Hindawi
Security and Communication Networks
Volume 2022, Article ID 4152683, 17 pages
https://doi.org/10.1155/2022/4152683

Research Article

A New Image Encryption Technique Based on Sine Map, Chaotic Tent Map, and Circulant Matrices

Shamsa Kanwal,[1] Saba Inam,[1] Fahima Hajjej,[2] Omar Cheikhrouhou,[3,4] Zainab Nawaz,[1] Ayesha Waqar,[1] and Majid Khan[5]

[1] *Department of Mathematical Sciences, Faculty of Science and Technology, Fatima Jinnah Women University, The Mall, Rawalpindi, Pakistan*
[2] *Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P. O. Box 84428, Riyadh 11671, Saudi Arabia*
[3] *CES Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax, Tunisia*
[4] *Computer Science Department, Prince Sultan University, Riyadh, Pakistan*
[5] *Department of Applied Mathematics & Statistics, Institute of Space Technology, Islamabad, Pakistan*

Correspondence should be addressed to Shamsa Kanwal; shamsa.kanwal@fjwu.edu.pk

Received 1 November 2021; Revised 14 May 2022; Accepted 20 August 2022; Published 30 October 2022

Academic Editor: Barbara Masucci

Image encryption is one of the sensitive areas used recently to save information over the Internet and confirms the security on a higher level. A new cryptosystem has been proposed for the encoding and decoding of images using sine map, chaotic tent map, and circulant matrices. The process involves three stages. The sine map is used for the permutation phase. In the substitution phase, the Hill cipher method together with prime circulant matrix are used and a chaotic tent map is used in the diffusion phase. The algorithm becomes impenetrable to resist differential- and statistical-type attacks. The algorithm's key space is sufficient in size to withstand brute-force attacks. This symmetric image encryption algorithm indicates good results for correlation analysis, key space analysis, entropy analysis, key sensitivity analysis, histogram analysis, number of pixel change rate (NPCR), unified average changing intensity (UACI), and peak signal-to-noise ratio (PSNR). From all these simulation results, we come to know that the constructed image encryption cryptosystem is systematic and vigorous, supplying better protection for image encryption.

1. Introduction

With the development in the technology of computer networks, over this network, plenty of secret information can be transferred. Nowadays, the security of information is a more important factor. With the security of textual data, there is a need to secure the pictorial information also. For this purpose, image encryption is a successful technique of protecting the private images, while communication and a lot of methods have been proposed [1, 2, 3]. Impartment of image information is rapidly increasing [4], and cryptographers pay their attention towards this aspect. Due to some fundamental characteristics like a huge range of information and excessive correlation between the image pixel values, image encryption is different from text encryption. For image encryption, the traditional encryption techniques such as AES [5], DES, IDEA, and RSA are not acceptable because these ciphers need more computational time. Image encryption is of two types: one is analog image encryption and the other is digital image encryption. Analog images deal with two-dimensional signals, while digital images work for the analysis and manipulation of images. With the development of chaotic cryptanalysis, many new algorithms are proposed for the protection of image information till now [6, 7].

The features like compassion to subsequent conditions and irregular behavior of chaotic maps have captured the attention of cryptographers to generate modified image encryption cryptosystems. The image encryption process is classified into two steps: the permutation and the diffusion process. Permutation intermixes and interchanges the pixel positions to eliminate the association of pixel values and secure the important information about the real image. The permutation process is also called as the scrambling of the pixels. Its purpose is to change the pixel positions to demolish the association between the pixel values in the original image. Pixel values are being replaced in the diffusion process. Pixel shows the image that tells about the luminosity at a point. It plays a vital role in our daily life [8, 9, 10]. Cryptographic schemes reorganize and diffuse information by using encryption steps, whereas chaotic maps use iteration methods.

Chaotic encryption schemes are defined on real numbers, and they gave a better combination of security, speed, reasonable computational power, and complexity. Due to the sensitivity of initial conditions and complexity, chaotic system becomes a pseudorandom generator for the image encryption. Chaotic maps are used in color and grayscale images for encryption. The elementary design is also important for the protection of image encryption against statistical and cryptanalytic attacks [11]. Wu et al. [12] proposed a vigorous image encryption technique using three kinds of distinct one-dimensional chaotic maps and DNA computing like logistic sine map, logistic tent map, and sine tent map. The computational power is more, and the level of security increases when we compare it with remaining image encryption techniques. Mondal and Zhang. [13] presented an image encryption algorithm depending upon the cellular automata and a chaotic-skew tent map. The skew tent map is utilized to find the inceptive transmitter for the cellular automata. The first picture is transformed in the dispersion interaction by utilizing a pseudo-irregular succession.

Hua and Zhou. [14] proposed a two-dimensional modified logistic sine map to construct an image encryption algorithm with a small distortion confusion and diffusion. A random number is added in the neighboring pixel strength of an original image in each ring to increase the amount of protection. Fu et al. [15] presented an image encoding technique with a better spatial bit-level transformation scheme by utilizing a 3-dimensional cat map. This process has a capability of both confusion and diffusion. The keystream is gotten by utilizing the capacity of the plain image and mystery key by building the security of the picked plaintext assault. Due to some intrinsic properties of images like large data capacity and more association between the image pixel values, color image encryption is quite different from text encryption. Latterly, many chaos-based picture encryption systems were generated, which were based on a discrete chaotic system [16]. Liu [17] proposed a new color image encryption technique in which he gives a new idea of bit-level pixel permutation. He told that this method not only converts the pixel positions but also changes its values.

In another study, Tang et al. [18] break the primary picture into overlapping chunks, organize an arbitrary shuffling of blocks, and utilize a chaotic map and Arnold transform to compute a block-wise strong encryption matrix. In Ref. [19], Hayat and Azam generated an effective image encoding algorithm utilizing dynamic S-box and pseudo-arbitrary numbers over elliptic bend. The algorithm is resistant in the opposition to chosen plaintext attack and known plaintext attacks. Another study, constructed by Abd-el-Ltif and Niu [20], is a hybrid image encryption by utilizing a chaotic framework and cyclic elliptic bend. The new technique has a better level of protection. Liu [21] in 2012 presented a fingermark image encryption technique by utilizing two chaotic logistic maps. In this scheme, key space opposes comprehensive assault. It gives great security. Liu presented a new scheme [22] on image encryption using DNA complementary rule and chaotic maps. He used DNA coding to encode the pixel values of the gray image into four nucleotides. After this encoding process, he used the DNA complementary rules for the transformation of each nucleotide. Wang et al. [23] proposed a cryptosystem on a novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. They have presented that this cryptosystem perceives the content's double protection and the vision of the image, and also it has the capability of encrypting three gray images at a time. By keeping the literature study in mind, we have proposed a new cryptosystem for security purpose.

A modified image encryption cryptosystem is presented in the existing paper to connect a sine map and a chaotic tent map with a Hill cipher to enhance the protection level and to generate a modified algorithm. This chaotic image encryption scheme is very fast and efficient in terms of security and complexity. The introduction of the sine map enhances the time of iteration of a chaotic system. Due to an increase in the time of iteration, the security of the image increases [24]. The main goal of this work is to make advanced venture in the regime of image encryption using chaotic maps. More precisely, this proposal deals with developing and analyzing a novel image encryption that comprises three phases: pixel permutation process, substitution process, and pixel diffusion process. The permutation sequence for the first phase is generated by the sine map, and the pixels of the plain image are then permuted according to the permutation sequence. Instead of using S-boxes for the substitution phase, the substitution of pixels in the permuted image is determined by Hill cipher and prime circulant matrix. At the end, the diffusion process is completed by the chaotic tent map to ensure the secrecy of the entire image encryption technique. The key generated by using the prime circulant matrix in the second phase is self-invertible so that it can also make decryption efficient. The combined use of the prime circulant [25, 26, 27] matrix with Hill cipher enhances the security. This new technique uses sine map, Hill cipher in substitution phase, and bitwise XOR. The use of a self-invertible key matrix protects the algorithm from many problems. The new technique will be carried out and tried on both grayscale and shading pictures. Some security measures, like PSNR, entropy, UACI, NPCR, and correlation factors, are utilized to assess the achievement of this new technique. This network of chaotic systems has caught the attention of many people because of its unique features such as pseudo-randomness, sensitive initial condition, and the control parameters used in this system.

The remaining article is arranged as follows: The preliminaries on a sine map, circulant matrices, and chaotic tent map are given in Section 2. In Sections 3 and 4, the constructed encoded and decoded cryptosystems, respectively, are presented. Section 5 deals with the implementation of the proposed algorithms. The results and discussions of performance and comparison with some other schemes are provided in Section 6. The whole work is concluded in Section 7.

2. Preliminaries

2.1. Sine Map. Sine map is defined as follows [14]:

$$h_{n+1} = f(h_n, \beta) = \beta \sin(\pi h_n). \quad (1)$$

It has various effective characteristics such as Lyapunov type, arbitrary conduct, and uniform thickness work. That is why a sine map is considered a suitable candidate for using in cryptography. The sine map (1) bifurcation is shown in Figure 1.

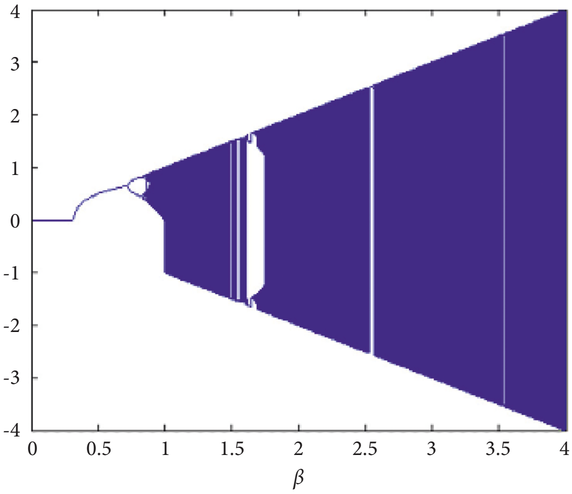

Figure 1: Bifurcation of the sine map.

2.2. Prime Circulant Matrices. A circulant matrix is a square matrix where each column vector is moved from one component to the relative right to the previous line vector. An $n \times n$ circulant matrix is a prime circulant if the GCD of the circulant vector is 1; that is, all the elements of the circulant vector are generally prime. For example, the 4×4 circulant matrix with circulant vector $(3, 8, 5, 7)$ is prime circulant if the $\gcd(3, 8, 5, 7) = 1$.

2.3. Chaotic Tent Map. The third cycle is carried out by consolidating a chaotic tent map [19] and XOR activity that adjust the pixel esteem.

Consequently, the pixel values of the scrambled image amazingly change due to even minor a little bit of adjustment in the first image. To accomplish this objective, an irregular arrangement is created by a chaotic tent map defined as follows:

$$Z_{n+1} = G(Z_n, \mu) = \begin{cases} \frac{\mu}{2} \times Z_n & \text{if} Z_n \leq 0.5, \\ \frac{\mu}{2} \times (1 - Z_n) & \text{if} Z_n \geq 0.5, \end{cases} \quad (2)$$

where the range of the system parameter μ is [0, 4]. The bifurcation analysis of chaotic tent property is given in Figure 2. Its chaotic range is μ ∈ [2, 4].

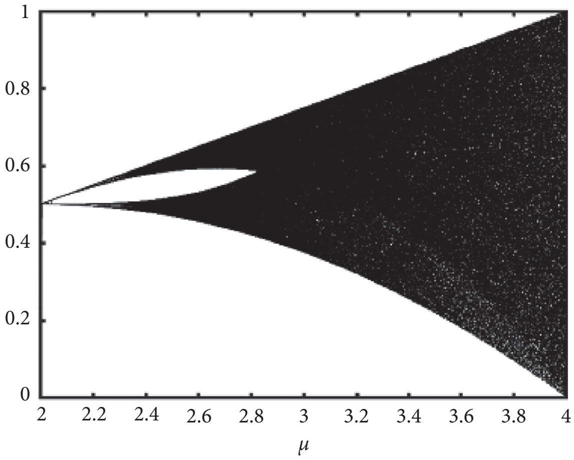

Figure 2: Bifurcation diagram of chaotic tent map.

3. Image Encryption Technique

In this section, we give the application of sine map (1) and CTM (2) to develop a symmetric encryption technique. The proposed technique uses the sine map to generate a sequence for permutation. For the substitution process, prime circulant matrices are used. At long last, a bit XOR is executed to get the scrambled image by utilizing CTM (2).

3.1. Choice of Control Parameters and Key Generation. For the encryption of an image containing $m \times n$ pixels, the choice of three secret keys and associated control parameters are as follows:

The first secret key for the permutation phase is $K = (h_0, \beta)$, where h_0 is an inceptive value of the arrangement generated by the sine map and the control parameter $\beta \in (0, 1]$ is used. For the substitution process, the second key $K' = (a, a_1, a_2, a_3)$ is obtained by selecting four arbitrary integers $a, a_1, a_2, a_3 \in [0, 255]$, where a_1, a_2, a_3 are utilized to generate a prime circulant matrix.

The CTM (2) is iterated mn times using third key $K'' = (z_0, \mu)$ with initial value z_0 and the control parameter μ. For testing purpose, the values of keys are set as $K = (0.99, 0.79)$, $K' = (123, 6, 24, 11)$, and $K'' = (0.66, 3.78)$. The overview of presented technique is displayed in Figure 3.

3.2. Permutation Technique. In this technique, the sine map is used to transform the original image's pixel location. To obtain a chaotic sequence, iterate the sine map, and then, arrange the terms of the sequence in an escalating pattern. Find out the transformation sequence by relating the positions of the chaotic and organized sequences. We use this permutation sequence for permuting the pixels of the original picture. The permutation of pixels is given in Algorithm 1.

The substitution is performed on the permuted image using the second secret key K'. A prime circulant matrix is

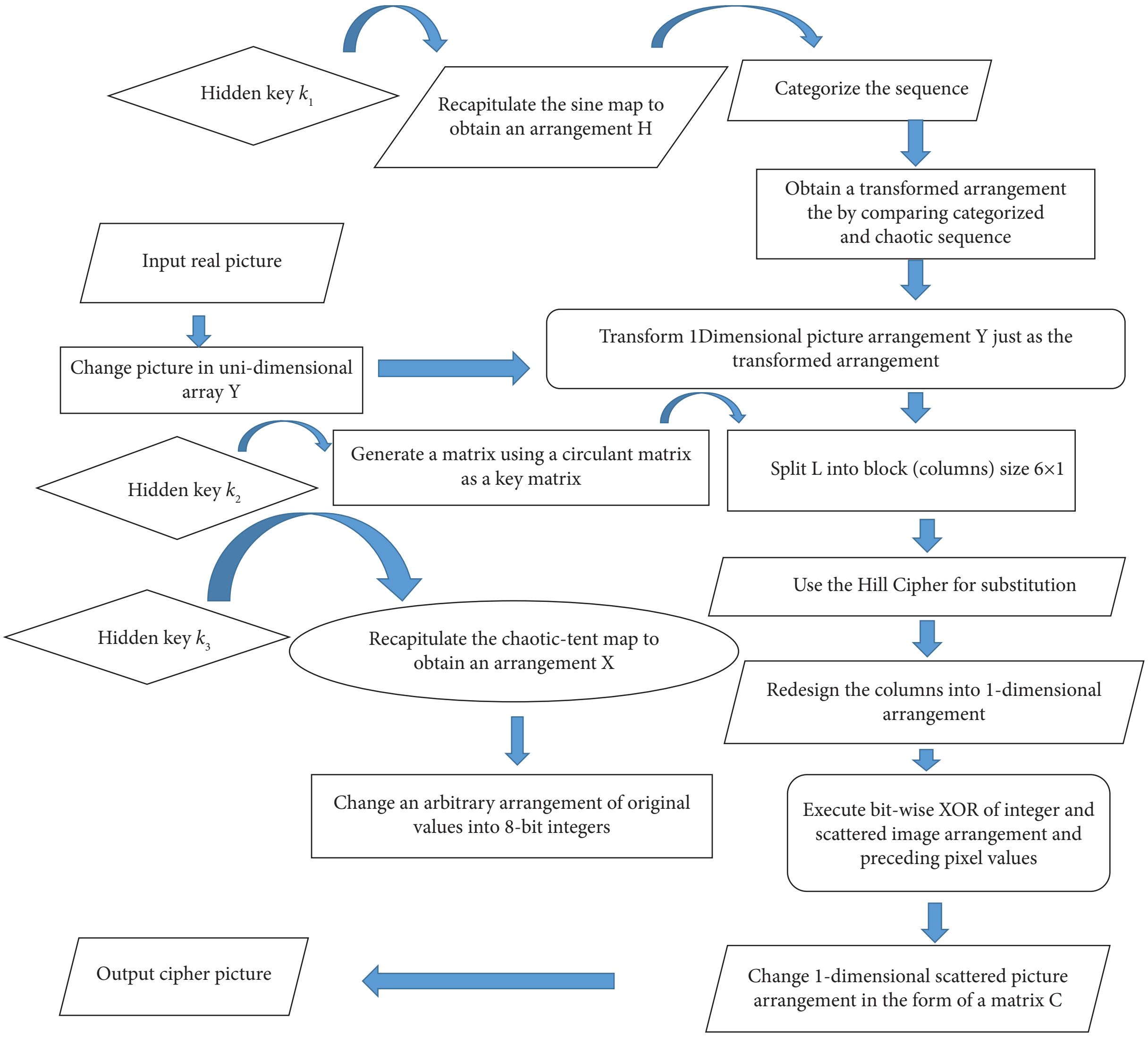
Hidden key k_1
Recapitulate the sine map to obtain an arrangement H
Categorize the sequence
Obtain a transformed arrangement the by comparing categorized and chaotic sequence
Input real picture
Change picture in uni-dimensional array Y
Transform 1Dimensional picture arrangement Y just as the transformed arrangement
Hidden key k_2
Generate a matrix using a circulant matrix as a key matrix
Split L into block (columns) size 6×1
Hidden key k_3
Recapitulate the chaotic-tent map to obtain an arrangement X
Use the Hill Cipher for substitution
Redesign the columns into 1-dimensional arrangement
Change an arbitrary arrangement of original values into 8-bit integers
Execute bit-wise XOR of integer and scattered image arrangement and preceding pixel values
Output cipher picture
Change 1-dimensional scattered picture arrangement in the form of a matrix C

Figure 3: Flowchart of the proposed image encryption algorithm.

```
Input: The primary color image $I$ to be encrypted, private key $K = (\beta, h_0)$, Sine Map defined as in (1).
Output: An array $L$ of pixels with confused positions.
(1) The digital matrix $I$ containing $m$ number of rows and $n$ number of columns corresponding to the original color picture is converted to a 1D array $Y = \{y_1, y_2, \dots, y_{mn}\}$.
(2) By iterating Sine Map (1) with the key $K$ and make a sequence $H = \{h_i\}_{i==1}^{mn}$.
(3) Produce the sequence $\overline{H} = \{\overline{h}_i\}_{i=1}^{mn}$ by organizing the sequence $H$ in escalating pattern.
(4) Obtain the permutation vector Perm $= \{j_i\}_{i==1}^{mn}$ by noting down the position of terms of $H$ in $\overline{H}$.
(5) Proceed with $Perm$ to permute the entries of array $Y$ to get $L$.
```

Algorithm 1: (Permutation algorithm).

obtained by means of components a_1, a_2, a_3 of K'. The substitution technique is expressed as Algorithm 2.

3.3. Diffusion Technique. To create diffusion, the third key K'' is utilized. With the assistance of K'' and CTM (2), a unique succession is created and afterward change into number arrangement. The output of the substitution algorithm is then bitwise XORed with this integer sequence to form the cipher image. The technique is defined in the following algorithm:

```
    Input: An arrangement $L$, $K' = (a, a_1, a_2, a_3)$, where $a, a_1, a_2, a_3 \in [0, 255]$ are any four random integer such that $\gcd(a, 256) = 1$ and $\gcd(a_1, a_2, a_3) = 1$.
    Output: An array $E$.
(1) Generate a matrix $A_{11}$ (mod256) of order $3 \times 3$ as
    $A_{11} = \begin{bmatrix} a_1 & a_2 & a_3 \\ a_3 & a_1 & a_2 \\ a_2 & a_3 & a_1 \end{bmatrix}$
(2) Compute
    $A_{12} = a(I - A_{11})\text{mod}256,$
    $A_{21} = a^{-1}(I + A_{11})\text{mod}256,$
    $A_{22} = -A_{11}\text{mod}256,$
    where $I$ represents a $3 \times 3$ unitary matrix.
(3) Create a $6 \times 6$ self-invertible matrix $A$ as
    $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$
(4) Hill cipher is implemented using the following formula:
(5) Combine all the $E_i's$ to make a 1D array $E$
(6) Transform one-dimensional array $L$ into block vectors $L_i$ of order $6 \times 1$, where $i = 1, 2, \ldots, mn/6$:
```

Algorithm 2: (Substitution technique).

```
    Input: An arrangement $E$, secret key $K'' = (z_0, \mu)$, CTM (2).
    Output: Encoded picture $C'$.
(1) Make a sequence $Z = \{z_i\}_{i=1}^{mn}$ by using key $K''$ and CTM (2).
(2) The integer succession is obtained by changing the sequence $Z$ with the assistance of the accompanying formula (3):
    $F = \text{floor}(\text{mod}(Z_i \times 10^{14}, 256)).$
(3) Perform bitwise XOR of every component of $E$ with the corresponding component of $F$ and foregoing ciphered elements as follows:
    $Q_i = F_i \oplus E_i \oplus Q_{i-1},\ i = 1, 2, \ldots, mn.$
(4) Transform an array $Q$ in a matrix $C'$ of size $mn$.
(5) Obtain the encrypted image corresponding the matrix $C'$.
```

Algorithm 3: (Diffusion algorithm).

$$E_i = A \times L_i\,(\text{mod}256), \tag{3}$$

$$E = \{E_1\}_{i=1}^{mn/6}. \tag{4}$$

4. Decoding Technique

The decoding technique is the reverse procedure of the encoding technique. Using the secret keys K, K', K'', the decoding of the scrambled picture is as per the converse activities of the encryption. The decryption technique is elaborated as in the following algorithm:

5. Implementation of Proposed Techniques

In our investigations, images are tested using MATLAB 2018a. Two test images, the Lena colored picture with 256 × 256 pixels and onion colored picture with 198 × 135 pixels, are chosen for the execution of our constructed techniques. For the comparison of results, a Lena image is chosen encrypted with different schemes. The aftereffects of the Lena picture utilizing the proposed methods is exhibited by Figure 4.

6. Performance Analysis

To assess the reliability of the recommended encryption cryptosystem, a series of statistical analyses on the constructed techniques are commenced. The detailed results are given in this section.

6.1. Histogram Analysis. In Figure 5 the encrypted image's histogram of red, green, and blue parts is displayed. The histograms of encrypted images are mostly consistent, as seen in Figure 5. In an original image, there are no data given concerning the conveyance of pixels.

```
     Input: Ciphered image $C'$, Secret keys $K, K', K''$, Sine Map (1), CTM (2).
     Output: Primary colored picture.
 (1) Place the cipher image $C'$ in an array of size $mn$.
 (2) Using the key $K''$ and CTM (2) to create a sequence $Z$
 (3) Every pixel of $C'$ is passed through the given formula:
     $R_j = C'_j \oplus F_j \oplus R_{j-1} \ldots j = 1, 2, \ldots, mn.$,
 (4) Receiver calculates the self-invertible matrix $A$ with the help of secret key $K'$.
 (5) Divide one dimensional array $R$ into column matrices $RM_j$ of order $6 \times 1$.
 (6) Reverse the substitution effect with the help of matrix $A$ as:
     $L_j = A \times RM_j \,(\mathrm{mod} 256)$,
     $j = 1, 2, \ldots, mn.$
 (7) Indicate all $L'_j s$ in 1-dimensional arrangement $N$.
 (8) Iterate the Sine map (1) with key $K$ to obtain a sequence $H$
 (9) The organized sequence $\overline{H}$ can be constructed by assembling $H$ in escalating pattern.
(10) Use the inverse transform position $(\mathrm{Perm})^{-1}$ to get permutated array.
(11) Apply permuted arrangement on $L$ to get $U$.
(12) Transform $U$ in a matrix of order $mn$ and acquire the corresponding image $I$.
```

Algorithm 4: (Decoding technique).

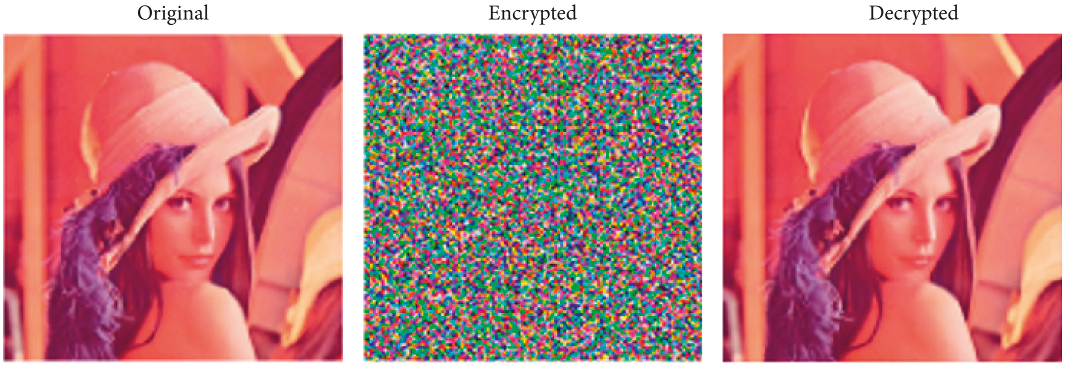

Figure 4: Original, encrypted, and decrypted images of Lena (colored 256 × 256 pixels).

The chi-square (χ^2) test [28] is used to assess the uniformity of histogram. Table 1 shows the result of χ^2 test for different encrypted images. It is evident from these results that the proposed algorithm accepts the null hypothesis with the p-values greater than 0.05 (5% significance) for the encrypted images that proves the uniformity of histogram. Therefore, the redundancy of original images is completely hidden confirming the resistance against the statistical attack.

6.2. Statistical Randomness Analysis. The permutation and distribution may be examined to utilize the correlation analysis between neighboring pixels in the first image and the matching encrypted picture. The worth of the connection is determined by using the following equation :

$$C_r = \frac{n\left(\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i\right)}{\left(n \sum_{i=1}^{n} (x_i)^2 - \left(\sum_{i=1}^{n} x_i\right)^2 \left(\left(n \sum_{i=1}^{n} (y_i)^2 - \left(\sum_{i=1}^{n} y_i\right)^2\right)\right)\right)}, \quad (5)$$

where x_i and y_i are the two adjacent pixel values and n denotes the all pixel values achieved for computing their relationship. The maximum interrelationship coefficient value “1” tells about the more correlation values between the nearest pixels. So our modified algorithm should encode the image with relationship coefficients, which are small furthermore, near 0, and subsequently, the hacker cannot find out any informational data. Figure 6 represents the interrelationship components of original image’s pixel entries in RGB components. Figure 7 represents the correlation entries of the ciphered image’s pixel entries in RGB color bands. Table 2 shows the relationship esteems in the level, vertical, and corner to corner guidelines for the genuine and encoded result. The worth of correlation coefficient formula (5) is close to 0 for the encrypted image that shows the continuous pixel values in the encrypted image are almost un-correlated.

6.3. Entropy Analysis

6.3.1. Global Entropy. The most important qualitative need for image arbitration is information entropy [29]. To quantify the irregularity in the coded image, the entropy of data is determined utilizing data entropy examination using the following formula:

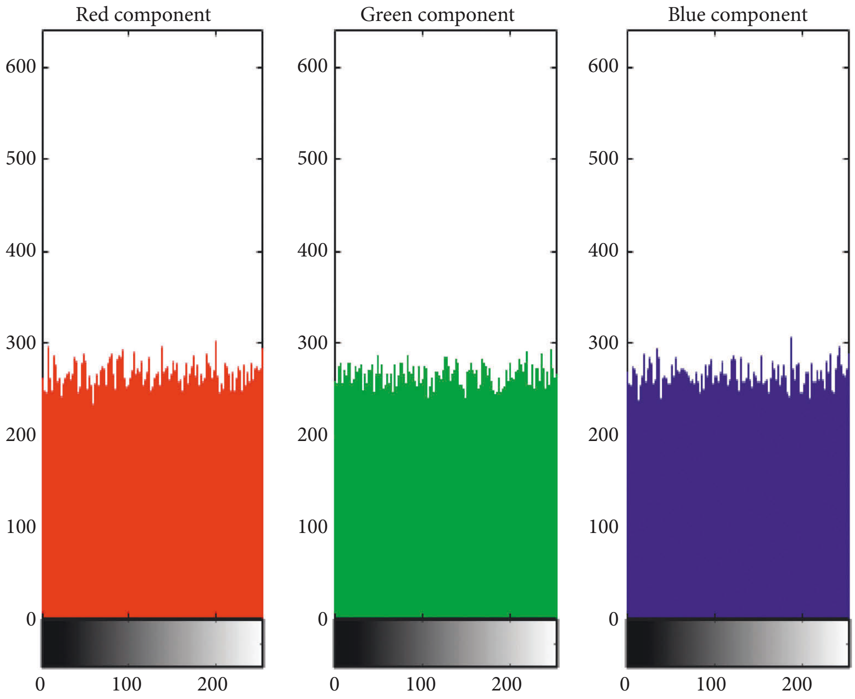

Figure 5: Histogram of the ciphered image of the colored Lena 256×256 image.

Table 1: χ^2-test results for the assessment of histogram uniformity.

Metrics	boat.512	Elaine	Lena	Goldhill	Peppers	Baboon
p-Value	0.5465	0.4369	0.1254	0.2465	0.4265	0.1564
Decision (H = 0 or 1)	0 Accepted	0 Accepted	0 Accepted	0 Accepted	0 Accepted	0 Accepted

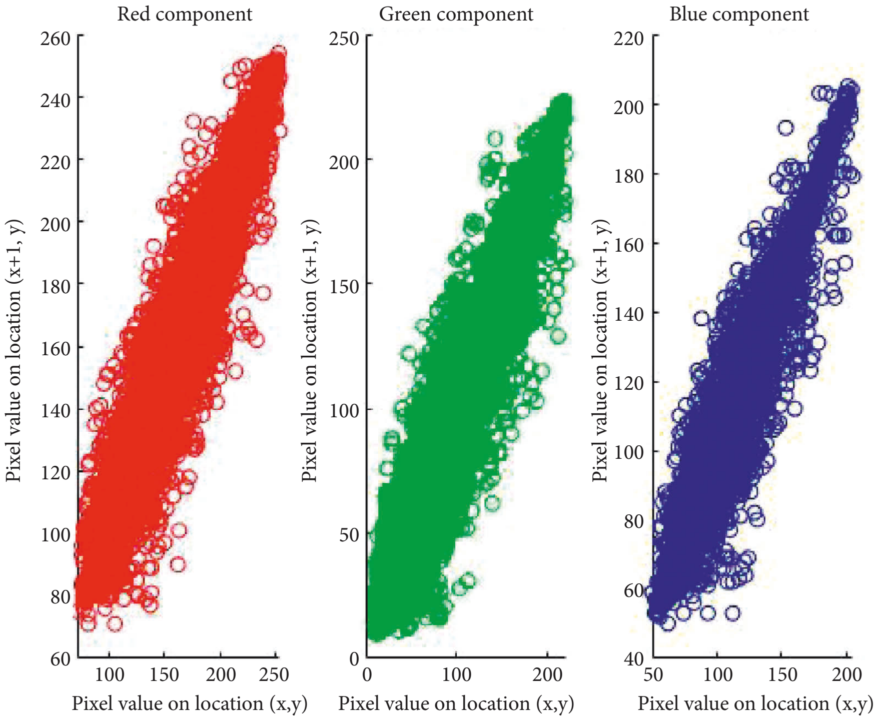

Figure 6: Correlation of Lena’s original image (colored 256 × 256 pixels).

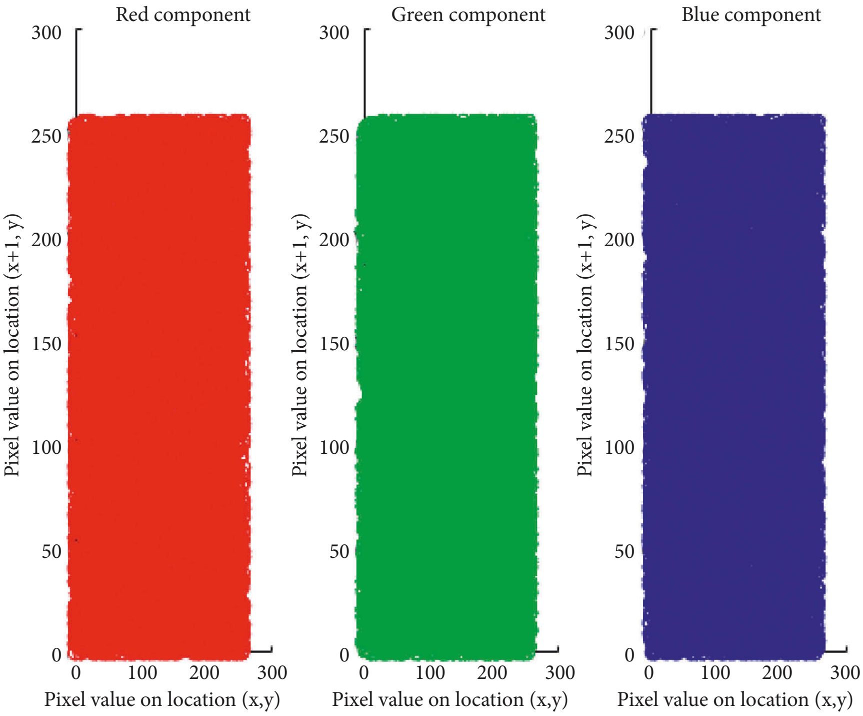

Figure 7: Correlation of Lena's encrypted image.

Table 2: Correlation coefficients of different pictures.

	Direction	Red		Green		Blue	
		Plain	Cipher	Plain	Cipher	Plain	Cipher
Lena	Horizontal	0.9910	0.0056	0.9889	−0.0024	0.9846	−0.0035
	Vertical	0.9781	0.0036	0.9741	−0.0012	0.9709	−0.0023
	Diagonal	0.9648	−0.0024	0.9613	0.0029	0.9563	0.0043
Girl	Horizontal	0.9519	−0.0065	0.9425	0.0016	0.9325	−0.0065
	Vertical	0.9791	0.0013	0.9652	0.0063	0.9856	0.0013
	Diagonal	0.8293	−0.0004	0.8292	−0.0044	0.8565	−0.0089
Boat	Horizontal	0.8578	0.0045	0.8895	−0.0053	0.8522	0.0045
	Vertical	0.9091	−0.0069	0.9254	−0.0089	0.9159	−0.0069
	Diagonal	0.8393	−0.0022	0.8263	0.0012	0.8152	−0.0022
Baboon	Horizontal	0.7307	0.0016	0.7205	0.0021	0.7141	0.0542
	Vertical	0.6683	0.0063	0.6545	−0.0024	0.6451	0.0063
	Diagonal	0.6511	−0.0044	0.6485	−0.0065	0.6487	-0.0044
Cameraman	Horizontal	0.9511	−0.0053	0.9455	0.0013	0.9412	−0.0078
	Vertical	0.9391	−0.0089	0.9855	−0.0004	0.9831	−0.0089
	Diagonal	0.8943	0.0056	0.8255	0.0056	0.8147	0.0056

$$H(G) = \sum_{i=0}^{2^N-1} P(G_i)\log_2 \frac{1}{P(G_i)}, \qquad (6)$$

where G indicates an encrypted image and $P(G_i)$ indicates the probability of a specific character in the enciphered image. It should have an unfeasible capability to judge the original image from the encrypted one for the security of the image enciphering technique. Some opportunities are accessible for the forecast of an original image from an encrypted image having an entropy value 8. The adversary will be able to crack an image when the value becomes closest to 8. The value of an entropy of the encrypted picture obtained from the constructed cryptosystem encryption is 7.9990 by using MATLAB R2018a. The outcome in Table 3 shows that the new data entropy value is closer and sufficient to the standard value of 8. It guarantees that none of the information will be stray in this procedure.

6.3.2. Local Entropy. Local Shannon entropy (LES) [36] is also used to measure the randomness of the encrypted image in the sense of viewing the randomness, locally. It can be calculated by the following equation:

Table 3: The comparison of data entropy values.

Image enciphering technique	Lena	Baboon	Girl
Reference [13]	7.9971	7.9771	7.9564
Reference [30]	7.9992	7.9692	7.9625
Reference [31]	7.9967	7.9767	7.9667
Reference [32]	7.9993	7.9263	7.9243
Reference [33]	7.9970	7.9700	7.9600
Reference [34]	7.9970	7.94545	7.9645
Reference [35]	7.9974	7.9565	7.9455
Proposed algorithm	7.9990	7.9800	7.9720

Table 4: The comparison of data entropy values

Image enciphering technique	boat.512	Elaine	Lena	Goldhill	Peppers	Baboon	Pass rate
Reference. [37]	**7.901879**	**7.902989**	7.904512	7.9015092	7.9053045	**7.902999**	3/6
Reference. [38]	7.9000555	7.90006208	**7.92938**	7.9009052	**7.9016155**	7.9004801	2/6
Reference. [39]	7.9009823	7.9029109	7.904671	**7.9020145**	7.9007481	7.9013492	1/6
Reference [40]	**7.9026992**	7.9009196	7.903462	**7.9025015**	**7.9024452**	**7.9033626**	4/6
Proposed algorithm	**7.9016972**	7.9029186	**7.903386**	**7.9028150**	**7.9025249**	**7.9018264**	5/6

Table 5: NCPR and UACI results.

Image encryption cryptosystem	NPCR	UACI
Reference. [13]	99.615	33.489
Reference. [30]	99.621	33.463
Reference. [31]	99.217	33.405
Reference. [32]	99.664	33.612
Reference. [33]	99.608	33.431
Reference [34]	99.586	33.253
Reference [35]	99.650	33.480
Proposed cryptosystem	99.6221	33.46

$$H_{m,n}(G) = -\sum_{i=1}^{m} \frac{H(G_i)}{m}, \tag{7}$$

where G_1, G_2 $\cdot \cdot \cdot$, G_m are m are the randomly chosen nonoverlapping image blocks and n is the number of pixels with in a test image G . For a test image to be passed through the LSE test, the values of $H_{m,n}$ must be within the interval of (7.901515698, 7.903422936) with a level of significance $\alpha = 0.001$.

Table 4 shows the LSE results of the proposed technique and its comparison with the results of the other algorithms. The test images encrypted by the proposed algorithm pass the test, and the pass rate is higher than the other algorithms, which shows the good randomness of the proposed algorithm.

6.4. Differential Analysis. Minor changes to the hidden key ought to be specifically delicate to a certified encryption strategy [29]. An admissible algorithm ought to be profoundly delicate to its secret key, which tells about a small change in the secret key should yield completely unique code outcomes.

Besides, having a marginally altered real key, the calculation must not be able to decrypt a coded image or retrieve a few examples from the genuine image. In this existing algorithm, the consequence of encoded calculation is completely changed or valid if a tiny alteration in any piece of the key is obtained. The aftereffect of our plan decoding is changed by a small change in any of the given three keys K, K', K''. This shows that if we include 0.798079790000001 to a single part of the keys, utilizing that key for decoding will not give us an original image after decoding.

In cryptography, plaintext affectability examination is otherwise called differential investigation. We utilize net pixel transformation rate (NPCR) to check change of solitary pixel esteem in original image, and brought together normal evolving force (UACI) of contrast among plain and encoded picture, to check the presentation of making single pixel change in the encoded image just as in the unique image. These two estimating qualities can be determined by the following formulas:

$$\text{NPCR} = \frac{\sum_{i,j} K(i,j)}{m \times n} \times 100, \tag{8}$$

$$\text{UACI} = \frac{1}{m \times n} \left[\sum_{i,j} \frac{\left| X(i,j) - X'(i,j) \right|}{255} \right] \times 100, \tag{9}$$

where m and $\mathbf{n}$ display the stature and width of the encoded picture, respectively. $\mathbf{X}$ shows the encrypted picture, while X' indicates a one-pixel alteration in the primary image. If $X \neq X', K(i,j) = 1;$ else, $K(i,j) = 0$. It must be impervious to differential assaults when the upsides of UACI and NPCR approach their correct values. We differentiate the values of the encrypted image of Lena's NPCR and UACI in Table 5.

It is shown that the current plan gets max operation for the two qualities. For this situation, the current plan gives a decent insurance against the "realized plaintext assault" and "picked plaintext assault." So, the outcomes indicate that the constructed cryptosystem has good plaintext vulnerability.

Table 6: Estimate of critical values of NPCR and UACI.

Image encryption algorithm	Obtained value (%)	NPCR test results		
		0.05-level	0.01-level	0.001-level
			Theoretical NPCR values	
		99.5693%	99.5527%	99.5341%
Proposed algorithm	99.62	Pass	Pass	Pass
			UACI test results	
		0.05-level	0.01-level	0.001-level
			Theoretical UACI values	
		33.2824% to 33.6447%	33.2255% to 33.7016%	33.1594% to 33.7677%
Proposed algorithm	33.46	Pass	Pass	Pass

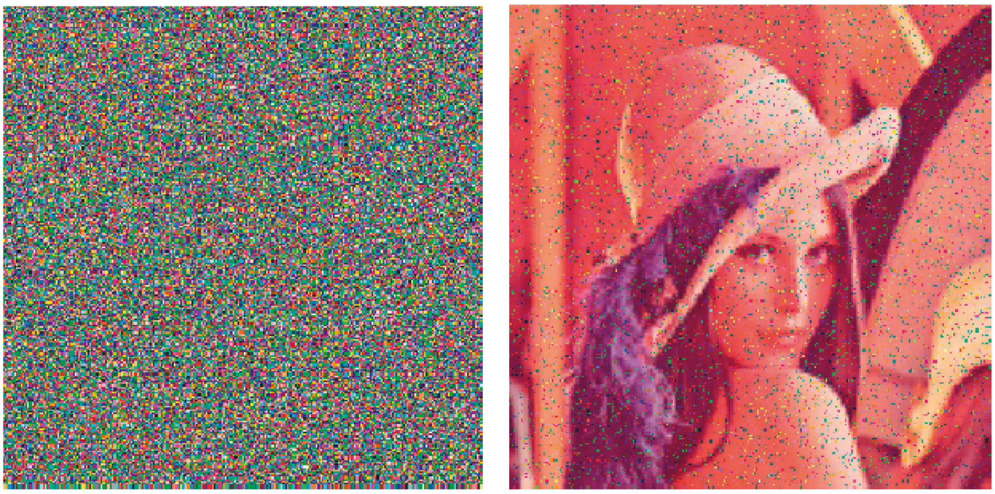
(a) (b)

Figure 8: Data loss attacks on the encrypted image. (a) and (b) are cipher images and decryption result of corresponding images using our algorithm with 1% salt and pepper noise, respectively.

The estimate of critical values of NPCR and UACI [41] of the proposed scheme is given in Table 6.

6.5. Noise and Data Loss Attacks. In the cipher image of test image Lena, we add 1%, 5%, and 10% salt and pepper noise as shown in Figure 8(a), 9(a), and 10(a), respectively. The corresponding decrypted images of noised cipher images are shown in Figure 8(b), 9(b), and 10(b), respectively. From these figures, it is evident that when the cipher image bear salt and pepper noise or data loss attacks, the decrypted image preserves huge majority of original image information having only a small portion of uniformly distributed noise [42].

6.5.1. Mean Square Error Analysis. The distinction associating the genuine and coded images is determined by the mean square error (MSE). Mean square error has a high worth when the distinction between the genuine and the code image is enormous. It is produced by the recipe given in the following condition:

$$\mathrm{MSE} = \frac{1}{m \times n \times 3} \sum_{i=0}^{m-1} \sum_{i=0}^{n-1} \sum \left(I_P(i,j) - I_D(i,j) \right)^2, \tag{10}$$

where m shows the quantity of lines and n shows the quantity of segments individually. I_P and I_D indicate the original image and scrambled image, respectively. To have a divergence between original and the scrambled image, MSE ≥30 db. The mean square error of the algorithm is shown in Table 7.

6.5.2. Peak Signal-to-Noise Ratio Analysis. The term PSNR [43] is an articulation for the proportion between the most extreme conceivable worth (force) of a sign and the force of bending of commotion that influences the nature of its portrayal. This proportion is utilized as a quality estimation between the first and a compacted picture. The higher the

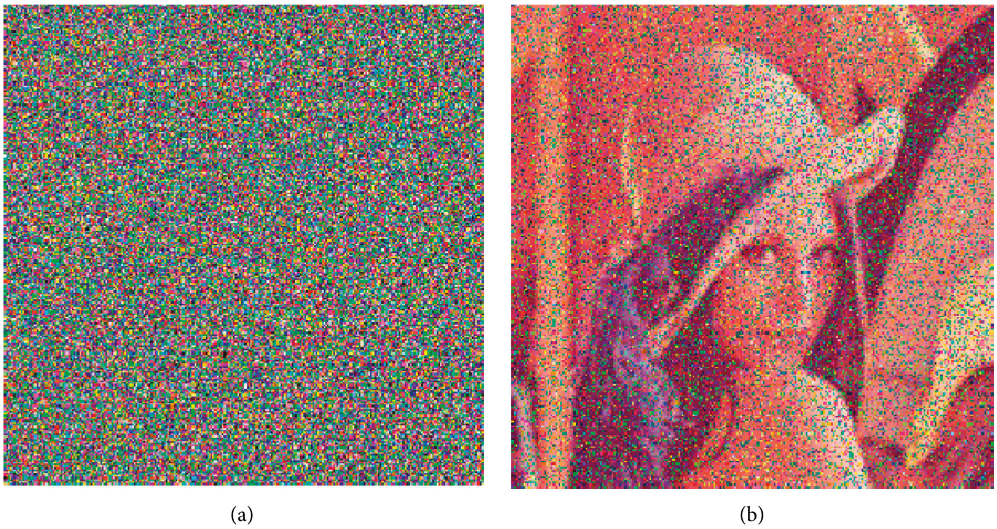

Figure 9: Data loss attacks on the encrypted image. (a) and (b) are cipher images and decryption result of corresponding images using our algorithm with 5% salt and pepper noise, respectively.

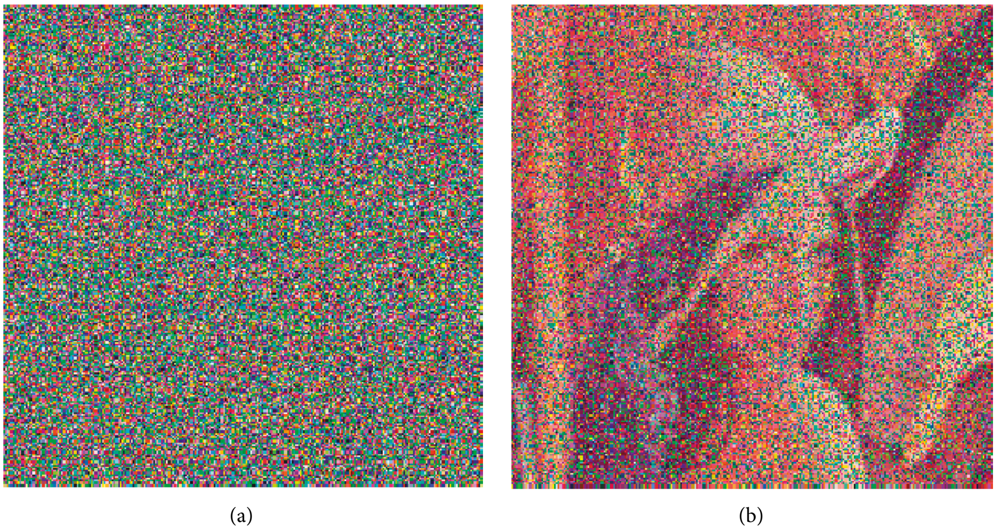

Figure 10: Data loss attacks on the encrypted image. (a) and (b) are cipher images and decryption result of corresponding images using our algorithm with 10% salt and pepper noise, respectively.

Table 7: Execution of MSE and PSNR.

Picture encryption schemes	MSE	PSNR
Reference [32]	7747.309	9.23929
Proposed algorithm	8736.9	8.7172

PSNR, the better the idea of the compacted, or revamped picture. A similarity that combines the genuine and scrambled images is estimated by NPCR. It can be obtained by using the following expression:

$$\text{PSNR} = 10.\log \frac{255^2}{\text{MSE}} \, (db). \qquad (11)$$

For a superior encryption calculation, the PSNR esteem that joins the plain and coded images ought to be pretty much as less as could be expected. The PSNR worth of built cryptosystem is given in Table 7.

The constructed cryptosystem is also registered to another selected colored image of onion having 198×135 pixels. The onion image entropy value is 7.9978. The real and ciphered results are presented in Figure 11. The encrypted image histogram and the correlation of the nearest pixel values of real and encrypted images are presented in Figure 12, 13, and 14, respectively. The coefficient correlation of the cipher result of onion is given in Table 8.

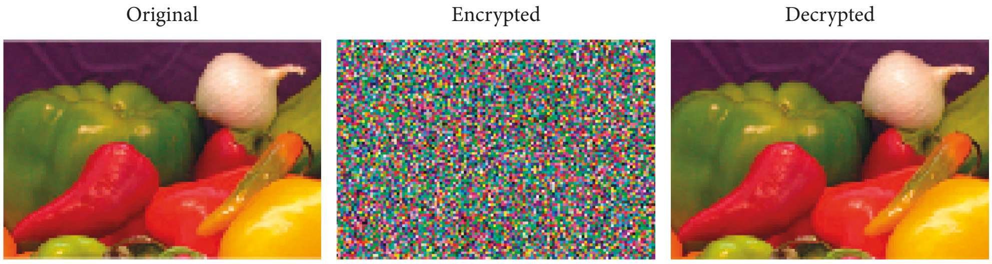

FIGURE 11: Original, encrypted, and decrypted images of onion (colored 198×135 pixels).

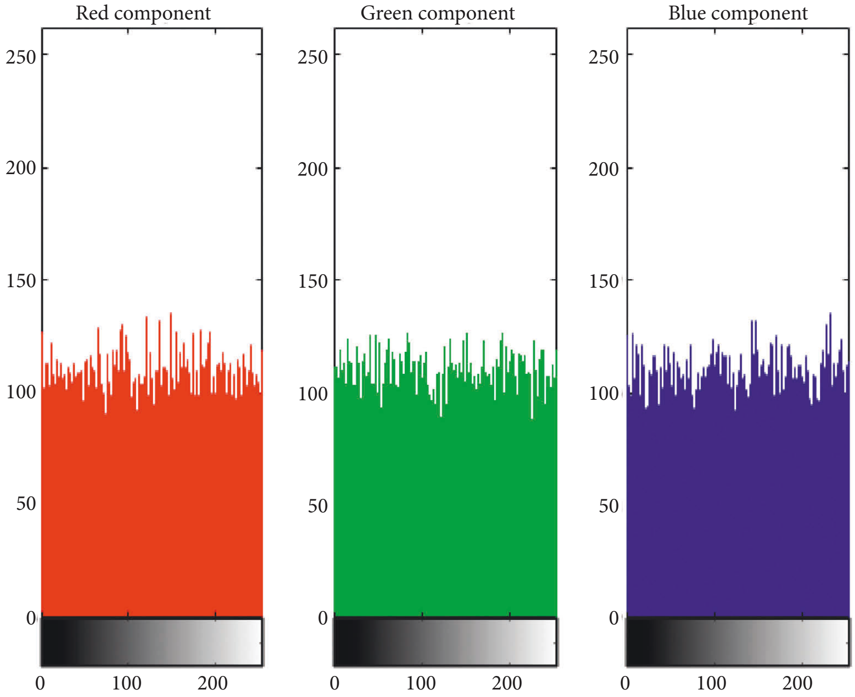

FIGURE 12: Histogram of encoded image of colored 198×135 onion.

6.6. *Security Analysis*

6.6.1. Key Space Analysis. Key space in security points should be viable. To oppose the savage power assault, the key space should be of huge order for a safe coded image. It is a principle part of any cryptosystem. For common sense, utilize a sizable key space is agreeable. With the progression of time, a PC's ability of an encryption cryptosystem can sidestep complete strike [44] if the secret key space is greater than 10^{38}. In our developed cryptosystem, the secret key is made out of three mystery keys, and each key is diverse for an alternate period of the plan. The first key is used for the progression made from the sine map, the second key is created from a circulant network and is used for Hill figure, and the third one is used for the course of action delivered from a turbulent tent guide. In this manner, the built cryptosystem's key space is $10^{72} > 10^{38}$ that is too enormous to even think about saving the data against savage power assaults. The correlation of key space size is given in Table 9.

6.6.2. Computational Complexity. The computational intricacy of our proposition is portrayed as follows. A quickest registering machine can figure 10^{24} calculations each second. Thus, the quantity of estimations executed by the processing machine each year is $10^{24} \times 365 \times 24 \times 60 \times 60$.

Thus, $10^{72}/10^{24} \times 365 \times 24 \times 60 \times 60 = 10^{43}$ years are needed to break the proposed calculation. The time span of 10^{43} years is adequately immense to get our proposed encryption cryptosystem against the monster power attack.

6.6.3. Key Sensitivity Analysis. Minor changes to the mysterious key ought to be especially delicate to a certified encryption technique [44]. A sufficient estimation should be significantly delicate to its mysterious key, which tells about a minor change in the mysterious key should yield absolutely interesting code results.

The antidynamic degradation theorem and the theory presented in the article [45] prove that the chaotic flow cryptosystem is safe. Moreover, with a marginally changed

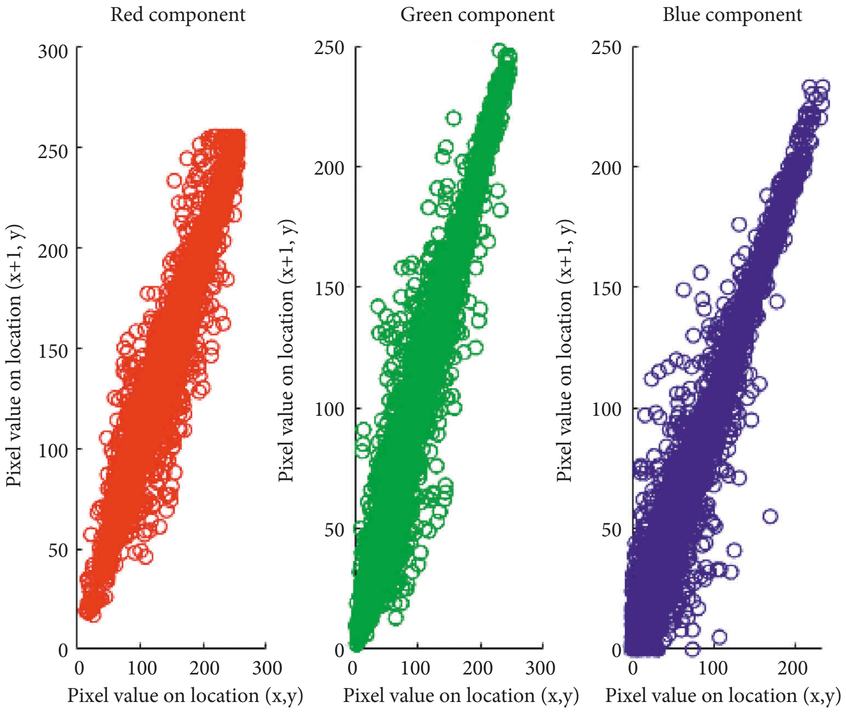

Figure 13: Correlation investigation of original colored 198×135 image of onion.

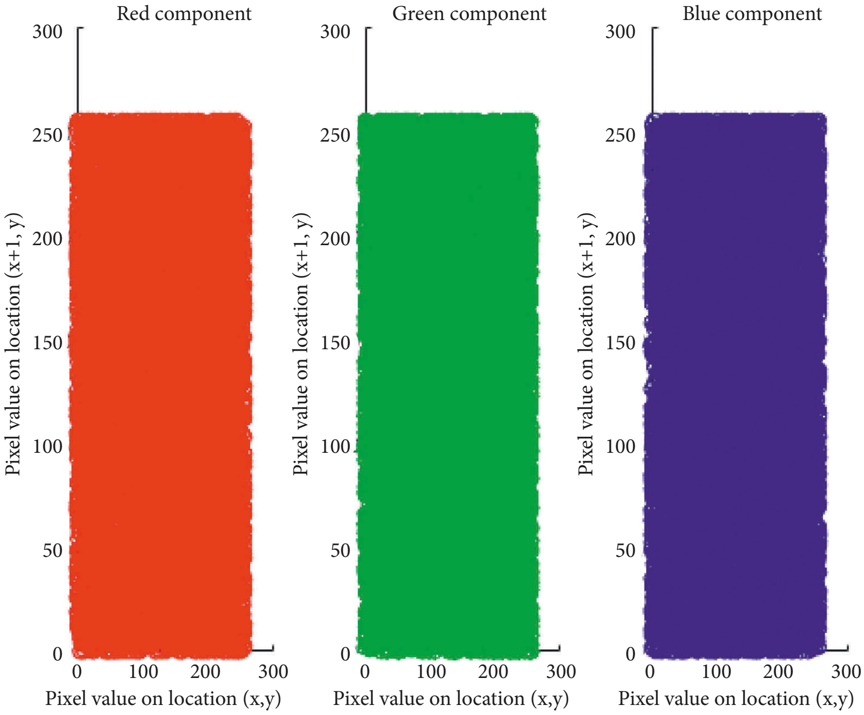

Figure 14: Correlation investigation of color bands of colored 198×135 ciphered image of onion.

genuine key, the calculation must not be able to decode a coded image or retrieve a few examples from the genuine image. In this present cryptosystem, the aftereffect of encoded calculation completely change is valid if a smidgen change in any piece of the key is made. The aftereffect of our plan's decoding is totally reshaped with a minor control in any of the three keys K, K', K''. This implies that on the off chance that we add 0.000000000000001 to the first key, utilizing that key for the most common way of interpreting will not give us the genuine image after decoding.

Table 8: Correlation coefficients of adjoining pixels of the original and encrypted images of onion.

Direction	Red		Green		Blue	
	Original	Encrypted	Original	Encrypted	Original	Encrypted
Horizontal	0.9826	−0.0016	0.9786	0.0040	0.9648	0.0086
Vertical	0.9900	−0.0073	0.9880	−0.0012	0.9751	0.0039
Diagonal	0.9721	−0.0025	0.9675	−0.0071	0.9427	−0.0082

For the analytical investigation of key sensitivity, CDR (ciphertext difference rate) has been used that is defined in the following equations [46]:

Table 9: Key space size comparison.

Encrypted cryptosystem	Key space size
Reference [30]	10^{70}
Reference [31]	10^{51}
Reference [34]	10^{16}
Proposed algorithm	10^{72}

$$\begin{aligned}
Y &= C(I, K),\\
Y_1 &= C(I, K + \Delta K),\\
Y_2 &= C(I, K - \Delta K),
\end{aligned}$$

$$\operatorname{Diff}(A, B) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} \operatorname{Diff} p(A(i, j), B(i, j)), \operatorname{Diff} p(A(i, j), B(i, j)) = \begin{cases} 1, & (A(i, j) \neq B(i, j)),\\ 0, & (A(i, j) \equiv B(i, j)),\end{cases} CDR = \frac{\operatorname{Diff}(Y, Y_1) + \operatorname{Diff}(Y, Y_2)}{2 \times N^2} \times 100. \tag{12}$$

The minor changes in the factors (h_0, β, z_0, μ) affect the key space. We carried four different tests for four factors and updated by ± ΔK as follows: $(\pm \Delta K = (\pm \Delta h_0, \pm \Delta\beta, \pm \Delta z_0, \pm \Delta\mu)$ represents the small change in these factors:

h_0 is changed from 0.99 to $h_{0+} = h_0 + \Delta h_0$ and $h_{0-} = h_0 - \Delta h_0$ for $\Delta h_0 = 10^{-15}$

β is changed from 0.79 to $\beta_+ = \beta + \Delta\beta$ and $\beta_- = \beta - \Delta\beta$ for $\Delta\beta = 10^{-15}$

z_0 is changed from 0.66 to $z_{0+} = z_0 + \Delta z_0$ and $z_{0-} = z_0 - \Delta z_0$ for $\Delta z_0 = 10^{-15}$

μ is changed from 3.78 to $\mu_+ = \mu + \Delta\mu$ and $\mu_- = \mu - \Delta\mu$ for $\Delta\beta = 10^{-15}$.

To calculate the values of Y, Y_1 and Y_2, $h_0 = 0.99$, $h_{0+} = 0.990000000000001$ and $h_{0-} = 0.989999999999999$ are used and consequently the value of CDR is 99.56%. The key sensitivity over 99% is considered to be acceptable. For the other factors, the values of CDR are given in Table 10. From Table 10, it can be seen that the proposed encryption technique has key sensitivity over the desired threshold.

6.7. Contrast Analysis. The variation in local intensity in an image is measured by the contrast analysis. This statistical test ensures how much the texture of an image is homogeneous. It enables to detect the objects in the texture of an image. Greater values of contrast measurement designates that the image has considerably different gray levels and the lesser values is a symbol for constant gray levels. The following formula is used to estimate the contrast of an image [34]:

$$\mathrm{C} = \sum_{i,j} |i - j|^2 \times p(i, j), \tag{13}$$

where *p(i, j)*is the number of gray-level co-occurrence matrices (GLCM). The results of the contrast test of the plain image and encrypted images are shown in Table 11. It can be noticed from the results that the new scheme has higher contrast levels as compared to the values of plain images in [47, 48]. The higher values of contrast in the proposed algorithm indicate that there is a high level of randomness.

6.8. Execution Time. For the security level, the execution time is also a significant feature [49]. The execution time of the proposed encryption algorithm is evaluated and compared with some previous proposals for the grayscale images of different sizes. The results are given in Table 12, which establishes the dominance of our proposal, in terms of its efficiency and speed.

7. Conclusion

With the development of computer networks and communication technology, the security problems of transferring information have become an important factor and a secure process to transfer the information is an encryption method. Due to strong correlation, large quantity of information, and a large restriction of the picture, a new solution is required. The advancement of disorder hypothesis put together a goal to image encryption research. A few elements of bedlam are pseudo-randomness, history, and the affectability of beginning conditions, which meets the fundamental cryptographic prerequisites that are disarray and dissemination. For the security of data, a changed

Table 10: CDR values of encrypted images for various values of R.

Test factor	$R=1$ (%)	$R=2$ (%)	$R=6$ (%)
h_0	99.56	99.55	99.57
β	99.57	99.60	99.59
z_0	99.59	99.57	99.60
μ	99.58	99.59	99.61

Table 11: Contrast test of plain and encrypted images.

Images	Plain image	Reference [47]	Reference [48]	Proposed algorithm
Lena	0.7207	0.2213	10.4511	11.5012
Baboon	0.8582	0.2722	10.4784	11.5187
Girl	0.3058	0.2101	10.3345	11.3748
Boat	0.7207	0.2332	10.4423	11.4921
Cameraman	0.3058	0.2627	10.1365	11.1782

Table 12: Execution time (ms) comparison.

Image size	Reference [50]	Reference [51]	Reference [52]	Reference [49]	Proposed algorithm
256 × 256	109	7641	189	48	45
512 × 512	390	34768	758	139	130
1024 × 1024	1482	151709	3097	481	478

Table 13: Results compared with different techniques.

Techniques	NPCR	UACI	Correlation coefficients			Entropy
			Horizontal	Vertical	Diagonal	
Reference [13]	99.6881	37.5600	0.0015	0.0043	0.0023	7.9877
Reference [30]	99.631	33.499	−0.00002	0.0008	−0.0002	7.988
Reference [31]	99.5956	33.5512	−0.0023	0.0011	0.0004	7.9975
Reference [32]	99.664	33.612	0.0004	0.0030	−0.0391	7.9993
Reference [33]	99.6352	33.5614	0.0053	-0.0089	0.0126	7.9987
Reference [34]	99.586	33.253	0.0019	0.0038	−0.0019	7.9970
Reference [35]	99.650	33.480	0.0022	−0.0002	0.0044	7.9974
Proposed algorithm	99.61	33.46	−0.0001	0.00003	0.0015	7.9991

picture encoding cryptosystem is created. The article is made out of another shaded picture calculation utilizing a sine map and a turbulent tent guide for encryption. The change stage is regulated by a sine guide and scattering is done by a tumultuous tent guide and XOR movement. Key space is sufficient to oppose beast power assault. The key sensitivity of the method, the entropy, and correlation of scrambled image and security analysis of the method have an ascendancy on the security and authenticity of Lena and onion images. The suggested image encryption technique is extremely stable, as evidenced by a variety of assessment tests. Table 13 summarizes the outcomes of the tests and efficiency checks, which are compared to various techniques.

Data Availability

All data used to support the findings of the study are included within the article.

Conflicts of Interest

All authors declare that there are no conflicts of interest.

Acknowledgments

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R236), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

References

[1] X. Y. Wang, Y. Q. Zhang, and X. M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015.

[2] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[3] Y. Q. Zhang and X. Y. Wang, "A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice," *Information Sciences*, vol. 273, pp. 329–351, 2014.

[4] A. Uhl and A. Pommer, *Image and Video Encryption, Digital Rights Management to Secured Personal Communication*, Springer, Berlin, Germany, 2004.

[5] R. Anderson, E. Biham, and L. Kundsen, "A proposal for the advanced encryption standard," in *Proceedings of the 1st Advanced Encryption Standard AES Conference*, Ventura, CA, USA, August 1998.

[6] X. Yuan, L. Yang, and R. Liu, "A chaotic image encryption based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, 2010.

[7] X. Wang and J. Yang, "A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient," *Information Sciences*, vol. 569, pp. 217–240, 2021.

[8] X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Information Sciences*, vol. 486, pp. 340–358, 2019.

[9] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, pp. 1154–1169, 2021.

[10] Y. Guodong, P. Chen, and H. Xiaoling, "A Chaotic Color Image Encryption Algorithm Based on Information Entropy," *International Journal of Bifurcation and Chaos*, vol. 28, 2021.

[11] S. Li and X. Zheng, "Cryptanalysis of a chaotic image encryption method, " international symposium on circuit and systems," *Proceedings*, vol. 2, 2002.

[12] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.

[13] X. Wang and H. Zhang, "A color image encryption with heterogeneous but-permutation and correlated chaos," *Faculty of Electronic Information and Electrical Engineering*, vol. 342, pp. 51–60, University of Dalian, China, 2015.

[14] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[15] C. Fu, J. B. Huang, N. N. Wang, Q. B. Hou, and W. M. Lei, "A symmetric chaos based image cipher with an improved bit-level permutation strategy," *Entropy*, vol. 16, no. 2, pp. 770–788, 2014.

[16] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.

[17] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, no. 16-17, pp. 3895–3903, 2011.

[18] Z. Tang, X. Zhang, and W. Lan, "Efficient image encryption with block shuffling and chaotic map," *Multimedia Tools and Applications*, vol. 74, no. 15, pp. 5429–5448, 2015.

[19] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, 2019.

[20] A. Abd-el-latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption, " AEU," *International Journal of Electronics and Communications*, vol. 67, no. 2, pp. 136–143, 2013.

[21] R. Liu, "Chaos-based fingerprint image encryption using symmetric cryptography," in *Proceedings of the 9th International Conference on Fuzzy Systems and Knowledge Discovery*, pp. 2153–2156, Sichuan, China, May 2012.

[22] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.

[23] X. Wang, C. Liu, and D. Jiang, "A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT," *Information Sciences*, vol. 574, pp. 505–527, 2021.

[24] P. He, K. Sun, and C. Zhu, "A novel image encryption algorithm based on the delayed map and permutation-confusion-diffusion architecture," *Security and Communication Networks*, vol. 539, pp. 195–214, 2020.

[25] B. Acharya, G. Rath, S. Patra, and S. Panigraphy, "Novel methods for generating self-invertible matrix for hill cipher algorithm," *International Journal of Security*, vol. 1, no. 1, pp. 14–21, 2007.

[26] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26–36, 2016.

[27] A. Firdous, A. ur Rehman, and M. M. Saad Missen, "A highly efficient color image encryption based on linear transformation using chaos theory and SHA-2," *Multimedia Tools and Applications*, vol. 78, no. 17, pp. 24809–24835, 2019.

[28] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, 2016.

[29] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[30] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290–299, 2012.

[31] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Optics and Lasers in Engineering*, vol. 115, pp. 7–20, 2019.

[32] I. Yaseer and F. Khalifa, "A new image encryption scheme based on hybrid chaotic maps," *Complexity*, vol. 2020, Article ID 9597619, 23 pages, 2020.

[33] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[34] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, 2015.

[35] D. Zou, M. Li, J. Li, and Z. Li, "An image encryption algorithm based on a new hybrid power exponent power system," *Information Sciences*, vol. 579, pp. 128–149, 2021.

[36] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local shannon entropy measure with statistical tests for image randomness," *Information Sciences*, vol. 222, pp. 323–342, 2013.

[37] Y. Zhou, L. Bao, and C. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Processing*, vol. 93, no. 11, pp. 3039–3052, 2013.

[38] H. Zhu, C. Zhao, and X. Zhang, "A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem," *Signal Processing: Image Communication*, vol. 28, no. 6, pp. 670–680, 2013.

[39] H. Zhu, C. Zhao, X. Zhang, and L. Yang, "An image encryption scheme using generalized Arnold map and affine cipher," *Optik*, vol. 125, no. 22, pp. 6672–6677, 2014.

[40] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "A novel image encryption scheme using the composite discrete chaotic system," *Entropy*, vol. 18, no. 8, p. 276, 2016.

[41] Y. Wu, J. P. Noonan, and S. S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," *Journal of Selected Areas in Telecommunications (JSAT)*, 2011.

[42] E. Yavuz, "A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme," *Optics & Laser Technology*, vol. 114, pp. 224–239, 2019.

[43] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[44] X. Wang, H. Zhao, L. Feng, X. Ye, and H. Zhang, "High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices," *Optics and Lasers in Engineering*, vol. 122, pp. 225–238, 2019.

[45] X. Wang and P. Liu, "A new full chaos coupled mapping lattice and its application in privacy image encryption," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 3, pp. 1291–1301, 2022.

[46] E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Computers & Electrical Engineering*, vol. 54, pp. 471–483, 2016.

[47] F. Ahmed, A. Anees, VU. Abbas, and M. Y. Siyal, "A noisy channel tolerant image encryption scheme," *Wireless Personal Communications*, vol. 77, no. 4, pp. 2771–2791, 2014.

[48] J. Ahmad and SO. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13951–13976, 2016.

[49] E. Yavuz, "A new parallel processing architecture for accelerating image encryption based on chaos," *Journal of Information Security and Applications*, vol. 63, Article ID 103056, 2021.

[50] A. Souyah and K. M. Faraoun, "An image encryption scheme combining chaos-memory cellular automata and weighted histogram," *Nonlinear Dynamics*, vol. 86, no. 1, pp. 639–653, 2016.

[51] Y. Wu, G. Yang, and H. Jin, "Image encryption using the two-dimensional logistic chaotic map," *Journal of Electronic Imaging*, vol. 21, no. 1, Article ID 013014, 2012.

[52] F. K. Mohamed, "A parallel block-based encryption schema for digital images using reversible cellular automata, " Engineering Science and Technology," *An International Journal*, vol. 17, pp. 85–94, 2014.