Hindawi
Mathematical Problems in Engineering
Volume 2023, Article ID 2003724, 13 pages
https://doi.org/10.1155/2023/2003724

Research Article

A Chaos-Based Image Encryption Scheme Is Proposed Using Multiple Chaotic Maps

Muhammad Akraam, Tabasam Rashid, and Sohail Zafar

Department of Mathematics, University of Management and Technology, Lahore State 54770, Pakistan

Correspondence should be addressed to Tabasam Rashid; tabasam.rashid@umt.edu.pk

Received 22 February 2022; Revised 6 October 2022; Accepted 12 October 2022; Published 18 May 2023

Academic Editor: Akif Akgul

Everybody wants to maintain solitariness to some extent or entirely in his dealings with other people during different modes of communication. To retain privacy, researchers materialized distinct image encryption algorithms using chaotic maps. Due to their extraordinary features, most researchers employed multidimensional chaotic maps to barricade clandestine information or digital images from potential invaders. Still, multidimensional chaotic maps have many impediments conferred in the literature review. In this paper, we developed a cryptosystem utilizing multiple chaotic maps to mitigate the shortcoming of multidimensional chaotic maps. A distinctive approach is adopted to sire a key stream using a combination of chaotic maps and create a sequence of random integers linked with the pixels of the plain image to shatter the association between neighboring pixels of a plain image. Finally, diffusion is accomplished using the previously diffused pixels at a decimal level. Security and statistical analysis demonstrate that the presented encryption algorithm is robust against well-known attacks. An ample key space indicates that it is best suited for secure communication.

1. Introduction

The importance of image encryption is increased to transmit confidential data (images, videos, audios, and agreements) via the internet because digital images are frequently used to communicate and share sensitive information, whether in the military, banking, or personal moments. Many image encryption techniques [1] have been constructed based on a variety of chaotic [2, 3] to protect the plain images from prying eyes or unlawful access. Traditional security encryption schemes like AES [4], DES [5], and IDEA [6] are inadequate to maintain acceptable standards for the safety of digital images because of the strong association among neighboring pixels, enormous storage capacities, and significant redundancy.

Chaotic systems are deemed to be appropriate for image encryption schemes due to their features like ergodicity, pseudorandomness, ambiguity, high sensitivity to initial conditions, and controlled parameters. Most researchers designed cryptosystems [7, 8] either by modifying existing chaotic systems [9, 10] or developing new chaotic systems [11, 12], keeping in mind the usefulness of chaotic systems due to their characteristics, as mentioned earlier. The authors of [13] proposed a 2D-LSM chaotic system and ascertained that it is more chaotic than some lately developed two-dimensional chaotic maps using a bifurcation diagram, LE, phase plane trajectory, and sample entropy. Furthermore, it materializes a color image encryption algorithm (CIEA) using orthogonal Latin square and 2D-LSM. Hua et al. [14] conferred a new 2D-PPCS (two-dimensional parametric polynomial chaotic system) to mitigate the flaws of existing chaotic systems, and theoretical analysis exhibits the chaotic behavior of the 2D PPCS. The study of [15] modifies the chaotic behavior of a 1-dimensional chaotic map, further analyzed the chaotic behavior through phase diagram and Lyapunov exponent spectrum, and constructs a novel image encryption scheme. There are two types of chaotic systems: (i) one or 2– dimensional chaotic maps and (ii) multidimensional chaotic maps. Most recent image encryption techniques are based on multidimensional chaotic maps [16, 17], which are more sensitive than 1-dimensional chaotic maps. It contains many initial values and controlled parameters that help enlarge the length of key space to resist brute force attacks. In [18], Malik et al. developed a cryptosystem for a color image using two multidimensional chaotic maps and used the idea of histogram equalization to equalize histogram of chaotic sequences of Lorenz system. Hua et al. [19] suggested an image encryption scheme using S-box, yielded using a complete Latin square. Experimental consequences divulge that the presented cryptosystem can defy all well-known security and statistical seizures from potential invaders. The authors of [20] designed an image encryption scheme utilizing parallel compressing sensing with adaptive thresholding sparsification. In [21], to get the random sequences of a 5-dimensional hyperchaotic map, first generate the initial values that depend on pixels of a plain image. A unique key is generated after rearranging the random sequences and constructed an image encryption algorithm. Multidimensional chaotic maps take more time during the execution process due to their intricate structure and method to find the solutions of a multidimensional chaotic map. Alternatively, one or 2 – dimensional chaotic maps are simple in structure and execute efficiently in the available MATLAB versions, not taking more time during the computational process. Therefore, we use a combination of chaotic maps rather than the multidimensional chaotic system in this paper. The logistic map, piecewise linear chaotic map, tent map, and Henon map are used to propose an encryption algorithm. Two unique keys are generated using the aforementioned chaotic maps to diffuse the pixels of the plain image at the decimal level. To break the connection among nearby pixels in a plain image, generate a random sequence of integers using any chaotic map, relate it with the diffused pixels, and further use it to scramble the diffused pixels. Finally, the presented encryption algorithm is evaluated on various images, including Lena, Baboon, Pepper, Cameraman, and House. The experimental results demonstrate the effectiveness of our presented image encryption algorithm.

The remaining sections of the paper are organized as follows. The basic features of distinct chaotic maps are described in Section 2. Each step of the proposed encryption method is discussed in detail in Section 3. Various security and statistical tests are performed in Section 4 to assess the performance of the constructed cryptosystem. Conclusions are discussed in Section 5.

2. Chaotic Map

In this section, we will discuss some chaotic maps which are further utilized in an image encryption scheme.

2.1. Logistic Map. Logistic map is a 1-dimensional chaotic map with excellent chaotic features and its numerical expression is described as follows:

$$x_{(i)} = u_1 \times x_{(i-1)} \times \left(1 - x_{(i-1)}\right), \tag{1}$$

where u_1 is a controlled parameter and its range is $[0, 4]$, but the bifurcation diagram of a logistic map shows chaotic behavior only when $u_1 \in [3.567, 4]$ can be seen in Figure 1(a). This map highly sensitive to initial condition $x_{(i)}$ and the range of initial condition is (0, 1).

2.2. Piecewise Linear Chaotic Map. Piecewise linear chaotic map [22] is a one dimensional map that generates the random sequence necessary for image encryption scheme during the process of confusion and diffusion. Mathematical formula of piecewise linear chaotic map is given as follows:

$$y_{(i)} = \begin{cases} \dfrac{y_{(i-1)}}{u_2}, & \text{if } 0 \le y_{(i-1)} < u_2, \\[2ex] \dfrac{y_{(i-1)} - u_2}{0.5 - u_2}, & \text{if } u_2 \le y_{(i-1)} < 0.5, \\[2ex] 1 - y_{(i-1)}, & \text{if } 0.5 \le y_{(i-1)} < 1, \end{cases} \tag{2}$$

where $u_2 \in (0, 0.5)$ is a parameter and its initial value range is $(0, 1)$. The bifurcation diagram of piecewise linear chaotic is in Figure 1(b) that shows the chaotic behavior of piecewise linear chaotic map.

2.3. Tent Map. Numerical formula of tent map is described as follows:

$$z_{(i)} = \begin{cases} u_3 \times z_{(i-1),} & \text{if } 0 \le z_{(i-1)} < \dfrac{1}{2}, \\[2ex] u_3 \times \left(1 - z_{(i-1)}\right), & \text{if } \dfrac{1}{2} \le z_{(i-1)} \le 1, \end{cases} \tag{3}$$

where $u_3 \in (0.5, 2)$ is a parameter and its initial value range is $(0, 1)$. Chaotic behavior of tent map can be seen in Figure 1(c).

2.4. Hénon Map. Hénon map [23] is a 2-dimensional chaotic map and its mathematical equation is described as follows:

$$w_{1(i)} = 1 + w_{2(i-1)} - u_4 \times \left(w_{1(i-1)}\right)^2, \tag{4}$$

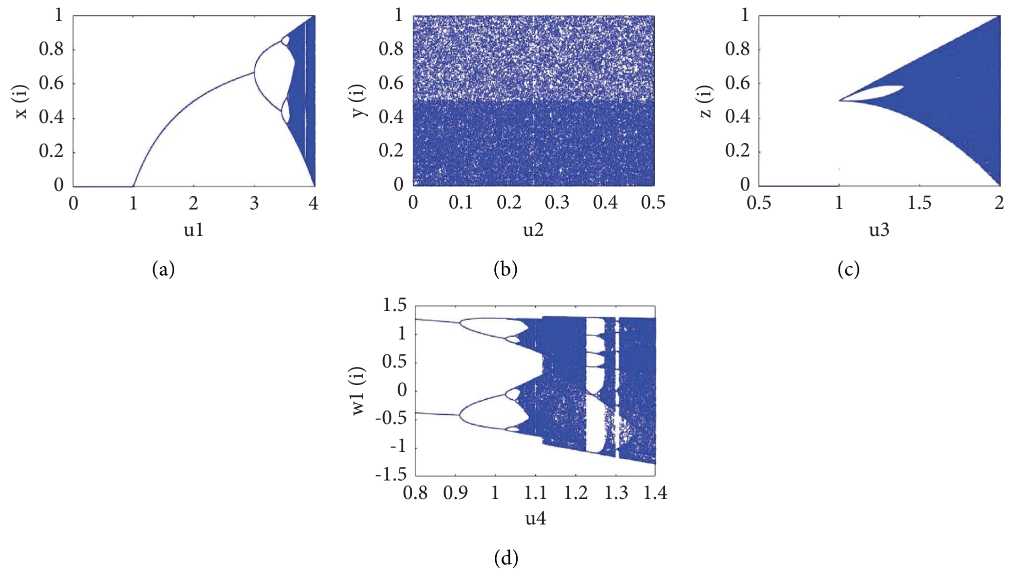
$$w_{2(i)} = u_5 \times w_{1(i-1)}. \tag{5}$$

The Hénon map depends on two control parameters u_4 and u_5, and highly sensitive to initial conditions which belongs (0, 1). The chaotic behavior of the Hénon map can be seen in bifurcation diagram against the parameter $u_4 \in [0.8, 1.4]$ in Figure 1(d).

3. Proposed Image Encryption Scheme

This section will discuss all the necessary things of an encryption process in detail, like key generation, block scrambling, and pixels scrambling process, and decimal level diffusion process.

Step 1. Transformation



(a)

(b)

(c)

(d)

Figure 1: Bifurcation diagrams of logistic map, piecewise linear chaotic map, tent map, and Henon map.

Let I be a grayscale image of size $M \times N$, where M and N indicate rows and columns, respectively. Now, we transform image I into a 1 – dimensional array P_1 of size $L = M \times N$.

Step 2. Key Stream Generation

(i) Let x_0, y_0, z_0, w_{10}, w_{20}, u_1, u_2, u_3, u_4, and u_5 be the initial conditions and control parameters that are used to iterate the equations from (1) to (5).

(ii) After iteration the pseudorandom generated sequences $\{x_{n_0+L}\}$, $\{y_{n_0+L}\}$, $\{z_{n_0+L}\}$, $\{w_{1_{n_0+L}}\}$, and $\{w_{2_{n_0+L}}\}$.

(iii) To remove the transient effect, discard the first n_0 iterations from each sequence $\{w_{2_L}\}$, $\{y_L\}$, $\{z_L\}$, $\{w_{1_L}\}$, and $\{x_L\}$ and obtained new sequences x_1, x_2, x_3, x_4, and x_5, respectively, of length L.

(iv) Choose the one sequence from the sequences x_1, x_2, x_3, x_4, and x_5 and after selecting the sequence, store them in A , in ascending order.

(v) Now generate sequence T of random integers by storing the position of each member of A in the selected sequence.

(vi) Divide the sequence T into four subsequences T_1, T_2, T_3, and T_4, the length of each subsequence is $L/4$;

$$T_i \cap T_j = \varnothing \text{ such that } i \neq j \text{ and } 1 \leq i, j \leq 4. \tag{6}$$

(vii) Now, select the state of variables from the remaining four sequence named as Y_1, Y_2, Y_3, and Y_4 and get the subsequences S_1, S_2, S_3, and S_4, respectively of length $L/4$ using the expression described as follows:

$$S_{n+j}(k) = Y_{n+j}(T_i(k)) \text{ such that } k \text{ from 1 to } \frac{L}{4}, \tag{7}$$

where n means number of encryption rounds and for each n, $i = 1, 2, 3, 4$ and $j = 0, 1, 2, 3$. if $(n + j) > 4$ then $(n + j) = (n + j) \bmod 4$.

(viii) The subsequences S_1, S_2, S_3, and S_4 are used to form a sequence of length L.

(ix) We have 4! ways to form a sequence of length L by using the subsequences S_1, S_2, S_3, and S_4.

(x) Now obtained two sequences B_1 and B_2 of length L using two different arrangements of S_1, S_2, S_3, and S_4.

B_1 = arrangement of sequences $\{S_2, S_1, S_3, S_4\}$.

B_2 = arrangement of sequences $\{S_3, S_2, S_4, S_1\}$.

(xi) Compute the key streams D_1 and D_2 using the mathematical formula described as follows:

$$\begin{aligned} D_1(i) &= \left\lfloor \left| \frac{B_1(i) \times w_1(i) \times y(i)}{x(i) \times 255^5} \right| \times 10^{16} \right\rfloor \bmod 256, \\ D_2(i) &= \left\lfloor \left| \frac{B_2(i) \times w_2(i) \times z(i)}{x(i) \times 255^5} \right| \times 10^{16} \right\rfloor \bmod 256, \end{aligned} \tag{8}$$

where $i = 1$ to L.

Step 3. Decimal Diffusion Level 1

The following analytical equation is used to diffuse the pixels of P_1 using D_1 and previously diffused pixels;

$$I_1(i) = \begin{cases} (P_1(i) + d_1) \bmod 256, & \text{if } i = 1, \\ (P_1(i) + D_1(i) + I_1(i-1)) \bmod 256, & \text{if } 1 < i \leq L, \end{cases} \tag{9}$$

where d_1 is a seed value used to diffuse the first pixel of P_1.

Step 4. Block Scrambling Process

(i) First, divide I_1 into blocks, and the size of each block is $M_1 \times N_1$; then, the number of blocks is h, where $h = M \times N/M_1 \times N_1$.

(ii) Now, obtain a subsequence Q_1 of length h from the sequence, which is selected from the sequences $w_{1,}y, z, w_2x$ and generate the sequence Q_2 of random integers using the same procedure on Q_1, described in Step 2 (iv, v).

(iii) Q_2 is used to scramble the blocks of I_1 for n_1 times where n_1 indicates the number of scrambling rounds; after block scrambling of $I_{1,}$ transform the I_1 into a 1-dimensional array I_2.

Step 5. Decimal Diffusion Level 2

The pixels of I_2 is diffused using the sum of previously diffused pixels and D_2, with mathematical expression described as follows:

$$I_3(i) = \begin{cases} (I_2(i) + d_2) \bmod 256, & \text{if } i = L, \\ (I_2(i) + D_2(i) + sum(I_3(L - i\colon L))) \bmod 256, & \text{if } 1 \le i < L, \end{cases} \tag{10}$$

where d_2 is the seed value used to diffuse the first pixel of I_2.

Step 6. Pixels Scrambling Process

(i) Let T be a random integers sequence of length L, described in Step 2. (v).

(ii) T is used to scramble the pixels of I_3 for n_2 times where n_2 indicates the number of pixels scrambling rounds.

Step 7. Cipher Image

Transform the I_3 into matrix C of size $M \times N$. Figure 2 illustrates the encryption process.

Decryption is performed in the opposite direction as encryption.

4. Performance Evaluation

The performance of a presented cryptosystem is tested utilizing statistical and security analysis on distinct images such as Lena, Baboon, Pepper, Cameraman, and House. The parameters of the secret key are $x_0 = 0.23$, $y_0 = 0.25$, $z_0 = 0.25$, $w_{10} = 0.2$, $w_{20} = 0.01$, $u_1 = 3.8956$, $u_2 = 0.25678900$, $u_3 = 1.5$, $u_4 = 1.4$, $u_5 = 0.3$, $d_1 = 234$, $d_2 = 234$, $n_0 = 700$, $n = 1$, $n_1 = 1$, and $n_2 = 1$, and all experimental results are computed in MATLAB 2018b on a compatible computer with Windows 10, 8.00 GB RAM, and an Intel(R) Core(TM) i5-6300U CPU @ 2.5 GHz. Figure 3 demonstrates the encryption effect of our presented cryptosystem, and all experimental data are documented in tables, demonstrating that our cryptosystem's performance is outstanding against any security and statistical threats.

4.1. Key Space Analysis. The key space analysis helps us to decide whether or not our cryptosystem can withstand brute force attacks. The length of a key space is crucial to withstand a brute force assault because a prospective intruder would try every possible combination of key space to crack the cryptosystem. It is believed that if a cryptosystem's key space is larger than 2^{100}, it is robust. Let x_0, y_0, z_0, w_{10}, w_{20}, u_1, u_2, u_3, u_4, and u_5 be the secret key parameters, and each has a computational accuracy of 10^{-15}, and d_1, d_2, and d_3 are the positive integers used at diffusion level, and n_0 is the number of discarding iterations where $100 \le n_0 \le 1000$. Consequently, the length of the key size 9×10^{159} which is higher than 2^{100}, demonstrating that our presented encryption technique is resistant to brute force attacks. Table 1 shows the key space comparison to some existing encryption cryptosystems.

4.2. Histogram Analysis. Histogram analysis is the simplest and pictorial way to see the frequency distribution in plain and encrypted images. If the frequency distribution is uniform, then it is considered that the proposed encryption scheme is suitable for the secure transmission of data through the internet in daily use applications. In 8– bit grayscale image, the range of pixels value is 0 to 255. Histogram of plain and encrypted images (Lena, Baboon, Pepper, Cameraman, and House) can be seen in column (b, d) of Figure 3, and column (b) shows that the frequency distribution of pixels is not uniform. Still, on the other side, column (d) shows that the frequency distribution of pixels is uniform. The uniform distribution of pixels demonstrates that our proposed image encryption scheme can resist any statistical attack. A potential invader does not get any reliable information from the histogram of encrypted images.

4.3. Entropy. It is deemed that entropy is used to compute the uncertainty present in the source of information (digital image); if m is a source of information, the entropy of m can be computed described as follows:

$$\text{Entropy: } E(m) = \sum_{i=0}^{255} p(m_i)\log_2 \frac{1}{p(m_i)}, \tag{11}$$

where p(m_i) is a frequency of the symbol m_i, the entropy of a source of information m is 8 according to entropy formula, if the frequency of symbol m_i is uniformly distributed. The entropy of different encrypted images (Lena, Baboon, Pepper, Cameraman, and House) is nearly equal to 8, as shown in Table 2.

Sometimes global Shannon entropy does not measure the true randomness in the encrypted image; we estimate the local Shannon entropy [30] to overcome this drawback. In local Shannon entropy, the encrypted image divided into randomly selected K nonoverlapping blocks with T_B pixels

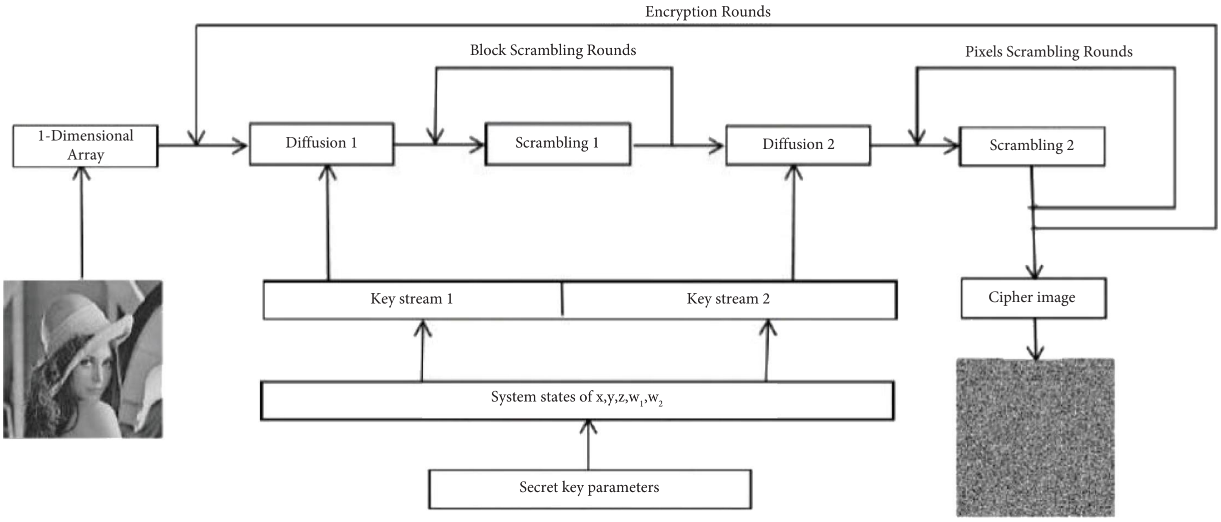


Figure 2: Visualization of the proposed cryptosystem.

in each block. Compute the entropy of each block using (11). Finally, compute the mean of all the block's entropy. The mathematical formula to calculate the local Shannon entropy is described as follows:

$$\overline{H_{K,T_B}}(I) = \sum_{i=1}^{K} \frac{E(i)}{K}. \tag{12}$$

The benchmark of local Shannon entropy is 7.90. It is evident from the Table 2 that our proposed encryption scheme can produce adequate randomness in an encrypted image that a potential invader cannot get any reliable information about the plain image.

4.4. *Chi-Square Analysis.*

Chi-square is a quantitative method of assessing pixel uniformity. Chi-square is a statistical technique that is described mathematically as follows:

$$\chi^2 = \sum_{i=1}^{2^8} \frac{(C_i - 256)^2}{256}, \tag{13}$$

where C_i indicates the actual frequency of i^{th} pixel, the range of pixels value is 0 to 255 because we are working on the 8-bit grayscale image. The numerical value $\chi^2_{(255,0.05)} = 293.2478$ for the level of significance 0.05. The distribution of pixels in encrypted images is highly uniform if the Chi-square score of the encrypted image is lower than 293.2478 as much as possible. The Chi-square score of distinct encrypted images (Lena, Baboon, Pepper, Cameraman, and House) is listed in Table 2, which proved that our proposed encryption scheme uniformly distribute the pixels value 0 to 255 in different rounds of encryption.

4.5. *Majority Logic Criteria (Texture Analysis of the Image).*

To evaluate the presented encryption scheme's efficiency on digital images, the MLC [31, 32] tool is utilized, which is a collection of five statistical tests such as correlation, contrast, entropy, energy, and homogeneity.

4.5.1. *Contrast.*

The brightness deterioration of plain images throughout the encryption process is calculated using contrast analysis. The better the encryption technology, the higher the contrast value. The numerical equation is as follows:

$$\text{Contrast: } C = \sum |i - j|^2 p(i, j), \tag{14}$$

where $p(i, j)$ indicates the grayscale co-occurrences matrix.

4.5.2. *Correlation.*

The range of correlation values is $[1, -1]$. In plain images, the correlation value of a pixel to its neighboring pixels is one or nearly equal to 1. The correlation value one or almost equal to 1 shows that the correlation of a pixel to its neighboring pixels is very strong. On the other hand, the correlation value 0 or negative shows that the correlation of a pixel to its neighboring pixels is weak. The purpose of any encryption scheme is to break the correlation of a pixel to its adjacent pixels. Mathematical equation which is used to measure correlation is described as follows:

$$\text{Pixels Correlation: } K = \sum_{i,j} \frac{(i - \mu i)(j - \mu j)}{\sigma_i \sigma_j} p(i, j), \tag{15}$$

where $p(i, j)$ indicates the grayscale co-occurrences matrix, we also find the correlation of a pixel to its adjacent pixels in the horizontal, vertical, and diagonal direction. The correlation of a pixel to its adjacent pixels is listed in Table 3 and the correlation of a pixel to its neighboring pixel in a horizontal, vertical, and diagonal direction of plain and encrypted images (Lena, Baboon, Pepper, Cameraman, and House) listed in Table 4. Figure 4 shows the correlation of plain and encrypted images of Lena in a horizontal, vertical, and diagonal direction. The experimented results of correlation demonstrate that the performance of the proposed encryption scheme is excellent and able to resist any attack.

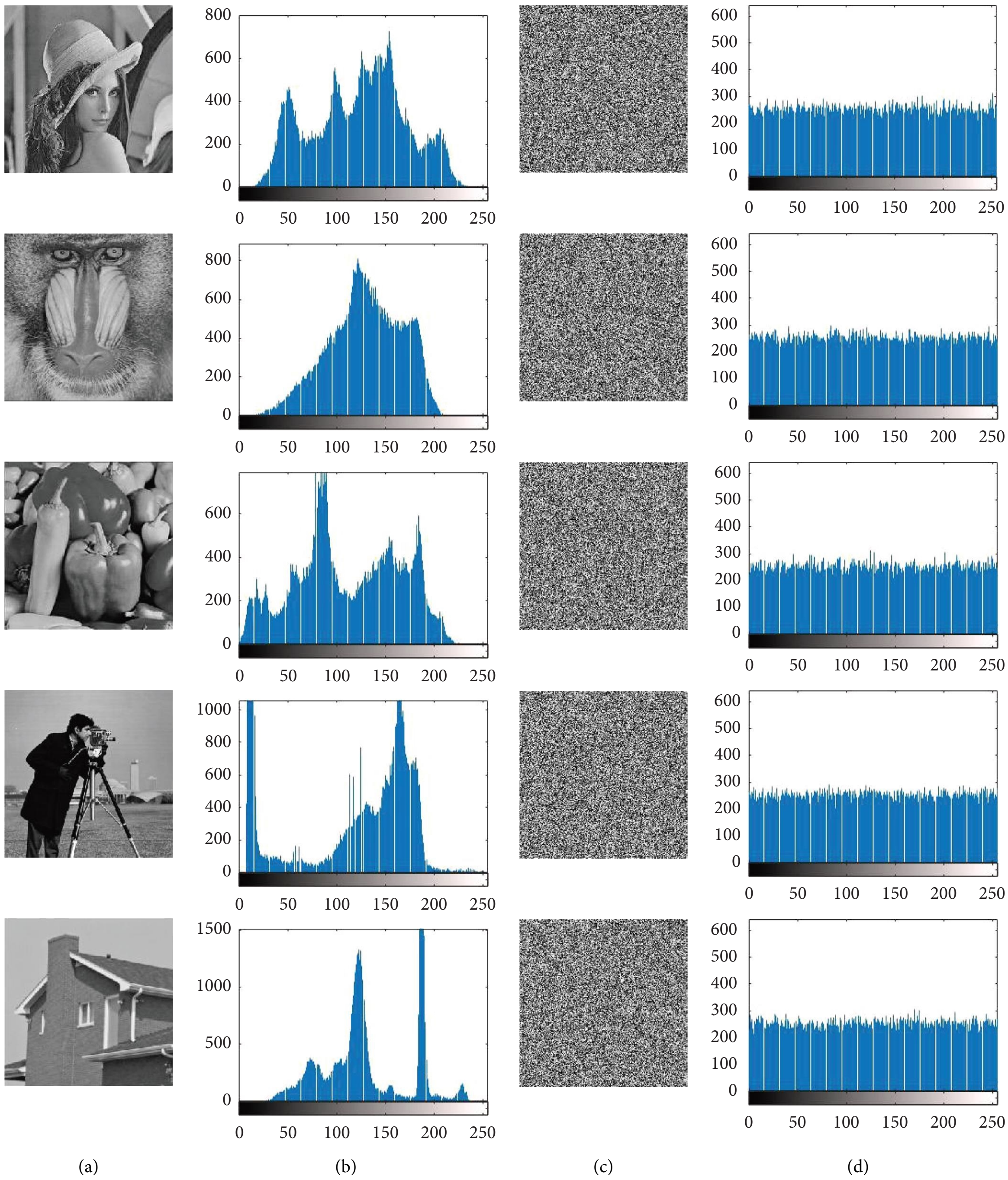


Figure 3: Histograms of plain and encrypted images. (a) the plain images; (b) the histograms of plain images; (c) the encrypted images; (d) the histograms of encrypted images.

Table 1: Key space comparison.

Schemes	Key space
Proposed	9×10^{159}
Reference [24]	10^{88}
Reference [25]	10^{60}
Reference [26]	2.4×10^{112}
Reference [27]	2.9645×10^{149}
Reference [28]	1.6777×10^{64}
Reference [29]	10^{70}

Table 2: Entropy, local entropy and Chi-square score of encrypted image of Lena, Baboon, Pepper, Cameraman, and House.

Images	Size	Entropy	Local entropy	Chi-square score
Lena	256 × 256	7.9969	7.9091	286.4766
Baboon	256 × 256	7.9976	7.9065	219.5625
Pepper	256 × 256	7.9976	7.9066	214.7813
Cameraman	256 × 256	7.9968	7.9069	291.6484
House	256 × 256	7.9972	7.9076	253.4357

Table 3: MLC score of the proposed cryptosystem for standard images.

Images	P/E	Contrast	Correlation	Energy	Homogeneity
Lena	Plain	0.5047	0.8918	0.1094	0.8525
	Encrypted	10.4180	0.0036	0.0156	0.3893
Baboon	Plain	0.4318	0.8495	0.1120	0.8193
	Encrypted	10.4939	−0.0004	0.0156	0.3906
Pepper	Plain	0.4868	0.9614	0.1061	0.8802
	Encrypted	10.4459	0.0036	0.0156	0.3915
Cameraman	Plain	0.5872	0.9227	0.1805	0.8953
	Encrypted	10.4980	0.0002	0.0156	0.3893
House	Plain	0.1863	0.9497	0.2029	0.9251
	Encrypted	10.5117	−0.0004	0.0156	0.3887
Average	Plain	0.4394	0.9150	0.1422	0.8745
	Encrypted	10.4735	0.0013	0.0156	0.3899

Table 4: Correlation coefficient results of plain and encrypted images of Lena, Baboon, Pepper, Cameraman, and House in the horizontal, vertical, and diagonal direction, respectively.

Images	Direction	Correlation	
		Plain image	Encrypted image
Lena	Horizontal	0.9907	0.0222
	Vertical	0.9380	0.0354
	Diagonal	0.9377	0.0006
Baboon	Horizontal	0.8341	0.0346
	Vertical	0.8989	0.0205
	Diagonal	0.8270	−0.0049
Pepper	Horizontal	0.9830	0.0017
	Vertical	0.9667	0.0222
	Diagonal	0.9511	0.0076
Cameraman	Horizontal	0.8842	0.0149
	Vertical	0.9201	0.0162
	Diagonal	0.8425	−0.0168
House	Horizontal	0.9218	−0.0312
	Vertical	0.9959	−0.0031
	Diagonal	0.9134	−0.0294

4.5.3. *Energy.*

To execute the energy analysis, we use a gray-level co-occurrence matrix. The numerical expression of energy is given as follows:

$$\text{Energy} = \sum_{i}\sum_{j} p(i,j)^{2}, \tag{16}$$

where $p(i,j)$ indicates the grayscale co-occurrences matrices.

4.5.4. *Homogeneity.*

Homogeneity analysis is used to compute the closeness of the grayscale level of co-occurrence matrices in (GLCM). The encryption method is deemed to be excellent if the homogeneity value is lower as much as possible. The mathematical expression of homogeneity is described as follows:

$$\text{Homogeneity} = \sum_{i}\sum_{j} \frac{p(i,j)}{1+|i-j|}, \tag{17}$$

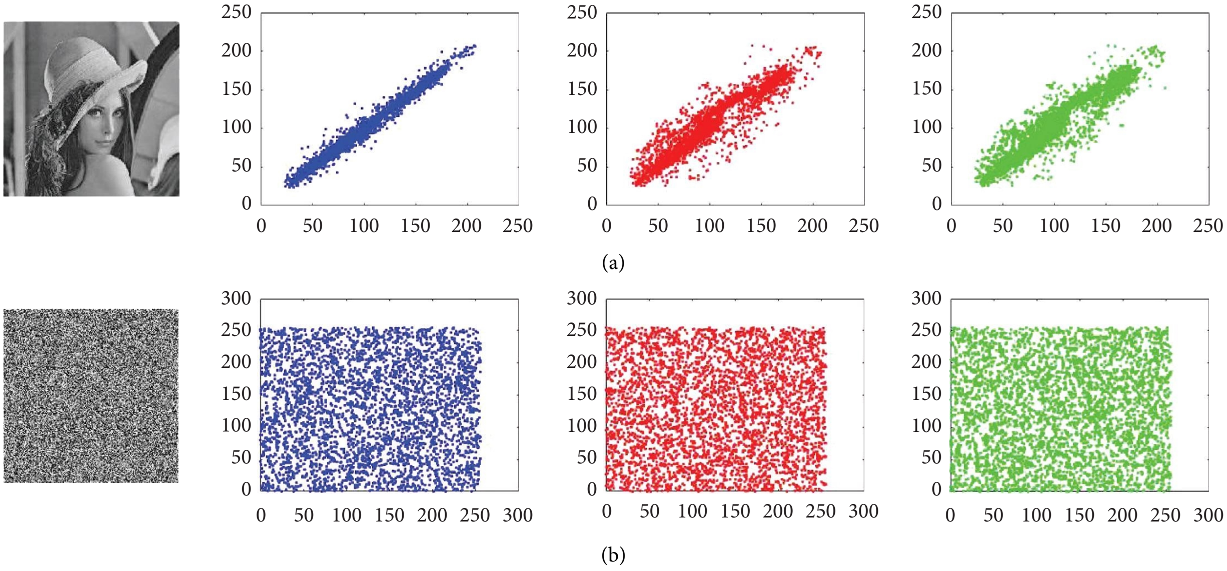
where $p(i,j)$ indicates the grayscale co-occurrences matrices.

The experimental MLC score of plain and encrypted images is listed in Table 3. MLC scores indicate that the encryption technique is excellent for digital images for secure transmission through the internet.

4.6. *MSE/MAD/PSNR/SSIM Analysis.*

A cryptosystem's encryption quality may be assessed using mean square error (MSE) and mean absolute difference (MAD) tests. MSE and MAD are mathematically expressed as follows:

$$\begin{aligned} \text{MSE} &= \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{M}\left(P(i,j)-C(i,j)\right)^{2}, \\ \text{MAD} &= \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{M}\left|P(i,j)-C(i,j)\right|, \end{aligned} \tag{18}$$



(a)

(b)

Figure 4: First and second row (left or right) represent the pictorial view of correlation coefficient in the direction of horizontal, vertical, and diagonal of plain and encrypted images of lena respectively.

where M and N indicate the dimensions of plain image P and encrypted image C, the cryptosystem is deemed efficient and secure if MSE and MAD values are higher.

The peak signal to noise ratio (PSNR) is inversely proportional to the square root of MSE, as seen in equation (19). The PSNR value should be as low as feasible for the best encryption quality. The PSNR is calculated using the following mathematical formula:

$$\text{PSNR} = 20\log_{10}\left(255/\sqrt{\text{MSE}}\right)dB. \tag{19}$$

The structural similarity index measurement (SSIM) evaluates how much an encrypted image deteriorates throughout the encryption process. The SSIM mathematical equation is as follows:

$$\text{SSIM} = \frac{\left(2\mu_P\mu_E + \alpha\right)\left(2\sigma_{PE} + \beta\right)}{\left(\mu_P^2 + \mu_E^2 + \alpha\right)\left(\sigma_P^2 + \sigma_E^2 + \beta\right)}, \tag{20}$$

where μ_P and μ_E are the average pixel values and σ_P, and σ_E are the variance of corresponding images P and E. Also, σ_{PE} represents the covariance between P and E, and α and β are two predetermined constants used to ensure stability. The MSE, MAD, PSNR, and SSIM experimental findings are presented in Table 5, and the experimental results show that the proposed cryptosystem can withstand any statistical attack.

4.7. Data Loss Attack Analysis.

A data loss attack means a potential invader artificially dethrones the pixels of a particular area of an encrypted image or loses some portion of the image during transmission through the internet. A cryptosystem is immaculate if it convalesces the critical information from the encrypted image, which loses the data. It is clear from Figure 5 that our proposed cryptosystem can retrieve helpful information from the encrypted images which lose data during communication. In Figure 5, a_1 to a_5 the figures which lose a block of data size 32 × 32 to demonstrate the data loss attack and a_6 lose data from all sides, and b_1 to b_6 represent the figures after performing the decryption process on the figures which lose data respectively.

Table 5: MAD, MSE, SSIM, and PSNR scores of the proposed encryption algorithm.

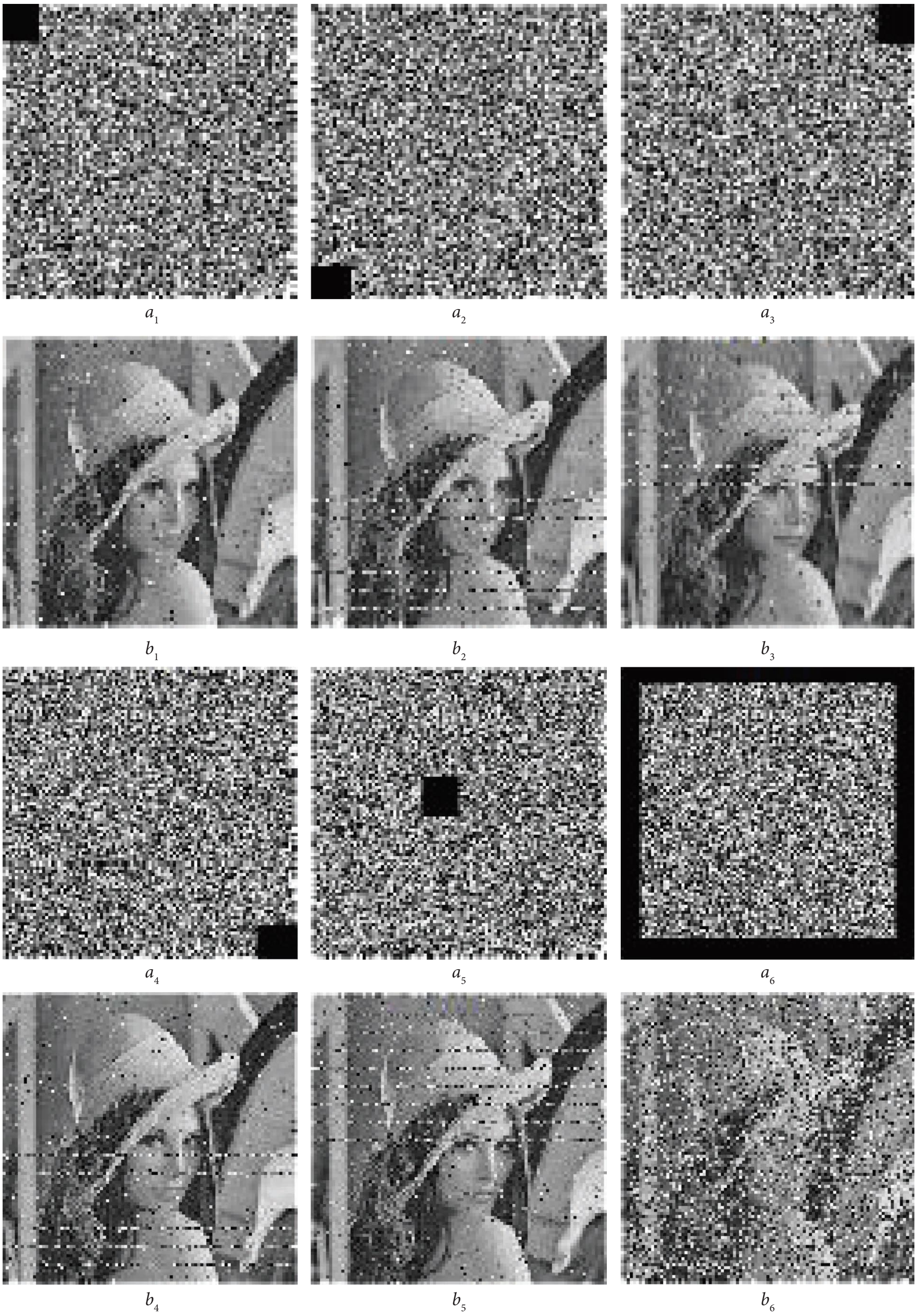
Images	MAD	MSE	SSIM	PSNR
Lena	73.0485	7782	−0.0012	9.2198
Baboon	73.2823	7833	−0.0015	9.1916
Pepper	73.1300	7780	0.0013	9.2210
Cameraman	73.1966	7796	0.000828	9.2118
House	73.0063	7792	−0.0015	9.2145
Average	73.1327	7797	0.0011	9.2117

4.8. Noise Attack Analysis.

Normally, images possess information, but during the transmission, the image is polluted with some noise. The appearance of noise will annihilate the original information from the image. The pepper and salt noise effect on our encryption algorithm is examined in this paper on Lena's image, and different salt and pepper noise ratios represent the attack intensity. In Figure 6, we use the pepper and salt noise ratios 0.01, 0.03, 0.05 on the figure a_1, a_2, and a_3, respectively. The decryption process are employed on the a_1, a_2, and a_3 and as a result get figures b_1, b_2, and b_3, respectively. Figure 6 demonstrates that our proposed system is flawless for dealing with polluted images and retrieving important information as much as possible.

4.9. Differential Attacks.

The two main criteria for evaluating the robustness [33] of a cryptosystem against a slight change in any pixel or secret key parameter are NPCR (number of



a_1 a_2 a_3

b_1 b_2 b_3

a_4 a_5 a_6

b_4 b_5 b_6

Figure 5: Analysis of data loss attack.

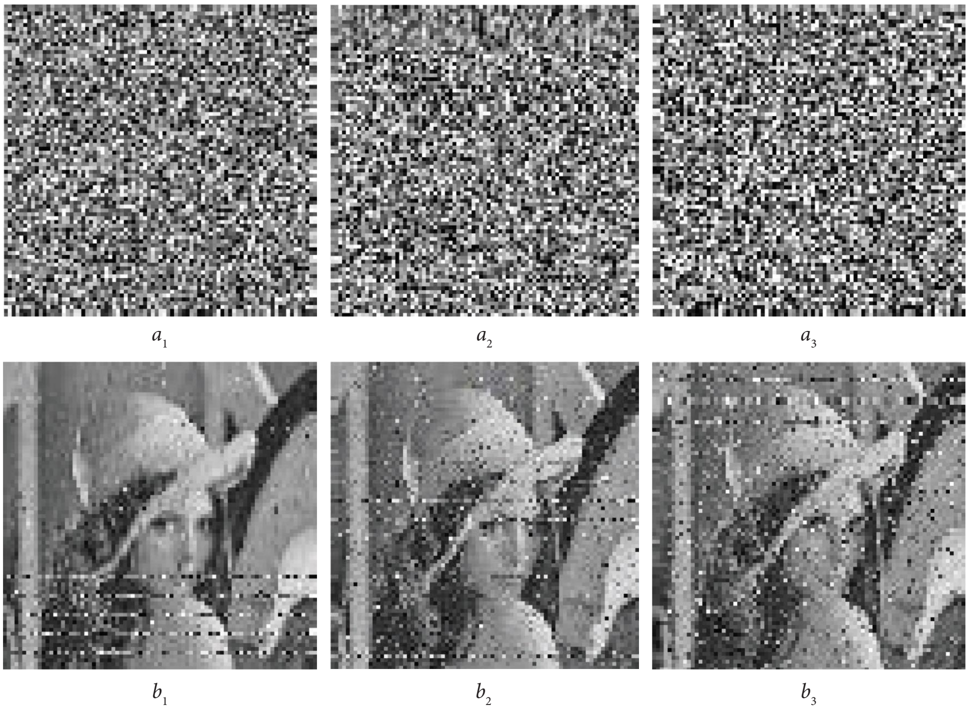


Figure 6: Analysis of noise attack.

pixel changing rate) and UACI (unified averaged changed intensity). The mathematical equations for NPCR and UACI are as follows:

$$\mathrm{NPCR}\left(E_1, E_2\right) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D\left(i, j\right) = \begin{cases} 1 & \text{if } E_1\left(i, j\right) \neq E_2\left(i, j\right) \\ 0 & \text{if } E_1\left(i, j\right) = E_2\left(i, j\right) \end{cases}}{M \times N} \times 100\%, \tag{21}$$

$$\mathrm{UACI}\left(E_1, E_2\right) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left|E_1\left(i, j\right) - E_2\left(i, j\right)\right|}{255} \times 100\%, \tag{22}$$

where M and N are the dimensions of an image, also E_1 and E_2 are two encrypted images corresponding to plain images differ by single pixel. Benchmark values of the NPCR and UACI for different sizes of images are listed in Table 6.

4.10. Plaintext Sensitivity Analysis. A cryptosystem is plaintext sensitive if a slight change in randomly selected pixel of plain image will produce a different encrypted image; that encrypted image does not provide any important clue about plain image. Method to test the plaintext sensitivity, let P_1 and P_2 be two plain images; all the pixels of P_1 and P_2 are the same except one randomly selected pixel. The original key is used to encrypt the plain images P_1 and P_2, get two encrypted images E_1 and E_2, respectively. NPCR and UACI between two encrypted images E_1 and E_2, are computed using equations (21) and (22). A cryptosystem is sensitive to plaintext if the value of NPCR > 99% and UACI is greater or closer to 33%. The procedure, as mentioned earlier of plaintext sensitivity employed on the image (Lena, Baboon, Pepper, Cameraman, and House) and compute the NPCR and UACI score, is listed in Table 7. The plaintext sensitivity score of different images demonstrates that our cryptosystem can resist any differential attack.

4.11. Key Sensitivity Analysis. The cryptosystem is regarded as extremely key sensitive; if the encrypted image acquired after a subtle change in any of the secret key parameters provided in Table 8 is distinctive from the encrypted image generated without any change in secret key parameters. To test the key sensitivity, first, encrypt plain image P using the original secret key parameters listed in Table 8, then encrypt the same plain image using a minor modification of 10^{-15} in any secret key parameter, yielding two encrypted images E_1 and E_2. NPCR and UACI are computed between to

Table 6: Benchmark values of NPCR and UACI.

Test/size of images	256 × 256	512 × 512	1024 × 1024
NPCR	99.5954	99.5893	99.5954
UACI	[33.2824, 33.6447]	[33.3730, 33.5541]	[33.4183, 33.5088]

Table 7: Results of and after a slight change in randomly selected pixel $P(x, y)$ of Lena, Baboon, Pepper, Cameraman, and House.

Images	Size	NPCR (%)	UACI (%)	Randomly selected pixel
Lena	256 × 256	99.6460	33.4271	$P_{(1,1)}$
Baboon	256 × 256	99.6426	33.4309	$P_{(256,256)}$
Pepper	256 × 256	99.6475	33.4078	$P_{(167,233)}$
Cameraman	256 × 256	99.6521	33.4538	$P_{(217,17)}$
House	256 × 256	99.6353	33.3731	$P_{(128,128)}$

Table 8: Results of NPCR and UACI after a minor change in any parameter of secret key.

Parameters	Change in parameter	NPCR (%)	UACI (%)
x_0	$x_0 + 10^{-15}$	99.6048	33.4169
y_0	$y_0 + 10^{-15}$	99.6124	33.3899
z_0	$z_o + 10^{-15}$	99.6613	33.3942
w_{10}	$w_{10} + 10^{-15}$	99.5941	33.3327
w_{20}	$w_{20} + 10^{-15}$	99.5911	33.5274
u_1	$u_1 + 10^{-15}$	99.5834	33.2567
u_2	$u_2 + 10^{-15}$	99.5728	33.3396
u_3	$u_3 + 10^{-15}$	99.6155	33.6749
u_4	$u_4 + 10^{-15}$	99.6094	33.6089
u_5	$u_5 + 10^{-15}$	99.5911	33.5005
n_0	$100 \leq n_0 \leq 1000$	99.5956	33.3028

encrypted images E_1 and E_2 using the equations (21) and (22). We performed a key sensitivity analysis on the Lena image by making minor changes to each secret key parameter one at a time. The resulting NPCR and UACI scores are shown in Table 8, indicating that our proposed cryptosystem is extremely key sensitive and resistant to differential attacks.

4.12. Randomness Test for Cipher. Our proposed cryptosystem creates enough randomness in the pixel of encrypted images; a potential invader can never acquire reliable information about the plain image. The Nist test in [34] is used to check the randomness present in the pixels of encrypted images. The Table 9 exhibits the two Nist test results, which confirm that the security of our proposed cryptosystem is excellent to resist any attack.

Table 9: Nist test analysis for distinct encrypted images.

Images/tests	Frequency	Runs	Rank
P_value for Lena	0.8265	0.3085	0.0852
P_value for Baboon	0.9761	0.4672	0.0852
P_value for Pepper	0.8420	0.1909	0.0852
P_value for Cameraman	0.2991	0.2048	0.0852
P_value for House	0.6390	0.4285	0.0852

4.13. Speed Analysis. The speed and security of any encryption scheme are the key characteristics in the application of real life. The analysis, as mentioned earlier, exhibits that the security of our proposed encryption scheme is immaculate. We test the speed of our encryption scheme in MATLAB 2018b on a compatible computer with Windows 10, 8.00 GB RAM, and an Intel(R) Core(TM) i5-6300U CPU @ 2.5 GHz. Table 10 shows the speed analysis of our proposed scheme with other encryption schemes developed using multidimensional chaotic maps. The speed analysis confirmed that our encryption scheme is unassailable and efficient. Also, the statistical test results of the baboon image are compared in Table 11 with the existing encryption scheme.

Table 10: Speed of distinct encryption schemes in seconds.

Images	Size	Proposed	[3]
Lena	256 × 256	3.222	3.350
Baboon	256 × 256	3.259	3.504
Pepper	256 × 256	3.316	3.079
Cameraman	256 × 256	3.319	3.371
House	256 × 256	3.284	3.624

Table 11: Comparison of statistical test of baboon image.

Comparison	Entropy	Chi-square	NPCR	UACI
Proposed	7.9976	219.5625	99.6426	33.4309
[16]	7.9969	229.73	99.6048	33.5547
[29]	7.9974	247.98	–	–

5. Conclusion

The novelty of this paper is to generate a unique key stream and scrambling process (blocks of plain image and pixels of plain images) using different chaotic maps, which is further utilized to propose a cryptosystem for the security of digital images during transmission from a potential invader. The aforementioned cryptosystem is employed on the standard grayscale images to see its effectiveness. The simulations and results of the experimental analysis demonstrate that the presented cryptosystem is exceptional in preserving high security and privacy requirements. We can confidently assert that the presented scheme is ideally suited to multimedia communications and online systems.

Data Availability

The data used to support the study are included in the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] 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.

[2] Z. Bashir, T. Rashid, and S. Zafar, "Hyperchaotic dynamical system based image encryption scheme with time-varying delays," *Pacific Science Review A:Natural Science and Engineering*, vol. 18, no. 3, pp. 254–260, 2016.

[3] Z. Bashir, J. Wątróbski, T. Rashid, S. Zafar, and W. Sałabun, "Chaotic dynamical state variables selection procedure based image encryption scheme," *Symmetry*, vol. 9, no. 12, p. 312, 2017.

[4] E. Tromer, D. A. Osvik, and A. Shamir, "Efficient cache attacks on AES, and countermeasures," *Journal of Cryptology*, vol. 23, no. 1, pp. 37–71, 2010.

[5] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and advanced encryption system," *Signal Processing*, vol. 141, pp. 217–227, 2017.

[6] L. Y. Zhang, Y. Liu, F. Pareschi et al., "On the security of a class of diffusion mechanisms for image encryption," *IEEE Transactions on Cybernetics*, vol. 48, no. 4, pp. 1163–1175, 2018.

[7] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Communications in Nonlinear Science and Numerical Simulation*, vol. 60, pp. 12–32, 2018.

[8] 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.

[9] R. A. Elmanfaloty and E. Abou-Bakr, "An image encryption scheme using a 1D chaotic double section skew tent map," *Complexity*, vol. 2020, Article ID 7647421, 18 pages, 2020.

[10] L. Moysis, C. Volos, S. Jafari et al., "Modification of the logistic map using fuzzy numbers with application to pseudorandom number generation and image encryption," *Entropy*, vol. 22, no. 4, p. 474, 2020.

[11] 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.

[12] S. Zhu and C. Zhu, "Secure image encryption algorithm based on hyperchaos and dynamic DNA coding," *Entropy*, vol. 22, no. 7, p. 772, 2020.

[13] Z. Hua, Z. Zhu, Y. Chen, and Y. Li, "Color image encryption using orthogonal Latin squares and a new 2D chaotic system," *Nonlinear Dynamics*, vol. 104, no. 4, pp. 4505–4522, 2021.

[14] Z. Hua, Y. Chen, H. Bao, and Y. Zhou, "Two-dimensional parametric polynomial chaotic system," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 7, pp. 4402–4414, 2022.

[15] P. He, K. Sun, and C. Zhu, "A novel image encryption algorithm based on the delayed maps and permutation-confusion-diffusion architecture," *Security and Communication Networks*, 2021.

[16] B. Idrees, S. Zafar, T. Rashid, and W. Gao, "Image encryption algorithm using S-box and dynamic Henon bit level permutation," *Multimedia Tools and Applications*, vol. 79, no. 9-10, pp. 6135–6162, 2020.

[17] M. G. A. Malik, Z. Bashir, N. Iqbal, and M. A. Imtiaz, "Color image encryption algorithm based on hyper-chaos and DNA computing," *IEEE Access*, vol. 8, Article ID 88093, 2020.

[18] D. S. Malik and T. Shah, "Color multiple image encryption scheme based on 3Dchaotic maps," *Mathematics and Computers in Simulation*, vol. 178, pp. 646–666, 2020.

[19] Z. Hua, J. Li, Y. Chen, and S. Yi, "Design and application of an S-box using complete Latin square," *Nonlinear Dynamics*, vol. 104, no. 1, pp. 807–825, 2021.

[20] Z. Hua, K. Zhang, Y. Li, and Y. Zhou, "Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing," *Signal Processing*, vol. 183, Article ID 107998, 2021.

[21] D. Fang and S. Sun, "A new secure image encryption algorithm based on a 5D hyperchaotic map," *PLoS One*, vol. 15, no. 11, Article ID e0242110, 2020.

[22] X. Wang and C. Jin, "Image encryption using game of life permutation and PWLCM chaotic system," *Optics Communications*, vol. 285, no. 4, pp. 412–417, 2012.

[23] M. Hénon, "A two-dimensional mapping with a strange attractor," in *The Theory of Chaotic Attractors*, vol. 50, pp. 69–77, Springer, New York, NY, USA, 1976.

[24] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Processing*, vol. 148, pp. 272–287, 2018.

[25] J. Chen, Z. L. Zhu, L. B. Zhang, Y. Zhang, and B. Q. Yang, "Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption," *Signal Processing*, vol. 142, pp. 340–353, 2018.

[26] X. Liao, X. Liao, M. A. Hahsmi, and R. Haider, "An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos," *Optik-International Journal for Light and Electron Optics*, vol. 153, pp. 117–134, 2018.

[27] X. Wang, Y. Wang, X. Zhu, and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level," *Optics and Lasers in Engineering*, vol. 125, Article ID 105851, 2020.

[28] H. G. Mohamed, D. H. ElKamchouchi, and K. H. Moussa, "A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences," *Entropy*, vol. 22, no. 2, p. 158, 2020.

[29] Y. Niu, Z. Zhou, and X. Zhang, "An image encryption approach based on chaotic maps and genetic operations," *Multimedia Tools and Applications*, vol. 79, no. 35-36, Article ID 25613, 2020.

[30] 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.

[31] N. Bibi, S. Farwa, N. Muhammad, A. Jahngir, and M. Usman, "Correction: a novel encryption scheme for high-contrast image data in the Fresnelet domain," *PLoS One*, vol. 13, no. 11, Article ID e0208305, 2018.

[32] S. Farwa, N. Bibi, and N. Muhammad, "An efficient image encryption scheme using Fresnelet transform and elliptic curve based scrambling," *Multimedia Tools and Applications*, vol. 79, no. 37-38, Article ID 28225, 2020.

[33] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption, Cyber journals: multidisciplinary journals in science and technology," *Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.

[34] J. K. M. S. Zaman and R. Ghosh, "Review on fifteen statistical tests proposed by NIST," *Journal of Theoretical Physics and Cryptography*, vol. 1, pp. 18–31, 2012.