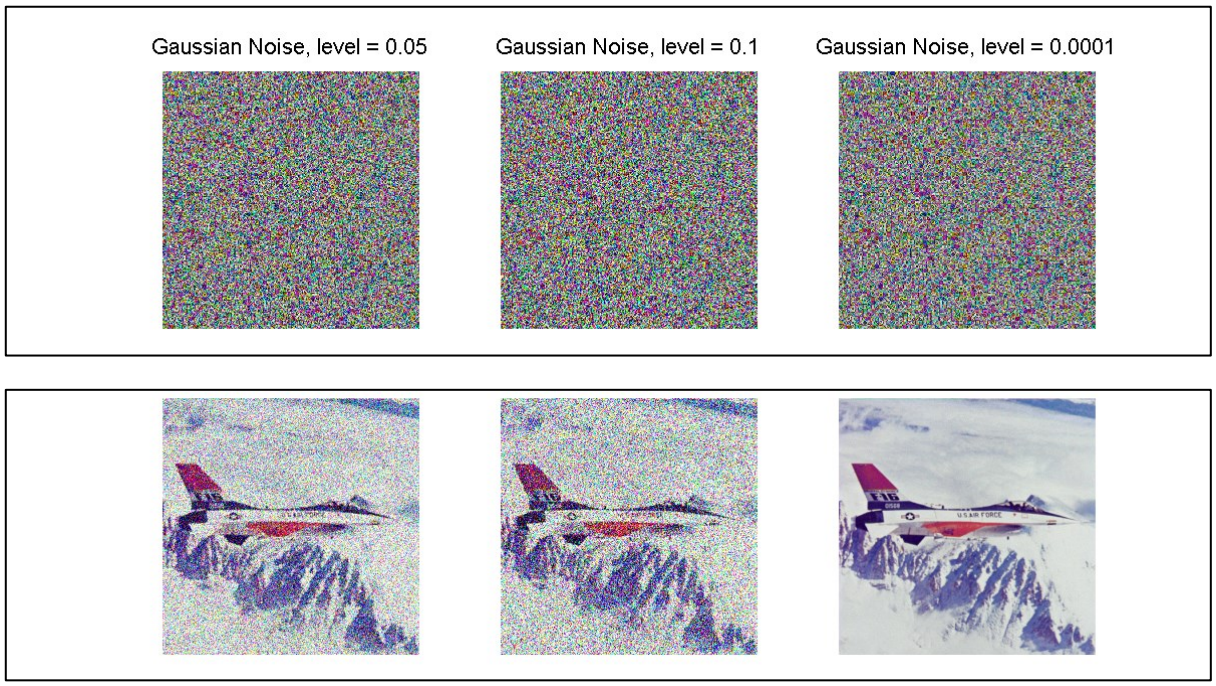

Figure 16. Data Loss Attack: $0.05, 0.1$ and 1×10^{-4}.

5. Conclusions

Here, we propose and initiate a novel technique that grips both chaotic and Hyperchaotic image encryption techniques to magnify security. The encryption technique is comprised of two approaches; the Permutation approach uses a Logistic map to rearrange the pixels of images. Additionally, the substitution method in which the encrypted image becomes the key generated from the image. In order to create a sequence for the subsequent Diffusion phase, a Hyperchaotic folded towel map is used.

Each pixel value in this sequence is then bitwise XORed with the values from this sequence. Combining both Hyperchaotic and chaotic encryption methods provide protection against a range of cryptographic assaults, including brute force attacks. The security of the encryption technique is additionally authenticated with Key sensitivity, key space, and entropy analysis, which are additional tools utilized in security analysis. The security analysis tests disclose that the security and authenticity of the proposed scheme are powerfully built.

Author contributions

Shamsa Kanwal: Conceptualized and designed the encryption technique and contributed to analyzing the algorithm's performance and security; Saba Inam: Implemented the algorithm, conducted experiments, and validated results through simulations and comparative studies; Fahima Hajjej: Contributed to writing the manuscript and interpreting the results; Ala Saleh Alluhaidan: Reviewed and approved the final version of the manuscript. All authors have read and approved the final version of the manuscript for publication.

Acknowledgement

This research project was funded by the Deanship of Scientific Research and Libraries, Princess Nourah bint Abdulrahman University, through the Program of Research Project Funding After Publication, grant No (RPFAP-73-1445).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

1. O. F. Mohammad, M. S. M. Rahim, S. R. M. Zeebaree, F. Y. Ahmed, A survey and analysis of the image encryption methods, *Int. J. Appl. Eng. Res.*, **12** (2017), 13265–13280. https://doi.org/10.1007/s13319-017-0148-5
2. M. Kumar, R. A. M. Lahcen, R. N. Mohapatra, C. Alwala, S. V. K. Kurella, Review of image encryption techniques, *J. Comput. Inf. Sci. Eng.*, **14** (2020), 31–37. https://doi.org/10.9790/0661-2201013137
3. M. Kaur, S. Singh, M. Kaur, Computational image encryption techniques: A comprehensive review, *Math. Probl. Eng.*, **2021** (2021), 5012496. https://doi.org/10.1155/2021/5012496
4. A. Shafique, A. Mehmood, M. Elhadef, K. H. Khan, A lightweight noise-tolerant encryption scheme for secure communication: an unmanned aerial vehicle application, *PLoS One*, **17** (2022), e0273661. https://doi.org/10.1371/journal.pone.0273661
5. F. Masood, W. Boulila, J. Ahmad, A. Syam Sankar, S. Rubaiee, W. J. Buchanan, A novel privacy approach of digital aerial images based on Mersenne Twister method with DNA genetic encoding and chaos, *Remote Sens.*, **12** (2020), 1893. https://doi.org/10.3390/rs12111893

6. M. A. S. Al-Khasawneh, M. Faheem, E. A. Aldhahri, A. Alzahrani, A. A. Alarood, A Map Reduce based approach for secure batch satellite image encryption, *IEEE Access*, **11** (2023), 62865–62878. https://doi.org/10.1109/access.2023.3279719
7. D. Li, S. Zhou, C. He, The application of image encryption method based on chaotic mapping in the field of radar transmitter remote monitor system, *Adv. Inf. Manag. Commun. Electron. Autom. Control Conf.*, 2019, 577–580. https://doi.org/10.1109/imcec46724.2019.8983923
8. H. Liu, L. Teng, Y. Zhang, R. Si, P. Liu, Mutil-medical image encryption by a new spatiotemporal chaos model and DNA new computing for information security, *Expert Syst. Appl.*, **235** (2024), 121090. https://doi.org/10.1016/j.eswa.2023.121090
9. M. Usama, M. K. Khan, K. Alghathbar, C. Lee, Chaos-based secure satellite imagery cryptosystem, *Comput. Math. Appl.*, **60** (2010), 326–337. https://doi.org/10.1016/j.camwa.2009.12.033
10. S. Kanwal, S. Inam, F. Hajjej, O. Cheikhrouhou, Z. Nawaz, A. Waqar, M. Khan, A new image encryption technique based on sine map, chaotic tent map, and circulant matrices, *Sec. Commun. Networks*, **2022** (2022), 4152683. https://doi.org/10.1155/2022/4152683
11. S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, H. Hamam, Analytic study of a novel color image encryption method based on the chaos system and color codes, *Complexity*, **2021** (2021), 5499538. https://doi.org/10.1155/2021/5499538
12. Y. Nagasree, C. Rupa, P. Akshitha, G. Srivastava, T. R. Gadekallu, K. Lakshmanna, Preserving privacy of classified authentic satellite lane imagery using proxy re-encryption and UAV technologies, *Drones*, **7** (2023), 53. https://doi.org/10.3390/drones7010053
13. Y. Bentoutou, E. H. Bensikaddour, N. Taleb, N. Bounoua, An improved image encryption algorithm for satellite applications, *Adv. Space Res.*, **66** (2020), 176–192. https://doi.org/10.1016/j.asr.2019.09.027
14. Q. Lai, L. Yang, G. Hu, Z. H. Guan, H. H. C. Iu, Constructing multiscroll memristive neural network with local activity memristor and application in image encryption, *IEEE Trans. Cybernetics*, **54** (2024), 4039–4048. https://doi.org/10.1109/tcyb.2024.3377011
15. Q. Lai, L. Yang, G. Chen, Design and performance analysis of discrete memristive hyperchaotic systems with stuffed cube attractors and ultraboosting behaviors, *IEEE Trans. Ind. Electron.,* **71** (2024), 7819–7828. https://doi.org/10.1109/tie.2023.3299016
16. Q. Lai, G. Hu, A nonuniform pixel split encryption scheme integrated with compressive sensing and its application in IoMT, *IEEE Trans. Ind. Informat.*, **20** (2024), 11262–11272. https://doi.org/10.1109/tii.2024.3403266
17. Q. Lai, L. Yang, G. Chen, Two-dimensional discrete memristive oscillatory hyperchaotic maps with diverse dynamics, *IEEE Trans. Ind. Electron.* https://doi.org/10.1109/tie.2024.3417974
18. Belmouhoub, M. Djemai, J. P. Barbot, Cryptography by discrete-time hyperchaotic systems, *In Proceedings of the IEEE Conference on Decision and Control*, **2** (2004), 1902–1907. https://doi.org/10.1109/cdc.2003.1272893
19. H. Liu, A. Kadir, J. Liu, Colorpathological image encryption algorithm using arithmetic over Galois field and coupled hyperchaotic system, *Opt. Lasers Eng.*, **122** (2019), 123–133. https://doi.org/10.1016/j.optlaseng.2019.05.027
20. S. Kanwal, S. Inam, M. Othman, A. Waqar, M. Ibrahim, F. Nawaz, et al., An effective color image encryption based on Henon map, tent chaotic map, and orthogonal matrices, *Sensors*, **22** (2022). https://doi.org/10.3390/s22124359

21. Q. Liang, C. Zhu, A new one-dimensional chaotic map for image encryption scheme based on random DNA coding, *Opt. Laser Technol.*, **160** (2022), 109033. https://doi.org/10.1016/j.optlastec.2022.109033
22. S. Benaissi, N. Chikouche, R. Hamza, A novel image encryption algorithm based on hybrid chaotic maps using a key image, *Optik*, **272** (2022), 170316. https://doi.org/10.1016/j.ijleo.2022.170316
23. W. Alexan, M. ElBeltagy, A. Aboshousha, RGB image encryption through cellular automata, S-Box and the Lorenz system, *Symmetry*, **14** (2022), 443. https://doi.org/10.3390/sym14030443
24. M. SaberiKamarposhti, A. Ghorbani, M. Yadollahi, A comprehensive survey on image encryption: Taxonomy, challenges, and future directions, *Chaos Solitons Fract.*, **178** (2024), 114361. https://doi.org/10.1016/j.chaos.2023.114361
25. C. Chen, K. Sun, Q. Xu, A color image encryption algorithm based on 2D-CIMM chaotic map, *China Commun.*, **17** (2020), 12–20 https://doi.org/10.23919/jcc.2020.05.002
26. T. Li, D. Zhang, Hyperchaotic image encryption based on multiple bit permutation and diffusion, *Entropy*, **23** (2021), 510. https://doi.org/10.3390/e23050510
27. H. Liu, J. Liu, C. Ma, Constructing dynamic strong S-Box using 3D chaotic map and application to image encryption, *Multimedia Tools Appl.*, **82** (2022), 23899–23914. https://doi.org/10.1007/s11042-022-12069-x
28. P. Liu, X. Wang, Y. Su, Image encryption via complementary embedding algorithm and new spatiotemporal chaotic system, *IEEE Trans. Circuits Syst. Video Technol.*, **33** (2023), 2506–2519. https://doi.org/10.1109/TCSVT.2022.3222559

AIMS Press