Hindawi
Complexity
Volume 2020, Article ID 9597619, 23 pages
https://doi.org/10.1155/2020/9597619

Research Article

A New Image Encryption Scheme Based on Hybrid Chaotic Maps

Ibrahim Yasser,[1] **Fahmi Khalifa**,[2] **Mohamed A. Mohamed**,[2] **and Ahmed S. Samrah**[2]

[1]*Communication and Electronics Engineering Department, Nile Higher Institute for Engineering and Technology, Mansoura, Egypt*
[2]*Electronics and Communications Engineering Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt*

Correspondence should be addressed to Ibrahim Yasser; ibrahimyasser14@gmail.com

Received 29 February 2020; Revised 8 May 2020; Accepted 19 May 2020; Published 25 July 2020

Academic Editor: Oveis Abedinia

Chaos-based encryption algorithms offer many advantages over conventional cryptographic algorithms, such as speed, high security, affordable overheads for computation, and procedure power. In this paper, we propose a novel perturbation algorithm for data encryption based on double chaotic systems. A new image encryption algorithm based on the proposed chaotic maps is introduced. The proposed chaotification method is a hybrid technique that parallels and combines the chaotic maps. It is based on combination between Discrete Wavelet Transform (DWT) to decompose the original image into sub-bands and both permutation and diffusion properties are attained using the chaotic states and parameters of the proposed maps, which are then concerned in shuffling of pixel and operations of substitution, respectively. Security, statistical test analyses, and comparison with other techniques indicate that the proposed algorithm has promising effect and it can resist several common attacks. Namely, the average values for UACI and NPCR metrics were 33.6248% and 99.6472%, respectively. Additionally, unscrambling quality can fulfill security and execution prerequisites as evidenced by PSNR (9.005955) and entropy (7.999275) values. In sum, the proposed method has enough ability to achieve low residual intelligibility with high quality recovered data, high sensitivity, and high security performance compared to some other recent literature approaches.

1. Introduction

With the fast development of innovations in data communication, it can end up crucial for private information security from prohibitive actions or attackers. Data exchange is closely related to existence, such as instruction, commerce, financial matters, military, e-learning, phone keeping money, and news telecasting. With the modern telecommunication and multimedia technologies progression, a huge amount of critical information voyages in a daily monotony through the shared and open networks. In order to keep security, sensitive and critical information ought to be secured before conveyance [1]. For data transmitting through any uncertain channel, certain cryptograph techniques are required to change over the coherent information to incomprehensible form before transmitting (encryption). The modern strategies of cryptography are effective for text information. However, due to the high redundancy and bulk information capacity, they fail to provide computational security.

Chaos-based encryption is one of the foremost important security technologies within the advanced encryption zone. Chaos hypothesis is created by mathematicians and physicists. Chaos hypothesis has qualified features as nonlinearity, deterministically, abnormality, and affectability to beginning conditions. Security investigative community receives chaos hypothesis in modern cryptography. A function that has some kind of chaotic behavior is defined as a work or a chaotic map. Within the following we discuss numerous sorts of proposed chaotic maps that are utilized in this paper. To apply a chaos map, there are two ways in a cipher system: (i) produce pseudorandom stream utilizing chaotic maps, and (ii) utilize the plain or secret key(s) as control parameters and the introductory conditions [2]. Finally, apply a few emphases on chaotic systems to get cipher data. The first way compares to stream cipher and the second to block ciphers. The implementation of chaotic maps within the improvement of cryptography systems lies within the truth that a chaotic outline is characterized by (i)

the beginning conditions and control parameters with high sensitivity, (ii) unpredictability of the orbital advancement, and (iii) the straight forwardness of the hardware and software execution that leads to a high encryption rate [3]. The techniques focused on chaos are considered effective in managing with voluminous, excess information. They give quick, profoundly secure strategies of encryption. In literature, various research works have exploited chaotic maps for data encryption. For example, Zahmoul et al. [4] presented a beta chaotic map for producing distinctive groupings in replacement, diffusion, and exchange. Their system viably moves forward the encryption security. Yavuz et al. [5] approached autonomous chaotic function framework to adequately apply diffusion principles and confusion. Differential assaults extended the cryptosystem resistance; it moreover requires extra circular turn operations and exclusive-or on the scrambled image pixel values. Zhang [6] utilized S-box and the piecewise liner chaotic outline to produce key stream with great factual for image encryption. The presented cryptosystem had undefined encryption get ready and decryption. It contains a key with large space and quick speed for encryption, but still contains a lot of correlation for the ultimate encrypted image. Aqeel-ur-Rehman et al. [7] suggested encryption image algorithm and hyperchaotic framework related to the initial image used for creating the key stream. Due to small key space, it easily is joined to that complex scheme. Song et al. [8] presented a modern framework using the defining of the neighborhood nonlinear map within the Coupled Map Lattices (CML). The outline was connected to the instrument of permutation-diffusion. The encryption scheme chaos considered that the merits of spatiotemporal chaos and the Nonlinear Chaotic Algorithm (NCA) is a great execution and has profoundly eccentric chaotic sequences. Wang et al. [9] proposed an image encryption algorithm with combined permutation and diffusion stages. Due to its little key space, the algorithm is still not secure. Parvaz and Zarebnia [10] characterized a chaotic framework based on calculated sine, and tent framework. Though the encryption conspire is not palatable, they demonstrated that the encryption is secure. Wu et al. [11] presented a Two-Dimensional Hénon-Sine Map (2D-HSM) that has higher characteristics. Slimane et al. [12, 13] presented an effective scheme for image encryption dependent on the settled nested chaotic map and Deoxyribonucleic Acid (DNA) utilizing The Secure Hash Algorithm (SHA-256) to produce the initial states of the chaotic attractor, and introduced a new chaotic system dependent on Julia's fractal procedure, tumultuous attractors, and logistic map in a complex set.

The assessment of literature work finds that some chaos-based image encryption algorithms have security vulnerabilities, including (i) standing up to chosen-plaintext attack; (ii) sensitivity to all the chaotic secret keys; (iii) decoding of primary pixel within the decryption process; and (iv) reversing rectangular transform system. To outdo the above-mentioned shortcomings and security defect, we propose an improved encryption algorithm utilizing two-dimensional alteration models. The main objective of our work is to propose a data encryption system with key sensitivity, low residual clarity, and keeping up great quality of information reproduced by chaotic maps. Security analysis and experimental results suggest that proposed map could encrypt digital images with powerful capability and high security to resist different attacks.

The remainder of this paper is organized as follows. Within the next section, the proposed chaotic systems details are fully explained. The proposed encryption and decryption frameworks are presented in Section 3. In Section 4, the quantitative measurements for system evaluation are presented. Section 5 presents the test results for the proposed cryptosystem. Finally, the concluding comments and recommended future avenues are given in Section 6.

2. The Proposed Chaotic Systems

We propose a novel chaotic system for improving encryption quality and execution, which is described below. Our system is a Two-Dimensional (2D), nonlinear, discrete-time technique that provides dynamical chaotic behavior. Due to the nonrepeatability and ergodicity of chaos in these algorithms, they can accomplish general searches at higher speeds than stochastic searches that depend on probabilities [14]. The proposed chaotic maps are used to create the chaotic sequence; it derives from the model of Chirikov standard map. Classical chaotic maps suffer from low control parameters which in turn lead to a limited chaotic range, but the better dimensional as the proposed chaotic maps can be used to increase the key space and excessive complexity and complement the randomness of pseudo sequence. To create such maps a chaotic pseudo code is employed and is described in Algorithm 1. Among the diverse proposed maps, four are examined and their characteristics are analyzed below. In short, the new chaotic maps have desirable characteristics such as a large phase space, high ergodicity, and high sensitivity to slight changes in initial conditions and/or control parameters. These characteristics are analogous to the requirements of encryption algorithms. In addition, these maps preserve the original structure of the classical maps in terms of their parameter range.

The first proposed chaotic map can be considered as 2D growth of the traditional logistic map. It has a mathematical expression similar to Hénon map. The modified map gives a thought of chaotic nature which is given by condition (1). In this, original position (x_n, y_n) can be mapped to a new position (x_{1+n}, y_{1+n}) using the following:

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

where the state variables x and y are the simulated time series, a, b, and r represent the external parameters of control, and n is an iteration number using this map. The graph of this map is obtained in Figure 1(a).

The second proposed chaotic map that is utilized in our technique is a new finance model. It is a discrete-time dynamical system that exhibits chaotic behavior. It takes a

//Chaotic proposed algorithm
Begin
(1) It could be a system of a discrete time that maps point (x_n, y_n).
(2) Define the initial value of maximum number of iterations t Max, upper boundary, and lower bound, population size n, number of dimensions dim and define the fitness function.
(3) Randomly initialize the positions of map.
(4) Begin iteration (n).
(5) Select one of the four proposed finance dynamical models.
(6) End for
End

Algorithm 1: Proposed chaotic pseudo code.

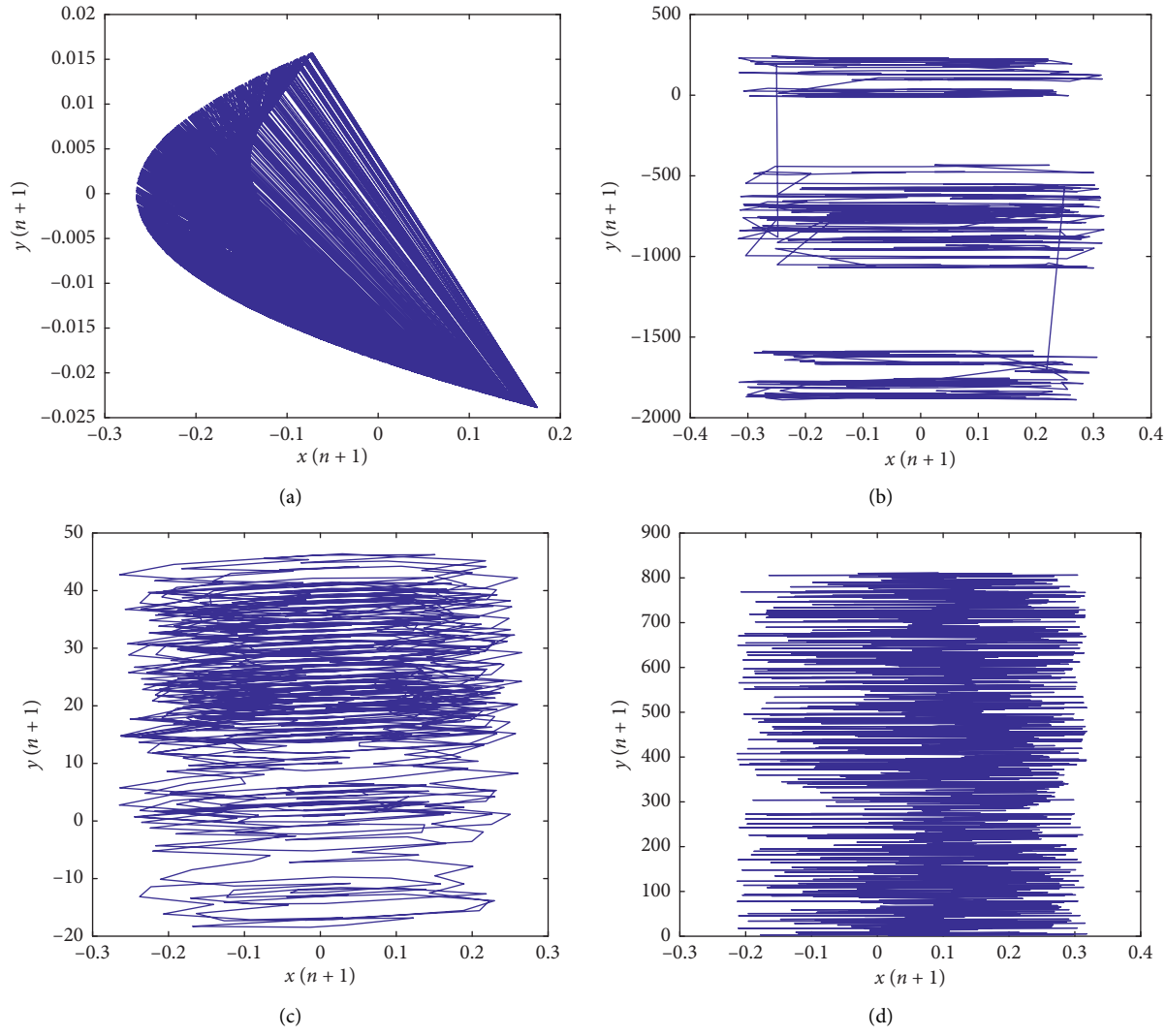


Figure 1: Numerical simulation of the 2D phase plot in (x, y) plane of the modern finance model defined by (a) equation (1), where $a = 1.4$ and $b = 0.3$; (b) equation (2); (c) equation (3); and (d) equation (4) where $a = 1.5$.

point (x_n, y_n) in the plane and maps it to a new point given by

$$\begin{cases} y_{n+1} = y_n - r.\tan x_n, \\ x_{n+1} = \sin x_n + \sin y_{n+1}. \end{cases} \quad (2)$$

The above set of equations is a dynamical nonlinear system with 2D nonlinearities. Within the finance dynamical illustration, the state factors x and y are the simulated time series, r acts the external control parameter, and n is an iteration number. The bifurcation diagrams with different parameters could be utilized to examine the distribution

property of the chaotic series. It could be certain that the proposed map possesses excellent chaotic property in terms of uniform distribution and has relatively large parametric space, which can be suitable for the field of image encryption. The graph of this map is demonstrated in Figure 1(b).

The third proposed chaotic map utilized in our pipeline is a 2D chaos map that includes generation of a permuted image which includes the change within the position of the pixel in unique image to some new position utilizing the taking after the following condition:

$$\begin{cases} y_{1+n} = y_n - r \tanh x_n, \\ x_{1+n} = \tanh x_n + \sin y_{n+1}, \end{cases} \tag{3}$$

where n is an iteration number using this map, the chaotic time, the state variables x and y are the simulated time series, and r represents the chaotic parameter. The graph of this map is observed in Figure 1(c).

Finally, the fourth proposed chaotic map that is introduced is obtained using the iterative function introduced by

$$\begin{cases} y_{1+n} = y_n + a \,.\, r \cos x_n, \\ x_{1+n} = \cos x_n + \sin y_{n+1}, \end{cases} \tag{4}$$

where the deterministic chaotic time series are produced in the interval $x_n, y_n \epsilon [0, 1]$, a and r speak to the external parameters control, and n is the number of the recreated focuses. The graph of this map is obtained in Figure 1(d).

The proposed characteristic types of the modern finance models are obtained using MATLAB for the financial parameters, e.g., initial state values as $x_{(0)} = 0.02$ and $y_{(0)} = 0.02$. The dynamics of chaotic map are indicated by orbits. The chaotic map orbit is characterized by a discontinuous motion, nonsmooth. The structures of the proposed chaotic maps are demonstrated. As can be readily seen from the figure, each chaotic system has its extraordinary signature, which could be a special attractor characteristic. The balance focuses of the other proposed chaotic system are gotten by fathoming the following pseudo code in Algorithm 1.

2.1. Chaotic Behavior Evaluation of the Proposed Maps. Chaotic performance can be evaluated using different techniques such as Lyapunov exponent, bifurcation, and trajectory. A quick overview of those methods are given below; then evaluation of the chaotic behavior for the proposed maps based on their bifurcation diagram, iteration function diagram, and Lyapunov exponent are detailed in the next section.

Lyapunov exponent represents the highlights of a disordered framework and can generally communicate the general execution of chaotic maps. It is utilized as a quantitative measure for the sensitive reliance on initial conditions. For a discrete system $x_{n+1} = f(x_n)$ and for an orbit beginning with x_0, the Lyapunov exponent can be described as follows [15]:

$$\lambda(x_0) = \lim_{n \longrightarrow \infty} \frac{1}{n} \sum_{i=1}^{\infty} \ln |f\prime(xi)|, \tag{5}$$

where f' is the subordinate of the capacity f. In the event that λ is negative, the framework is not clamorous. On the off chance that λ is zero, this implies the framework is impartially steady and is in consistent state mode. In the event that λ is certain, the advancement is touchy to introductory conditions and thusly disorganized. Additionally, it is not unexpected to allude to the Maximal Lyapunov Exponent (MLE), in light of the fact that it decides a thought of consistency for a riotous framework. The bigger MLE is, the more tumultuous the guide is and the less the quantity of cycles important to accomplish the necessary level of dissemination or disarray of data is, and this implies a superior clamorous guide. On the other hand, bifurcation diagram is normally alluded to as the subjective progress from ordinary to riotous conduct by changing the control parameter. The bifurcation outline is utilized to consider the clamorous framework as a component of the estimations of the control parameters. This chart permits knowing the districts of the framework showing intermingling, bifurcation, and bedlam relying upon the estimations of the control parameters [16]. At long last, iteration property plots the connection between the quantity of cycles n and the quadratic disorganized guide at various estimations of the disordered parameter r and at a particular introductory worth x_0 [17]. The parameter r can be partitioned into three areas, which can be analyzed by recreation utilizing MATLAB.

2.2. Analysis of the Proposed Chaotic Maps. Quadratic map is a fundamental case of a disorderly framework. It might give the well-known and broadly utilized One-Dimensional (1D) disordered logistic map which is portrayed by scientific iterative [18]:

$$x_{n+1} = r x_n (1 - x_n), \tag{6}$$

where r is the clamorous parameter and n is the quantity of iterations. The arrangement of the quadratic guide is riotous, in light of the fact that it is nonlinear. It is deterministic since it has a condition that decides the conduct of the framework. Likewise, a slight difference in the underlying worth x_o can prompt an altogether unique conduct of the guide. We can gather from Figure 2 that logistic map in general has a positive LE and scattered appropriation just for $3.57 \leq r \leq 4$. As featured in [19] the logistic guide has negative marks, for example, (i) low riotous range for control parameter r, (ii) has nonconfused areas in any event, when $3.57 \leq r \leq 4$, and (iii) has low biggest LE = 0.6923. Next, numerous plots for the examination of the proposed tumultuous maps will be concentrated, for example, the bifurcation diagram, the Lyapunov exponent, and the iteration property.

2.2.1. Analysis of the First Proposed Chaotic Map. The bifurcation graph of the first proposed turbulent map is introduced in Figure 3(a). This graph has three districts: (i) assembly area is at $r \epsilon$ [0, 0.55], (ii) the bifurcation locale at $r\epsilon$[0.55, 1.0]. The confusion locale is at $r\epsilon$[1.0, 1.4], where the disorderly conduct happens. Figure 3(b) shows the Lyapunov type of the main proposed chaotic map. It is

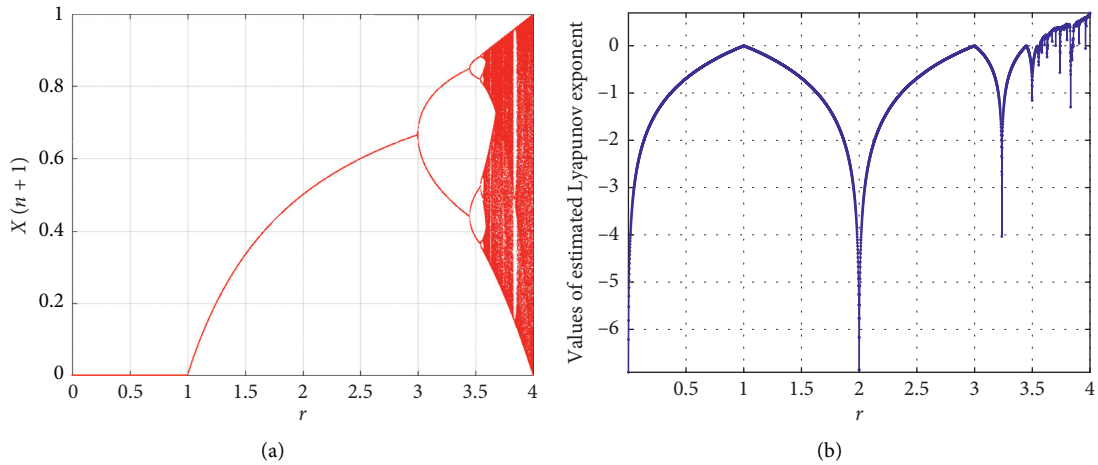


Figure 2: Logistic map: (a) Bifurcation diagram and (b) Lyapunov exponent.

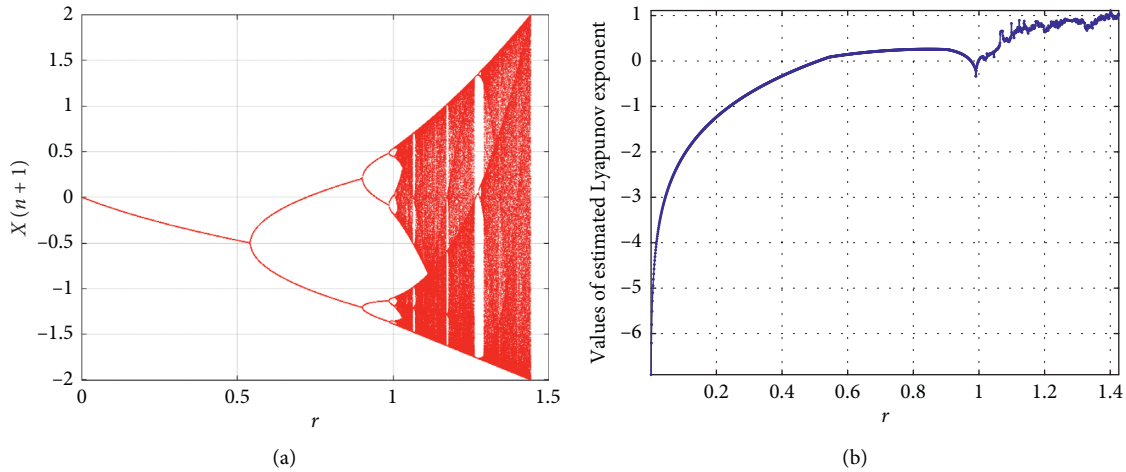


Figure 3: The Bifurcation diagram (a) and Lyapunov exponent (b) for the first proposed map at $x_{(0)} = 0.02$, $y_{(0)} = 0.02$, $a = 1.4$, and $b = 0.3$.

clearly evident that when $r\epsilon$ [0, 0.55] all Lyapunov exponents are less than or equivalent to zero. When $r\epsilon$ [0, 0.55], the Lyapunov exponents are positive and consequently tumultuous. The Maximal Lyapunov Exponent of the first chaotic map is 1.225.

The iteration and trajectory examinations are introduced in Figure 4. When $r\epsilon$ [0, 0.55] as shown in Figures 4(a) and 4(d), the determined qualities arrive at a similar outcome after a few emphases without any chaotic behavior. When $r\epsilon$ [0.55, 1.0], as shown in Figures 4(b) and 4(e), the framework shows up as having an intermittent conduct. When $r\epsilon$ [1.0, 1.4], it turns into a chaotic system as shown in Figures 4(c) and 4(f).

2.2.2. Analysis of the Second Proposed Chaotic Map. The conduct of the second proposed map is introduced through Figure 5. As exhibited by the bifurcation outline shown in Figure 5(a), plainly the guide displays a disorderly conduct at $r\epsilon$ [5, ∞[, the union district is at $r\epsilon$ [0, 4] expect little range (±0.2) around $r = 2.0$ and the bifurcation locale is at $r\epsilon$ [4, 5]. In Figure 5(b), for all estimations of r aside from $r\epsilon$ [5, ∞[, the Lyapunov exponent has a positive worth. Along these lines, the proposed map displays a turbulent conduct at the remainder of the range. The MLE of the proposed map is 3.317.

The iteration and trajectory analyses for the second proposed map are introduced in Figure 6. When $r\epsilon$[0, 4] expect little range (±0.2) around $r = 2.0$ as shown in Figures 6(a) and 6(d), the determined worth goes to the almost same outcome after a few cycles with no chaotic conduct. When $r\epsilon$ [4, 5], as shown in Figures 6(b) and 6(e), the system shows up as having an occasional conduct. When $r\epsilon$ [5, ∞[, it turns into a chaotic system as shown in Figures 6(c) and 6(f).

2.2.3. Analysis of the Third Proposed Chaotic Map. Figures 7(a) and 7(b) depict the bifurcation and Lyapunov exponent, respectively. As readily seen, convergence regions are at $r \in [0.0, 4.0]$, $r \in [6.8, 7.8]$, etc. to infinity. The bifurcation regions are at $r \in [4.0, 5.7]$, $r \in [7.9, 8.2]$, etc. to infinity. The chaos regions are at$r \in [6.0, 6.5]$, $r \in [8.5, 13.0]$,

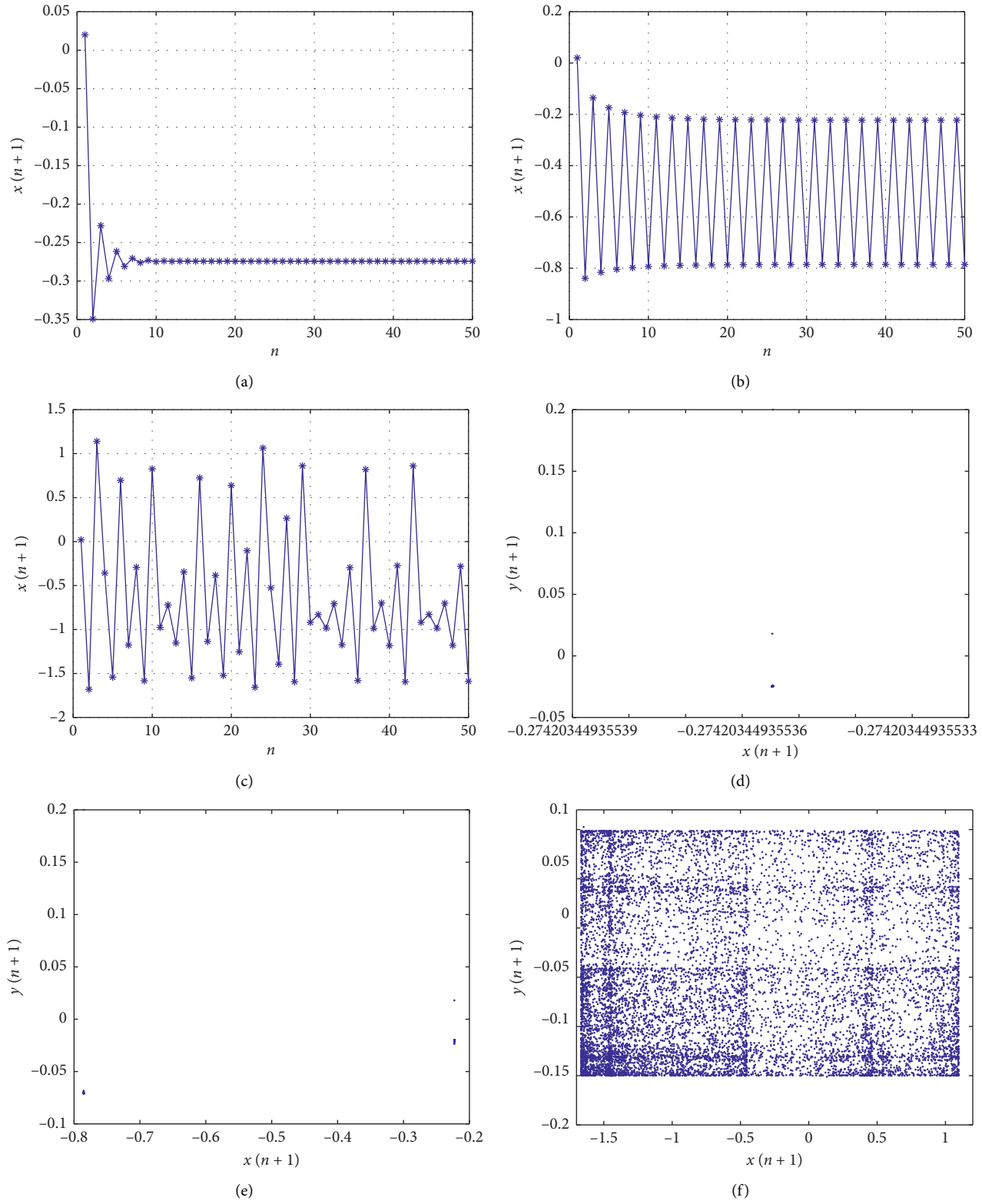


FIGURE 4: Iteration and trajectory analyses of the first proposed chaotic map at $x_{(0)} = 0.02$, $y_{(0)} = 0.02$. Iteration property at (a) $r = 0.25$, (b) $r = 0.6$, and (c) $r = 1.2$. Trajectory property at (d) $r = 0.25$, (e) $r = 0.6$, and (f) $r = 1.2$.

$r \in [14.5, 19]$, etc. to interminability, aside from the little locales of assembly and bifurcation, where the chaotic behavior happens. In Figure 7(b), the Lyapunov exponent has a positive incentive at all estimations of r aside from little scopes of combination and bifurcation. Henceforth, the proposed chaotic map shows a disordered conduct in the

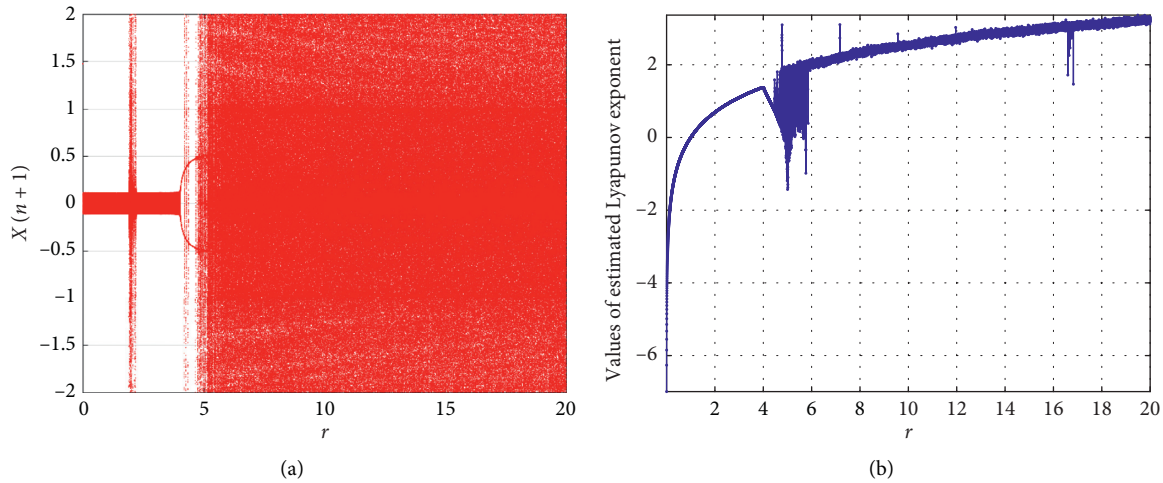


FIGURE 5: The Bifurcation diagram (a) and Lyapunov exponent (b) for the second proposed map, at $x_{(0)} = 0.02$, $y_{(0)} = 0.02$.

remainder of the range. The MLE of the third proposed map is 4.499.

The emphasis and trajectory analyses for the third guide are introduced in Figure 8. When $r \in [0.0, 4.0]$, $r \in [6.8, 7.8]$, and so forth to boundlessness as shown in Figures 8(a) and 8(d), the determined qualities arrive at a similar outcome after a few emphases with no disorganized conduct. When$r \in [4.0, 5.7]$, $r \in [7.9, 8.2]$, and so forth to unendingness, as shown in Figures 8(b) and 8(e), the framework shows up as having an intermittent conduct. When $r \in [6.0, 6.5]$, $r \in [8.5, 13.0]$, $r \in [14.5, 19]$, and so on to unendingness, it turns into a chaotic system as Figures 8(c) and 8(f) illustrate.

2.2.4. Analysis of the Fourth Proposed Chaotic Map. At long last, the disorderly conduct of the fourth guide is shown in Figures 9 and 10. The bifurcation chart in Figure 9(a) shows a few combination, bifurcation, and chaos regions. These districts stretch out to interminability. The bifurcation areas are at $r \in [4.4, 4.5]$, $r \in [8.55, 8.7]$, and so on to interminability. The assembly areas are at $r \in [4.2, 4.3]$, $r \in [8.4, 8.5]$, and so on to unendingness. The disorder locales are at $r \in [4.5, 8.4]$, $r \in [8.8, 12.5]$, and so on to limitlessness, where the confused conduct happens. In Figure 9(b), the Lyapunov exponent has a positive incentive at $r \in [4.5, 8.4]$, $r \in [8.8, 12.5]$, and so forth to unendingness and consequently the proposed fourth tumultuous map shows a clamorous conduct at these periods. The MLE of the proposed map is 3.091.

The iteration and trajectory examinations for the fourth proposed chaotic map are introduced in Figure 10. When $r \in [4.2, 4.3]$, $r \in [8.4, 8.5]$, and so on to vastness as shown in Figures 10(a) and 10(b), the determined qualities additionally arrive at a similar outcome after iterations with no chaotic conduct. When $r \in [4.4, 4.5]$, $r \in [8.55, 8.7]$, etc. to endlessness, as shown in Figures 10(b) and 10(e), the system shows up as having an occasional conduct. When $r \in [4.5, 8.4]$, $r \in [8.8, 12.5]$, etc. to infinity, it turns into a chaotic system as shown in Figures 10(c) and 10(f).

Table 1 sums up the investigation of the classical and proposed chaotic maps. It shows the improvement in both the turbulent parameter range r and MLE.

3. The Proposed Encryption System

An iterative handle to scramble arrangement of bytes that is 1D changed form of the 2D original image can be used in the suggested scheme. As given in equations (1) through (4), the proposed chaotic capacities are utilized. These capacities together guarantee perplexity and dissemination procedure required for encryption. For increasing security and to decrease encryption time, the algorithm is additionally backed with some logical operations help. The structures of encryption and decryption procedures are demonstrated in Figure 11. The DWT, based on operations of high-pass and low-pass filtering, consists in decomposing the image into sub-bands. For a single level decomposition, it presents an image as four sub-bands; the first sub-band represents an approximation image Low-Low (LL) and the others show image details in horizontal high-low (HL), vertical low-high (LH), and diagonal high-high (HH) directions. The four proposed maps are used to permute the positions of the four sub-bands pixels. The constructed proposed chaotic sequence is adopted to diffuse the overall permutation image; an auxiliary key is brought in the algorithm to make the algorithm sensitive to the secret keys. The Inverse Discrete Wavelet Transform (IDWT) allows perfect reconstruction of the image. The following subsection has details of encryption and decryption algorithms.

Within the presented cryptosystem for encryption and decryption forms, four of the proposed maps are utilized. The initial conditions and control parameters (key states) are extracted from the secret key and used to produce chaotic sequences from the proposed maps.

3.1. Encryption Process. The proposed image encryption plot dependent on chaos structure is delineated in Figure 11(a). DWT, permutation (confusion), and diffusion stages are

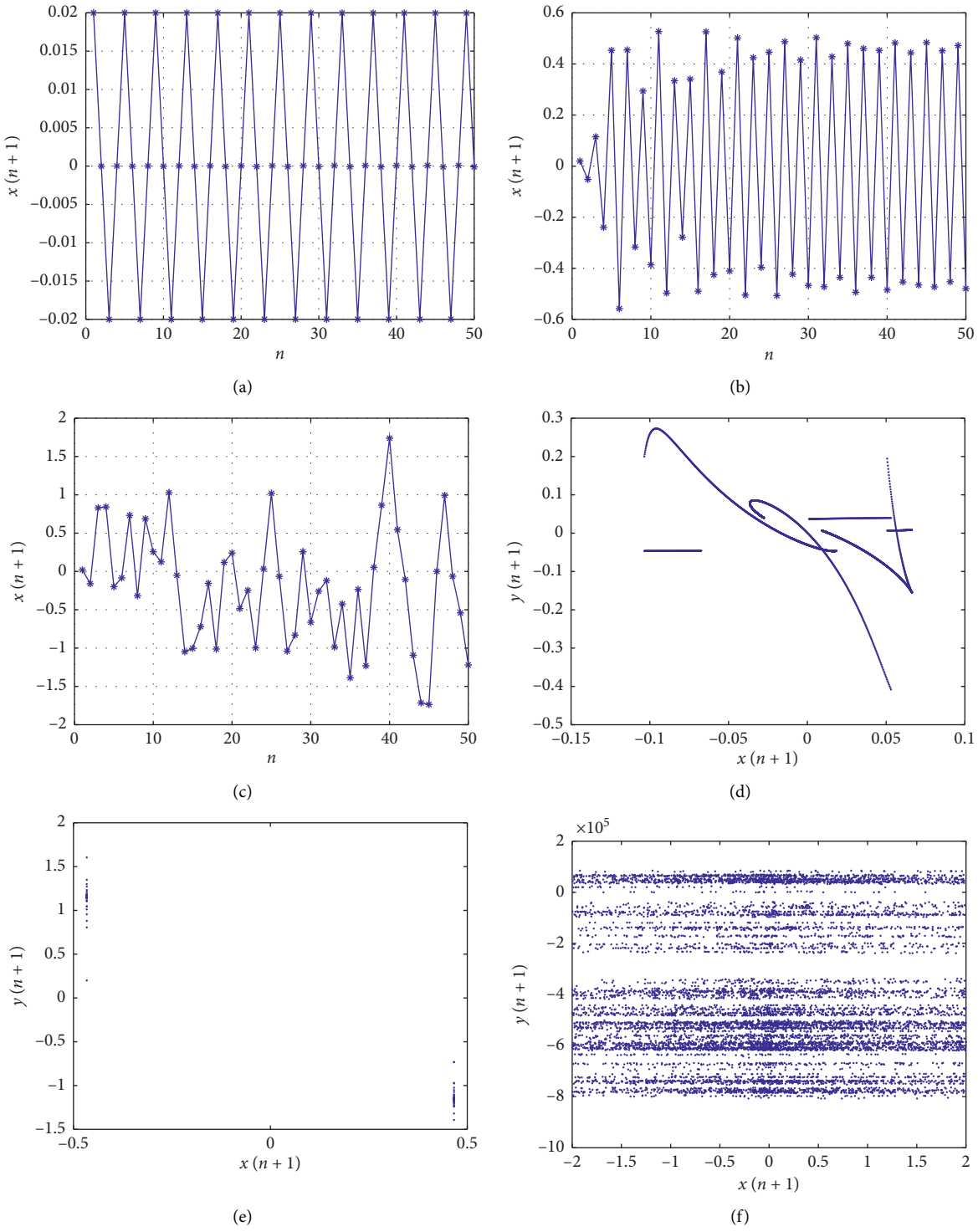
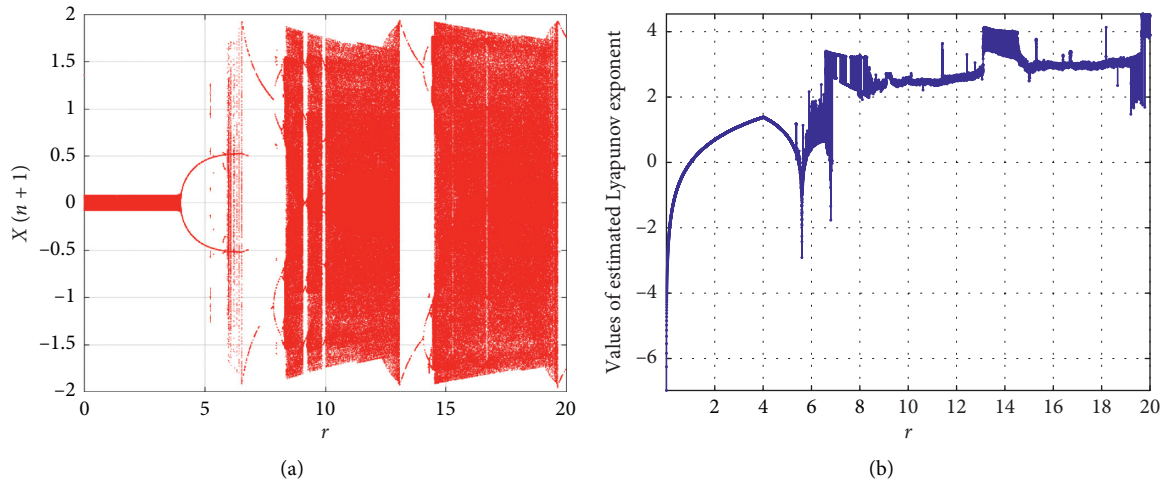


FIGURE 6: Iteration and trajectory analyses of the second proposed chaotic map at $x_{(0)} = 0.02$, $y_{(0)} = 0.02$. Iteration property at (a) $r = 3.0$, (b) $r = 4.6$, and (c) $r = 10.0$. Trajectory property at (d) $r = 3.0$, (e) $r = 4.6$, and (f) $r = 10.0$.

utilized to totally encode an image. Both the stage and dissemination tasks are intended to utilize tumultuous states and plain picture information to change pixel positions and substitute pixel esteems separately, bringing about a clamor-like cipher image.

3.1.1. Discrete Wavelet Transforms. DWT is famous in many image/video applications because of its multigoal portrayal. The fundamental thought of the DWT for a two-dimensional image is depicted as follows. With the pyramid-organized wavelet change, the original image will experience various



(a) (b)

Figure 7: The bifurcation diagram (a) and Lyapunov exponent (b) for the third proposed map, at $x_{(0)} = 0.02, y_{(0)} = 0.02$.

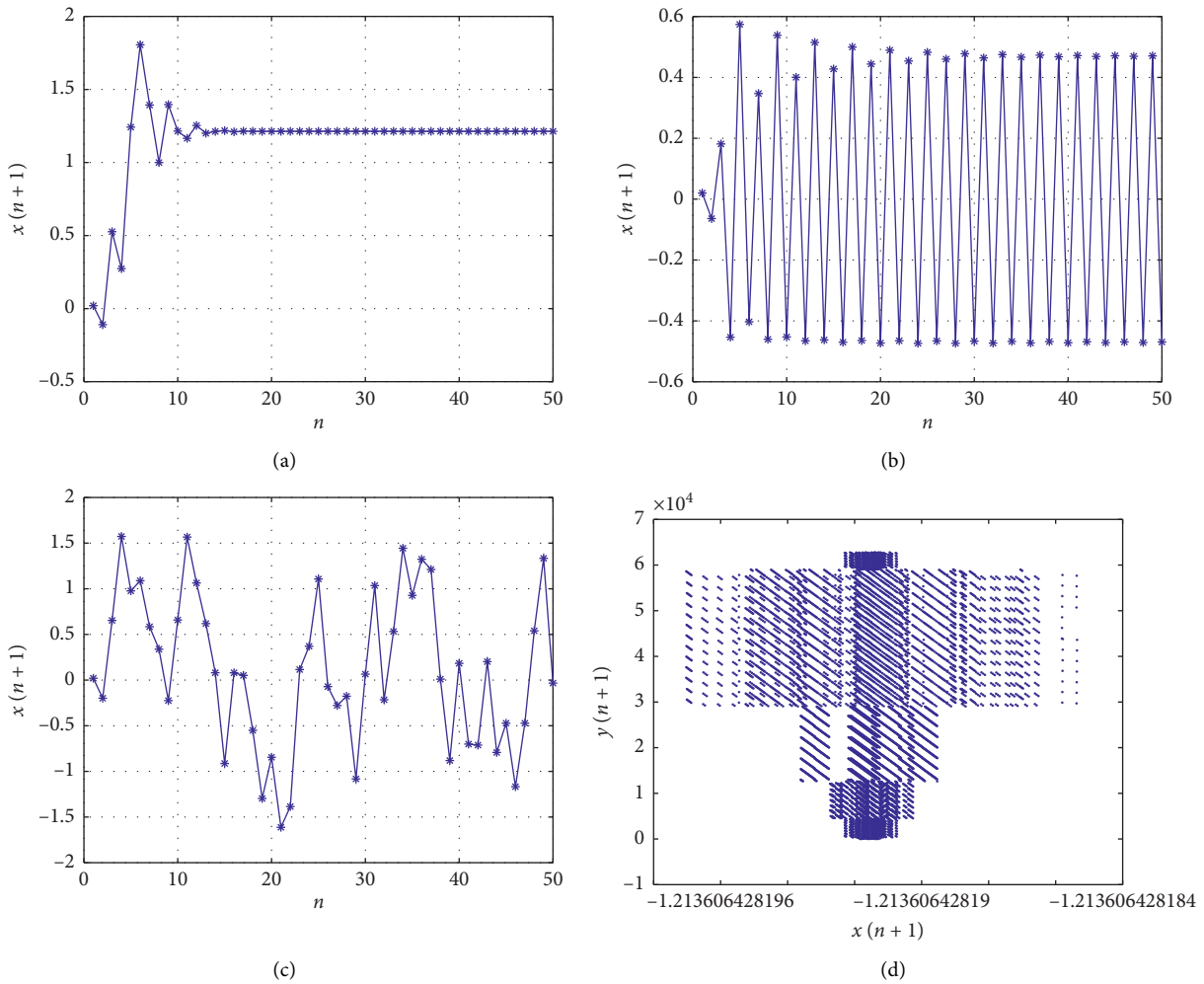


Figure 8: Continued.

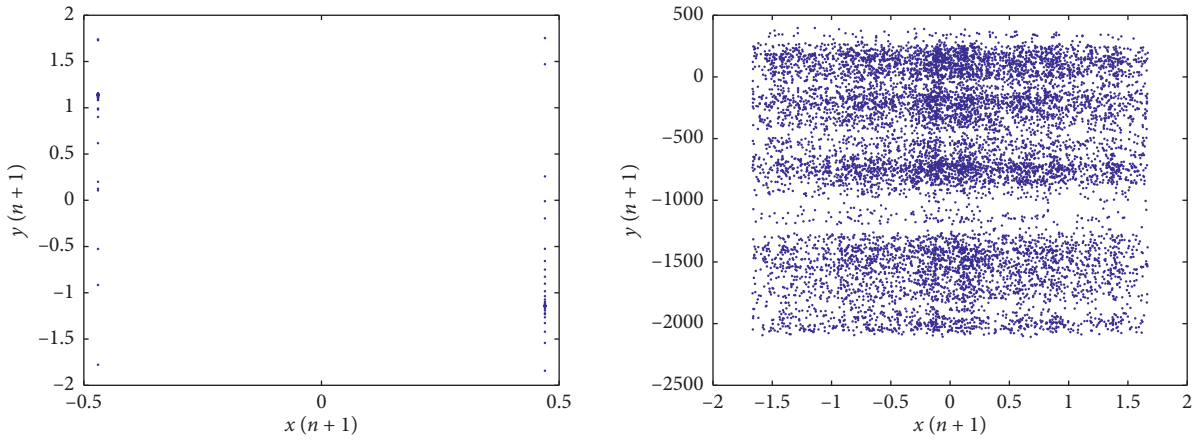


FIGURE 8: Iteration and trajectory analyses of the third proposed chaotic map at $x_{(0)} = 0.02$, $y_{(0)} = 0.02$. Iteration property at (a) $r = 7.5$, (b) $r = 5.2$, and (c) $r = 12.0$. Trajectory property at (d) $r = 7.5$, (e) $r = 5.2$, and (f) $r = 12.0$.

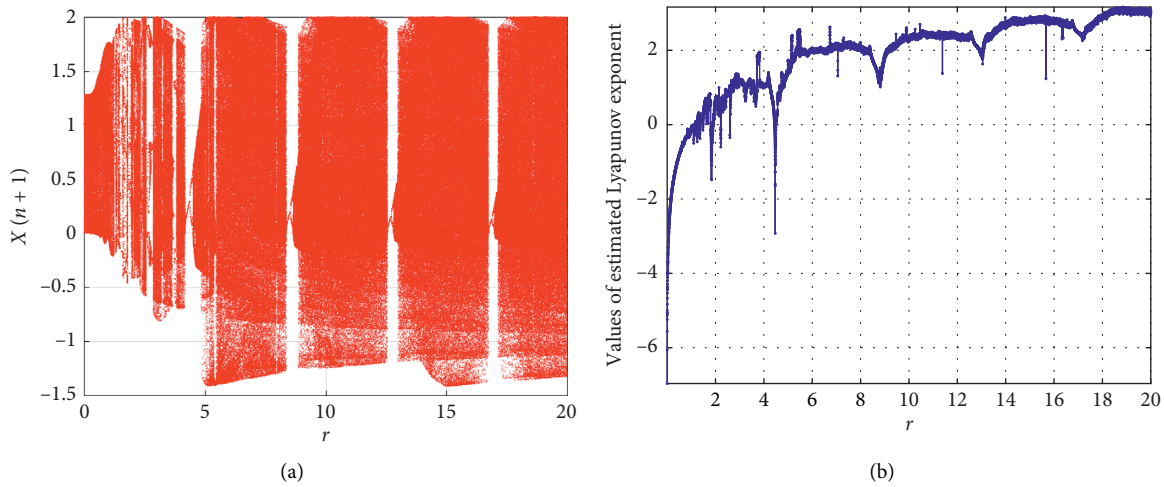


FIGURE 9: The bifurcation diagram (a) and Lyapunov exponent (b) for the fourth proposed map at $x_{(0)} = 0.02$, $y_{(0)} = 0.02$, and $a = 1.5$.

blends of a low-pass filter and a high-pass filter and afterward dependent on the convolution with these channels to produce the LL, LH, HL, and HH subgroups. To acquire the following coarser scaled wavelet coefficients, the sub-band LL is additionally disintegrated and fundamentally subexamined. This procedure can rehash several times, which is controlled by the application. With the pyramid-organized wavelet transform, the size of the original image is identical to adding all the decayed subimages up. Utilizing this decay structure, there will be no data lost when the disintegrated pieces are reproduced. This remaking procedure is called IDWT [20].

3.1.2. The Permutation Process. We utilize the proposed chaotic maps to produce tumultuous groupings and afterward sort that confused numbers in rising or plunging order for the age of the change key. We sort the chaotic sequences in the record network utilized in rearranging the original image to acquire the permuted image. In the wake of acquiring the rearranged image, the relationship among the neighboring pixels is totally upset and the image is totally unrecognizable. In this way, the permuted orderly conduct of the fourth g image is frail against factual assault, and realized plain-content assault [21]. Therefore, we utilize a dispersion procedure after change to improve the security.

3.1.3. The Diffusion Process. The dissemination step in the proposed encryption plot is performed by the key identified with the plain image calculation which utilized just one round dispersion activity and its key relies upon the initial key and the original image [22]. The diffusion procedure in

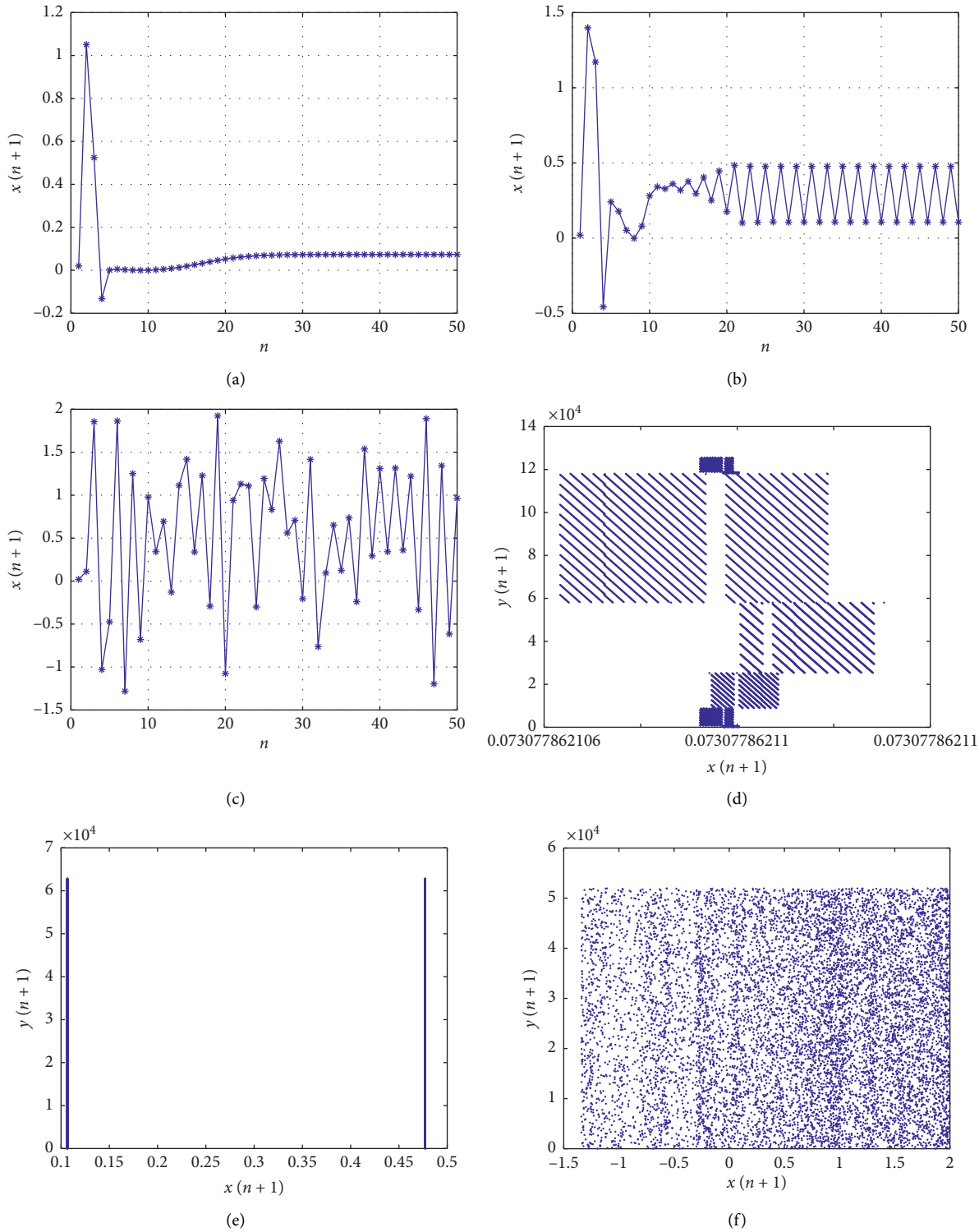


FIGURE 10: Iteration and trajectory analyses of the fourth proposed chaotic map at $x_{(0)} = 0.02$, $y_{(0)} = 0.02$. Iteration property at (a) $r = 8.4$, (b) $r = 4.45$, and (c) $r = 7.0$. Trajectory property at (d) $r = 8.4$, (e) $r = 4.45$, and (f) $r = 7.0$.

our scheme depends on the proposed chaotic maps. We will talk about the encryption procedure just in detail, because the decryption is the opposite procedure. The subtleties of the encryption procedure can be summed up by Algorithm 2.

3.2. Decryption Process. The decryption procedure is the opposite activity of the encryption procedure. The schematic representation of the structure of the decoding forms is shown in Figure 11(b). Utilizing similar mystery keys, it tends to produce a tumultuous record grouping

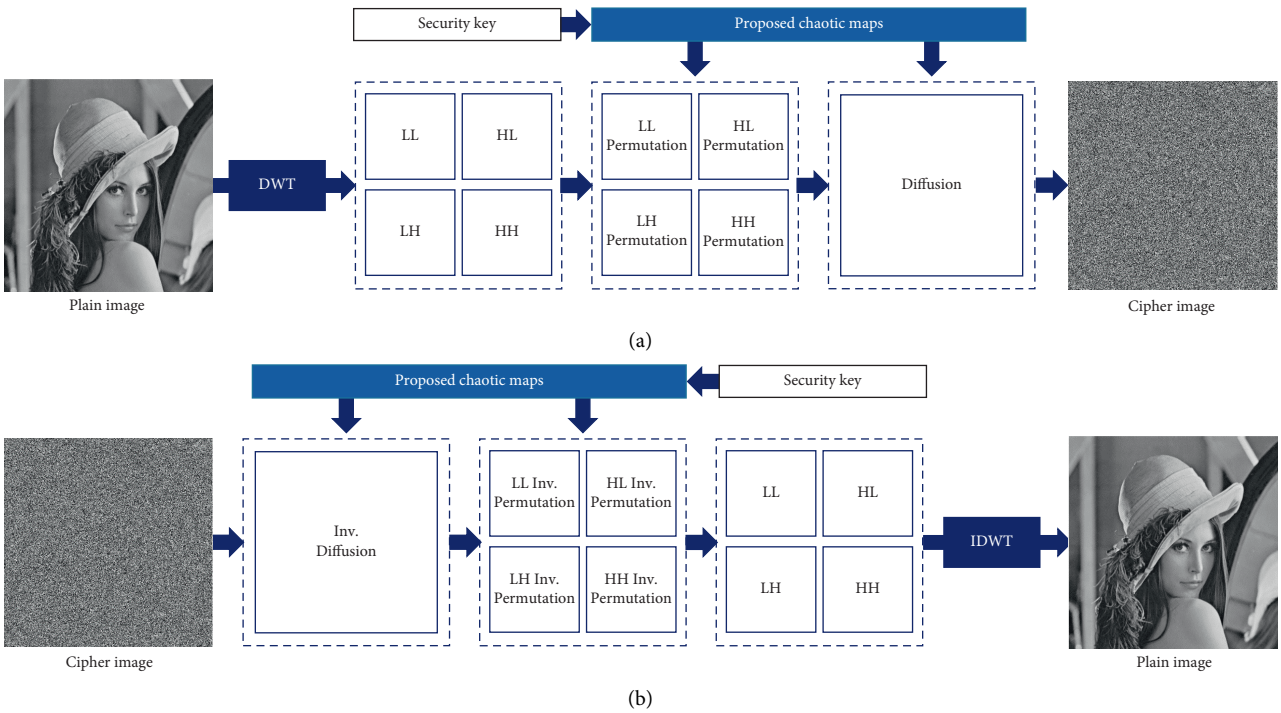


Figure 11: Schematic illustration: (a) the encryption processes, and (b) the decryption processes. Note that DWT, LL, LH, HL, HH Inv. Diffusion, Inv. Permutation, and IDWTstand for, Discrete Wavelet Transform, low-low, low-high, high-low, high-high, inverse diffusion, inverse permutation, and inverse Discrete Wavelet Transform, respectively.

and the disordered vectors created in encryption process. The decoding calculation additionally comprises three fundamental stages: inverse diffusion, inverse confusion, and IDWT. Initially, we convert the encoded picture C in size $M \times N$. At that point, we produce a reverse diffused vector. Besides, we acquire the consolidated permutated vector and recompose it into the four-stage subgroups (LL_P, LH_P, HI_P, and HH_P). At long last, converse stage for each sub-band (LL, LH, HI, and HH) utilizing the confused record arrangement, and get the original image P utilizing IDWT. The decryption procedure is given in detail in Algorithm 3.

4. Performance Metrics

The quantitative performance of proposed techniques compared with traditional techniques could be measured using different metrics. The latter include (i) statistical parameters, (ii) differential parameters, and (iii) efficiency parameters [23]. Details of those metrics are given as follows.

4.1. Statistical Parameters. Good cipher must have strong resistance against any measurable examination. To confirm the security of any encryption technique, the following statistical examinations should be performed [24].

4.1.1. Histogram Analysis. An image histogram depicts the conveyance of image pixels by plotting the number of pixels at each gray scale level. The redundancy of plaintext should be hidden in the distribution of cipher text and this distribution logically needs to be uniform [23]. The histogram equation of an image is gotten as follows:

$$P_n = \frac{\text{number of pixels with intensity } n}{\text{total number of pixels}}, \quad n = 0, 1, \ldots, L-1, \tag{7}$$

where I is represented as an r by c matrix of numbers extending of pixels from 0 to $L-1$. L is the number of conceivable concentrated values, more often than not 256, and P_n indicates the normalized histogram of [25].

4.1.2. Correlation Analysis. The relationship between two variables is called correlation coefficient (R) [26]. The cross-correlation coefficient between decrypted images and original is

$$R = \frac{\sum_m \sum_n \left(\mathrm{OI}_{mn} - \overline{\mathrm{OI}}\right)\left(\mathrm{DI}_{mn} - \overline{\mathrm{DI}}\right)}{\sqrt{\left(\sum_m \sum_n \left(\mathrm{OI}_{mn} - \overline{\mathrm{OI}}\right)^2\right)\left(\sum_m \sum_n \left(\mathrm{DI}_{mn} - \overline{\mathrm{DI}}\right)^2\right)}}, \tag{8}$$

where n is the column number, m is the row number, $\overline{\mathrm{OI}}$ is the pixels mean value of original image, and $\overline{\mathrm{DI}}$ is the pixels mean value of decrypted image. Ideally, the value of R should be 1.

4.1.3. Information Entropy Analysis. The entropy is a perfect feature to evaluate the degree of randomness. The entropy of a message source could be computed as [27]

Table 1: Comparison between the classical and proposed quadratic maps. Note: MLE is Maximal Lyapunov Exponent.

Chaotic map	Equation	Chaotic parameter range	MLE
Classical quadratic map [19]	$x_{n+1} = r - x_n^2$	$r \in [3.75, 4]$	0.6923
The first proposed chaotic map	$\begin{cases} y_{1+n} = b^2 x_n \\ x_{1+n} = (x_n)^2 + (y_n)^2 - a.r \end{cases}$	$a = 1.4,\ b = 0.3,\ r \in [1, 1.4]$	1.225
The second proposed chaotic map	$\begin{cases} y_{n+1} = y_n - r.\tan x_n \\ x_{n+1} = \sin x_n + \sin y_{n+1} \end{cases}$	$r \in [5, \infty[$	3.317
The third proposed chaotic map	$\begin{cases} y_{1+n} = y_n - r\tanh x_n \\ x_{1+n} = \tanh x_n + \sin y_{n+1} \end{cases}$	$r \in [6, 6.5],\ r \in [8.5, 13],\ r \in [14.5, 19]$ to ∞	4.499
The fourth proposed chaotic map	$\begin{cases} y_{1+n} = y_n + a.r\cos x_n \\ x_{1+n} = \cos x_n + \sin y_{n+1} \end{cases}$	$a = 1.5,\ r \in [4.5, 8.4],\ r \in [8.8, 12.5]$ to ∞	3.091

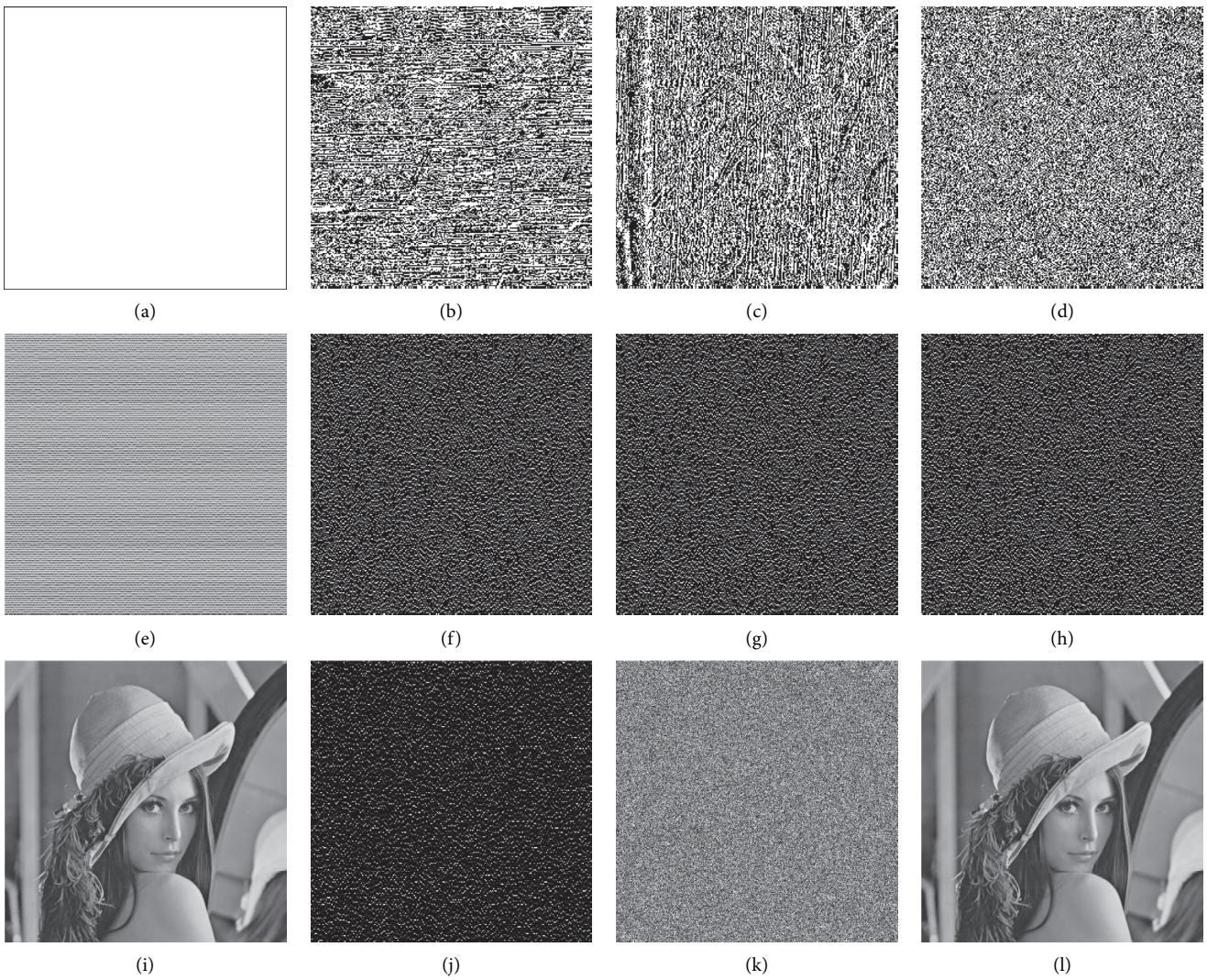


Figure 12: The simulation steps: (a) LL component; (b) LH component; (c) HL component; (d) HH component; (e) LL component confusion; (f) LH component confusion; (g) HL component confusion; (h) HH component confusion; (i) original image; (j) overall confusion; (k) encrypted image; and (l) decrypted image.

Input: plain image P
Output: cipher image C
Begin
//Permutation Process

Step 1: examine the plain image P in size $M \times N$. P can be a gray-scale or RGB image.
Step 2: decompose the image into four level sub-bands (LL, LH, HL, and HH) by the selected DWT.
Step 3: choose a two-dimensional chaotic system and generalize it by introducing the initial values (x_0, y_0, a, b, r) , these initial values as secret keys.
Step 4: generate the chaotic sequences using the proposed chaotic maps and set the appropriate values of the secret keys. Can use the 1st proposed chaotic map.
Step 5: change the chaotic sequence, with the same method, into a consistently dispersed grouping by altering the initial values and parameters.
Step 6: iterate the chaotic sequence for LL sub-band for scrambling LL_P row by row and column by column (starting from the first row and the first column)
Step 7: like step 3, compute the next quantized chaotic pair using the 2nd, 3rd, and 4th proposed chaotic maps to scramble the next sub-bands of LH, HL, and HH, respectively, and reiterate this step total times. (When the last row or the last column has been scrambled, switch to the first row or the first column over again.)
Step 8: combine the chaotic vectors (LL_P, LH_P, HI_P, and HH_P) into one vector with S_k in size $M \times N$.
Step 9: make the new vector of mistook pixels for S_P in size $M \times N$ as $S_P = S_K(\text{index})$.
//Diffusion Process

Step 10: adjust and change the vector S_P realizing that every component of level gray ranges in [0, 255] utilizing the accompanying condition: $S_P(i) = \text{mod}(\text{round}(10^{12} S_P(i)), 256)$, where $1 \le i \le M \times N$
Step 11: create the diffused vector with S_D in size $M \times N$ as follows: $S_D = S_P \oplus S_K$, where $\oplus$ denotes the exclusive OR operation bit by bit
Step 12: create the final matrix with cipher image C as follows: $C = \text{reshape}(S_D, M, N)$Algorithm 2: Proposed encryption process.

End

Input: cipher image C
Output: plain image P
Begin
Step 1: produce the deshuffled vector as follows: $S_P = S_D \oplus S_K$, where $\oplus$ denotes the exclusive OR operation bit by bit
Step 2: produce the permutated each vector as follows: $S_P = S_K$ (index)
Step 3: obtain the permutation sub-bands (LL_P, LH_P, HI_P, and HH_P)
Step 4: opposite stage and reshape vector components utilizing the chaotic index sequence to get sub-bands (LL, LH, HI, and HH)
Step 5: use IDWT recovers to obtain the original image
End

Algorithm 3: Proposed decryption process.

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i)\log_2(p(m_i)), \tag{9}$$

where N represents the number of bits for each symbol and $p(m)$ is the probability of symbol m_i.

4.2. Differential Parameters. Encrypted image needs to be sensitive to tiny changes in plain image. Attacker can change some features in the plain image to get changes within the encrypted one. If a small unsettling influence within the original image comes about in a significant change in the encrypted one, then differential attacks lose their efficiency and become useless [28].

4.2.1. Mean Square Error. The Mean Square Error (MSE) is used in this paper to measure difference between the plain and encrypted images. The high value of MSE corresponds to a high difference between plain and encrypted images. It can present as in equation (10) [29]:

$$\text{MSE} = \frac{1}{M_x N_x f} \sum_{K=1}^{f} \sum_{i=1}^{M} \sum_{j=1}^{N} [P(i, j) - C(i, j)]^2, \tag{10}$$

where N is the number of columns, M is the number of rows, and f is the number of image frames. The parameters $P(i, j)$ and $C(i, j)$ refer to the pixels of the plain and the encrypted images, respectively. For a MSE ≥30 dB, there is a difference between the plain and encrypted images.

4.2.2. Normalized Mean Square Error. Another popular performance measurement related to MSE is Normalized Mean Square Error (NMSE) which equals MSE divided by the maximum MSE as in equation (11) [30].

$$\text{NMSE} = \frac{\text{MSE}}{(\max \text{MSE})}. \tag{11}$$

4.2.3. Peak Signal-to-Noise Ratio. The peak signal-to-noise ratio (PSNR) measures the conformity between the original and decrypted images [31]. For an image of size $M \times N$, it can be evaluated as follows:

$$\text{PSNR} = 10 \log_{10}\left(\frac{\text{Max}_{01}^2}{\text{MSE}}\right)\text{dB}, \tag{12}$$

where Max_{01} represents the maximum possible pixel value of the original image. For a good encryption algorithm, the PSNR should be as low as possible between the plain and encrypted image.

4.2.4. Number of Pixels Change Rate. The Number of Pixels Change Rate (NPCR) is utilized to measure the percentage of different pixel numbers between the original and decrypted images and is assessed as within the following condition [31, 32].

$$\text{NPCR} = \left[\frac{1}{M \times N \times f} \sum_{K=1}^{f} \sum_{i=1}^{M} \sum_{j=1}^{N} D_i(i, j)\right] \times 100\%,$$
$$D_i(i, j) = \begin{cases} 0, & \text{if OI}(i, j) = \text{DI}(i, j), \\ 1, & \text{if OI}(i, j) \neq \text{DI}(i, j). \end{cases} \tag{13}$$

NPCR evaluates the rate of pixels change in the coded image after modification in one pixel of an original one; as with higher value for NPCR, more effective performance is got [32]. The practical value for 1-NPCR ought to be approximately 0.99 [33].

4.2.5. Unified Average Changing Intensity. The Unified Average Changing Intensity (UCI) measures the average intensity of difference between plain and decrypted images. It could be computed through the following equation [33].

$$\text{UACI} = \left[\frac{1}{M \times N \times f} \sum_{K=1}^{f} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\text{OI}(i, j) - \text{DI}(i, j)}{2^l - 1}\right] \times 100\%, \tag{14}$$

where the number of columns is represented by N, M is the number of rows, f is the number of image frames, DI is decrypted image, OI is the original image, and l is the number of bits per pixel of original image.

4.3. Efficiency Parameters. Efficiency and high speed are additionally imperative issues for a successful cryptosystem, particularly for real-time Internet application. Generally, encryption speed is highly dependent on the CPU/MPU structure, size of RAM, operation system, the programming language, and compiler option. So, there is no need to compare the encryption speeds of two ciphers image using two different devices [24]. The foremost common parameter related to efficiency analysis is the slipped-by-time (sec) which has spoken to the overall computation time for encryption as well as decryption prepared in seconds for each trial of experiments.

5. Experimental Results

Most encryption algorithms are tested by utilizing measurable examination. Those analyses are utilized to find a relation between the encrypted and the original image. All of our experiments have been conducted utilizing a core i5-2400 Windows 7 machine with a 4 GB RAM, 160 GB HDD, and the same version of MATLAB programming environment. Our device was connected to the web most of time. All tests have been connected more than one time and thus the elapsed time represents the average simulation time for all trials for each test. The execution of proposed algorithm is tested using MATLAB R2017a where it is inspected through an arrangement of tests.

The proposed approach is implemented using the proposed maps for encryption and decryption of an image. We used the benchmark images Lena, Cameraman, Baboon, etc. (each of which is 512×512 pixels) as plain (original) images. With multi-map orbit key, the proposed maps are performed. The foremost direct technique to choose the disorderly degree of the encrypted image is by the sense of sight. On the other hand, the stochasticity of encrypted images can be quantitatively calculated by the connection coefficient. Appling the proposed maps, the parameters r and n should be set agreeing with Step 1 in Algorithm 2. Based on the experimental encounter, general combos of r and n can continuously result in exceptionally disruptive outcomes at intervals of recreation. The beginning conditions of all proposed chaotic maps utilized are set as $x_{(0)} = 0.02$ and $y_{(0)} = 0.02$ as initial conditions for the first random key. The simulation results of the encryption process for Lena image are shown in Figure 12.

5.1. Encrypted and Decrypted Experiment Tests. Four pictures are utilized to test the encryption algorithm, "Lena," "Cameraman," "Baboon," and "Peppers." From the simulation results shown in Figure 13, these cipher images show up to be so boisterous such that any data from them cannot be gotten. Within the decryption process, by utilizing the proper secret keys, the decoded images are the same as initial plain images.

Conveyances of information values in a system comprised the histogram. Histogram investigation can be made by looking at information distributions in numerous diverse fields. In encryption practices, in case the conveyances of numbers that represent encrypted data are near, this implies encryption is performing well. The closer the encrypted data distributions, the higher their encryption level. The

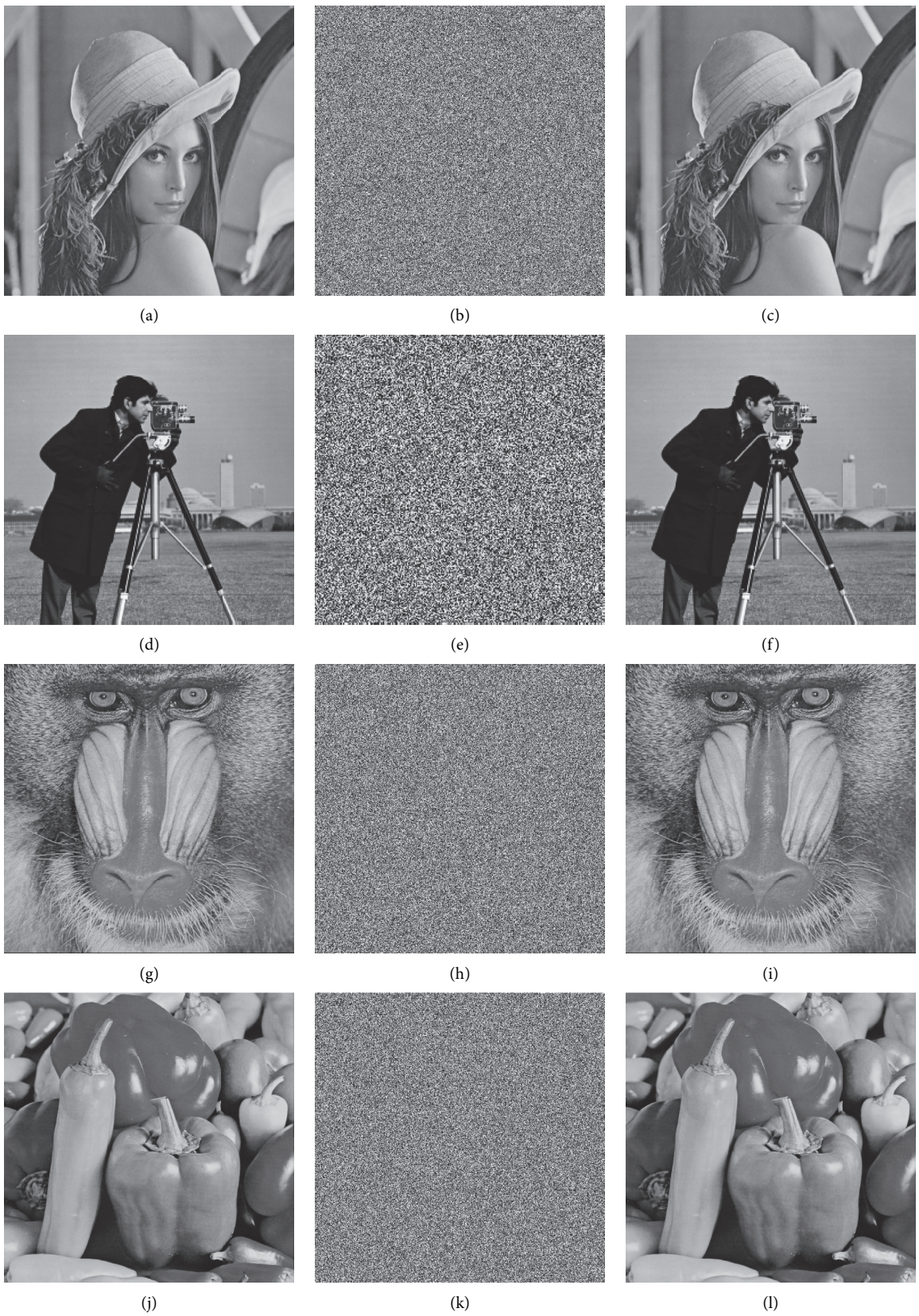


Figure 13: Encryption and decoding results: (a) Lena plain image; (b) Lena scrambled picture; (c) Lena decrypted image with right keys; (d) Cameraman plain image; (e) Cameraman encrypted image; (f) Cameraman decrypted image with right keys; (g) Baboon plain image; (h) Baboon encrypted image; (i) Baboon decrypted image with right keys; (k) Peppers plain image; (l) Peppers scrambled image; and (m) Peppers decrypted image with right keys.

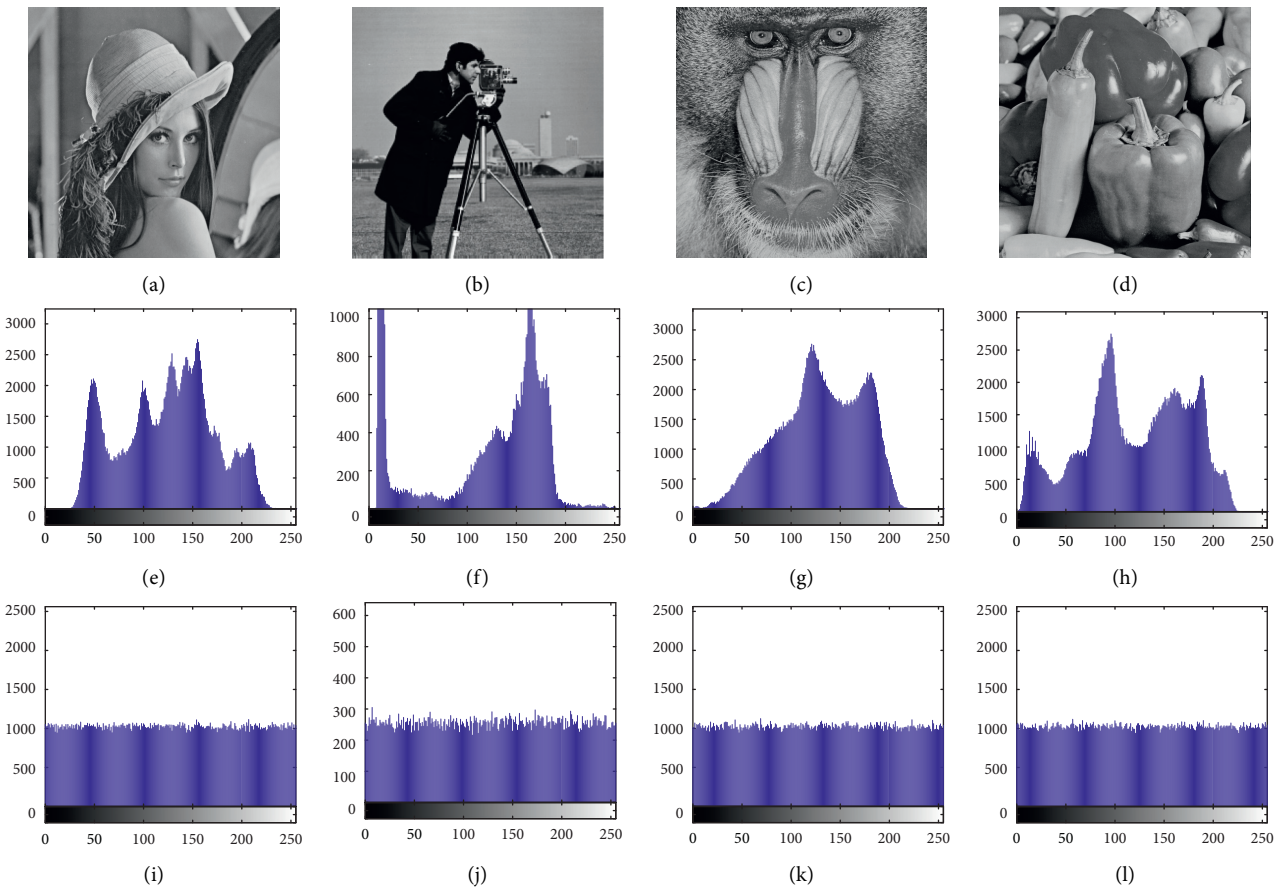


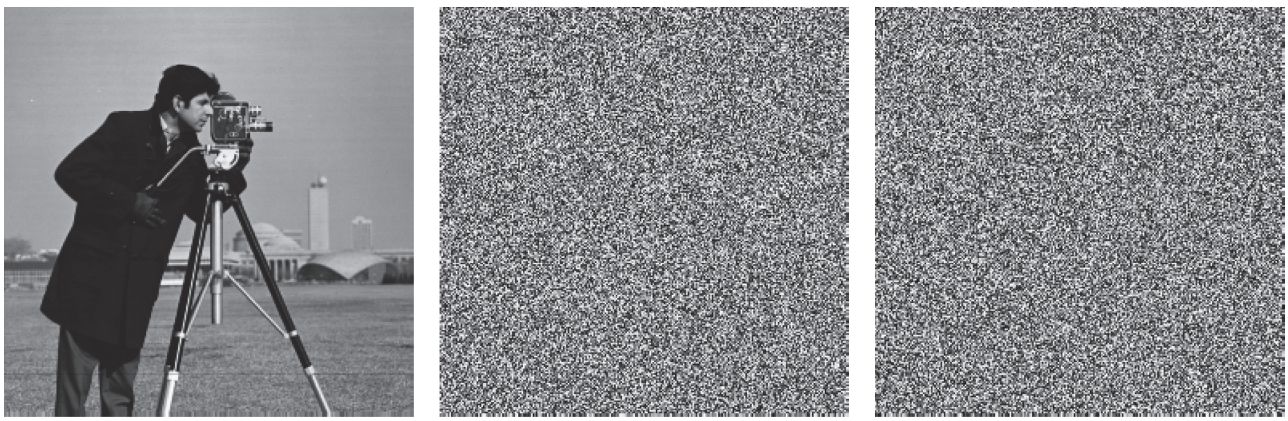
FIGURE 14: Simulation results of sample test images: (a) Lena, (b) Cameraman, (c) Baboon, and (d) Peppers, respectively; (e)-(h) histogram of original images; and (i)-(l) histogram of cipher images.

histogram investigation for the chosen sample images is shown in Figure 14. As shown in Figures 14(i)–14(l), the histograms of the encrypted images are uniform and do not give any clues to utilization of any factual examination assault. Subsequently, it is troublesome for attackers to perform the factual examination since there are no valuable data exposed within the cipher images.

5.2. Key Space Analysis. The key space is the all out number of various keys that can be utilized in the encryption procedure. The proposed calculation comprises two procedures: permutation and diffusion. In permutation process, we utilize the four proposed maps with autonomous factors x_0, y_0, a, b and r for the four sub-bands. In the diffusion process, the clench hand proposed map has independent variables x_0 and r. In the key identified with the plain content algorithm, we have a consistent whole number c and c [1, 255]. Thus, the key space is {x_0, y_0, a, b, r}. Sincex_0, y_0, a, b and r are twofold accuracy numbers, the absolute number of various qualities for x_0, y_0, a, b and r is more than 1014. In this way, the key space is bigger than $1014 \times 1014 \times 1014 \times 1014 \times 1014 \times 255$. This huge key space is sufficient to resist brute-force attack.

5.3. Key Sensitivity Analysis. In addition to histogram analysis, we employed another critical feature of chaos encryption, which is key sensitivity. During the decryption, any little alteration within the key leads to diverse results. Even if only one parameter has been changed, encrypted data cannot be unscrambled. Additionally, the information cannot be decrypted with knowing all the keys since the decryption does not occur within the correct order. Figure 15 shows the encrypted image of the proposed approach when utilizing the specific keys. Figure 15(a) shows the original cameraman image. Figures 15(b) and 15(c) show the encrypted images utilizing diverse encrypted keys and there are no patterns or shadows obvious within the corresponding decrypted image with utilizing off-base keys.

The decrypted image is shown in Figure 16, where Figure 16(a) shows the decrypted image using the same keys of encryption. Figures 16(b) and 16(c) show illegal decrypted images while using the error keys. The results show that the decrypted images are all unrecognized. This means that, without using the right key, the original image cannot be recovered. A little key change will produce the error decryption results. Therefore, the proposed encryption algorithm has high key sensitivity.

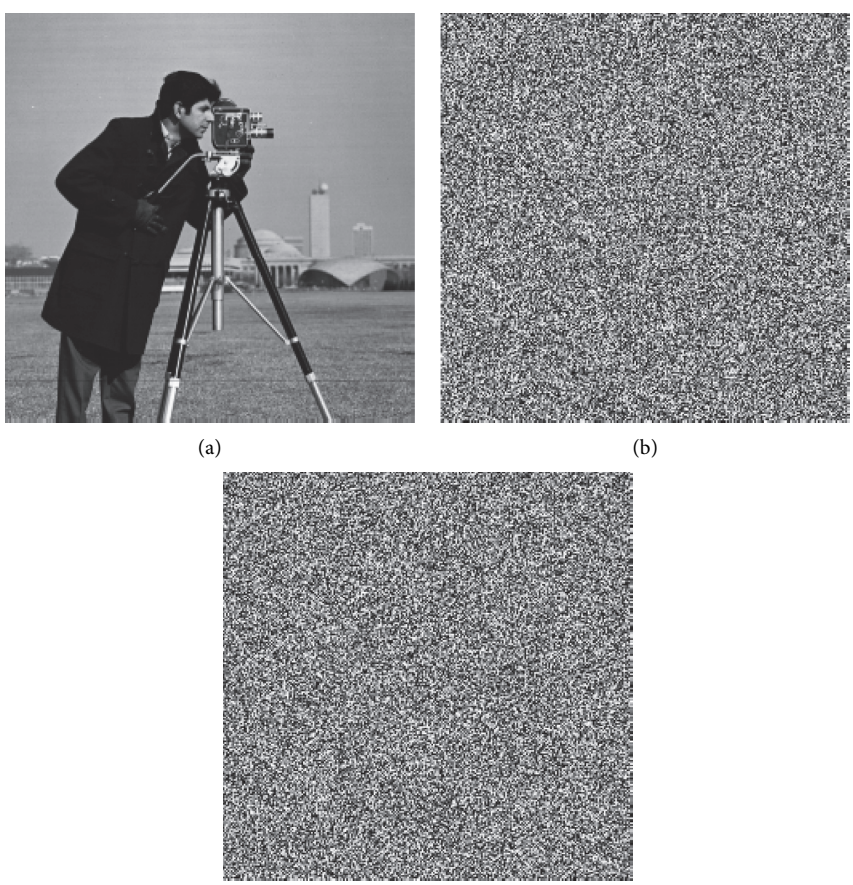


(a) (b) (c)

Figure 15: Key sensitivity of encrypted process: (a) Cameraman plain image; (b) Cameraman encrypted image with first key; and (c) Cameraman encrypted image with another key.

Table 2: Parameters of the encryption quality for different test image. Please note that MSE, PSNR (dB), and ET (sec) stand for minimum mean square error, peak signal-to-noise ratio, and elapsed time, respectively.

Image name	MSE	PSNR	ET	Entropy
Lena	7747.309	9.23929	0.28913	7.9993
Cameraman	9445.441	8.3785	0.17302	7.9991
Baboon	7254.201	9.52486	0.30186	7.9993
Peppers	8413.235	8.88117	0.20668	7.9994
Average	8215.0465	9.005955	0.2426725	7.999275



(a) (b)

(c)

Figure 16: Decrypted process with key sensitivity (a) using same keys of encrypted and (b,c) using the error keys.

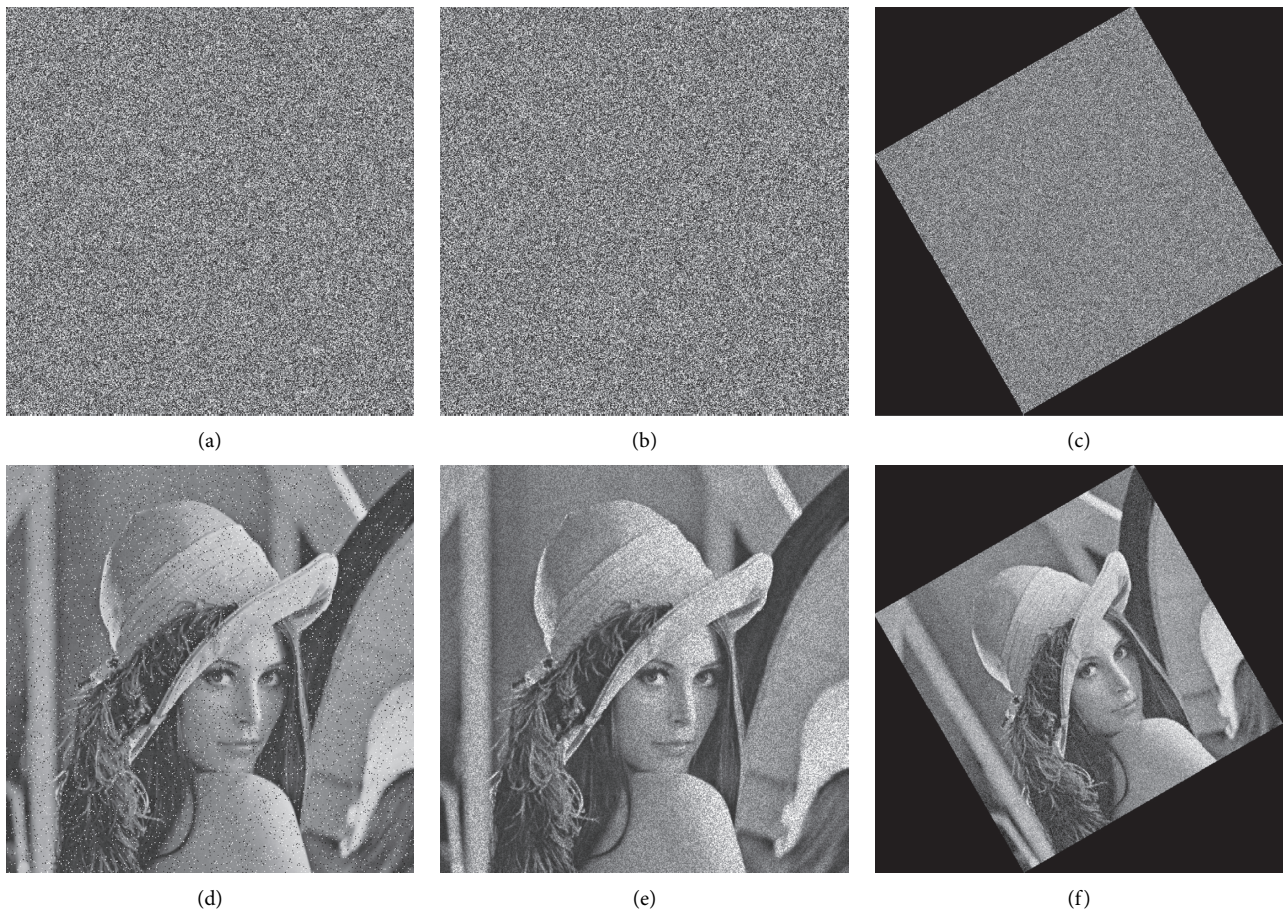


Figure 17: The effect of speckle noise attack: (a) encrypted picture with 5% salt & pepper noise; (b) encrypted picture with 4% speckle noise; (c) cipher picture with 2% Gaussian commotion and turn of 30°; (d) decrypted image with 5% salt & pepper noise; (e) decrypted image with 4% speckle noise; and (f) decrypted image with 2% Gaussian noise and turn of 30°.

Table 3: The NPCR (%) of encrypted images for our approach compared with other literature algorithms. Please note that NA stands for "not applicable."

Image name	Proposed method	Wu et al. [11]	Ben Slimane et al. [13]	Wang et al. [35]	Luo and Ge [36]	Amina and Mohamed [37]	Alawida et al. [38]
Lena	99.6641	99.6002	99.6271	99.59	99.6137	99.6452	99.620
Cameraman	99.6523	99.6082	NA	99.59	99.6131	NA	NA
Baboon	99.6438	99.5903	99.6145	99.56	99.6111	99.6154	99.601
Peppers	99.6287	99.6112	NA	99.61	99.6137	99.6315	99.617

Table 4: The UACI (%) of encrypted images for our approach compared with other literature algorithms. Note that NA stands for "not applicable."

Image name	Proposed method	Wu et al. [11]	Ben Slimane et al. [13]	Wang et al. [35]	Luo and Ge [36]	Amina and Mohamed [37]	Alawida et al. [38]
Lena	33.6124	33.5079	33.5589	33.48	33.4594	33.6152	33.505
Cameraman	33.6425	33.5574	NA	33.53	33.4615	NA	NA
Baboon	33.6430	33.5281	33.4277	33.58	33.4629	33.4354	33.424
Peppers	33.6012	33.5265	NA	33.41	33.3948	33.5073	33.391

Moreover, to assess the robustness of the proposed system the statistical analysis is conducted. Table 2 shows measurable analysis of our results; different measures are utilized: MSE, PSNP, ET, and Entropy.

The proposed encryption employs distinctive midpoints when scrambling distinctive input images. This progressively can impressively increment the resistance of the cryptography system against unknown/chosen attacks

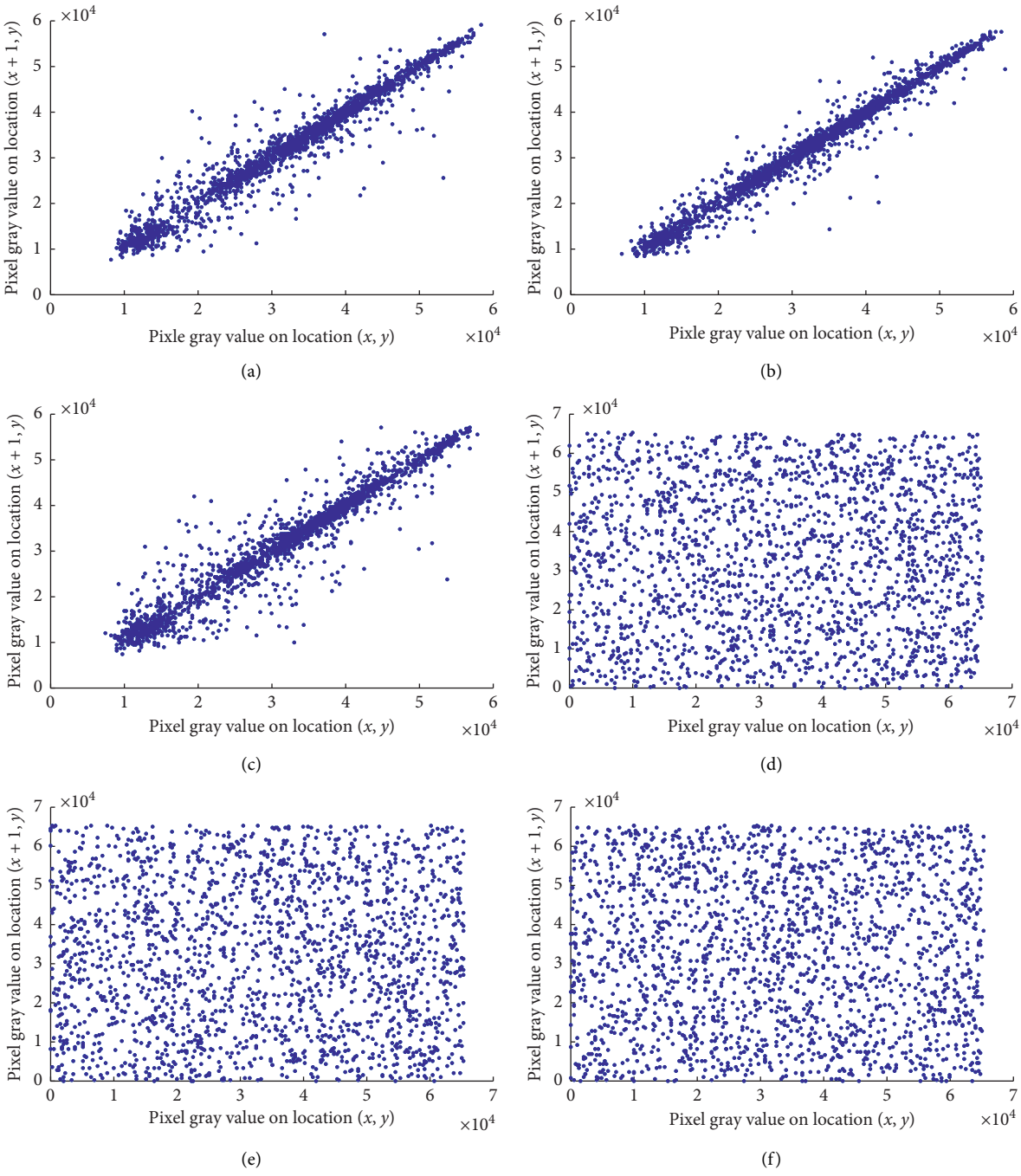


FIGURE 18: Adjacent pixels correlation test for Lena: (a) plain image by horizontal, (b) plain image by vertical, (c) plain image by diagonal, (d) cipher image by horizontal, (e) cipher image by vertical, and (f) cipher image by diagonal.

and differential assaults. Security performance of the proposed algorithm is better than those results mentioned in [34]. In order to test the algorithm's capacity to resist assaults, noise attack may be a common image assault strategy, which frequently happens within preparing of cipher image transmission. For assault analysis, two parameters were used, namely, the NPCR and UACI. The algorithm ought to have great sensitivity to plain image, which means great difference in cipher image caused by a small change in plain image. The effects of salt & pepper, speckle, and composite Gaussian and rotation attack are illustrated in Figure 17. It is concluded that the proposed scheme can resist different assaults (noise attack and rotation attack).

It may be a common form of cryptanalysis and a secure encryption scheme ought to have strong capacity of standing up to these attacks. For an image encryption scheme, by the number of pixels changing rate and bound together normal changed intensity can measure its capacity of standing up to differential attack. The results can be observed in Tables 3

Table 5: Correlation coefficient of the original images and their encrypted images using the proposed chaotic maps.

Image	Direction	Horizontal	Diagonal	Vertical
Lena	Plan image	0.98453	0.97553	0.95271
	Encrypted image	0.00047	0.00305	−0.03911
Cameraman	Plan image	0.92021	0.91321	0.90124
	Encrypted image	0.00212	−0.00205	0.00190
Baboon	Plan image	0.91251	0.9029	0.89215
	Encrypted image	0.00318	−0.00294	0.00285
Peppers	Plan image	0.97543	0.97697	0.95871
	Encrypted image	0.00198	0.02547	0.04321

Table 6: Result of the NIST (SP800) test suite.

Test name		P value	Result
Frequency		0.338753490	Success
Block frequency		0.375654387	Success
Runs ($M = 10.000$)		0.374565348	Success
Long runs of ones		0.334567898	Success
Rank		0.345345266	Success
Spectral DFT		0.464527	Success
No overlapping templates		0.527653	Success
Universal ($L = 7$, $Q = 1280$, $K = 141\ 577$)		0.264534567	Success
Lempel–Ziv complexity		0.565435	Success
Linear complexity		0.384534167	Success
Serial	P value 1	0.492345123	Success
Serial	P value 2	0.424355767	Success
Approximate entropy		0.543556665	Success
Cumulative sums forward		0.345456565	Success
Cumulative sums reverse		0.287662009	Success
Random excursions	$X = -4$	0.535435	Success
	$X = -3$	0.675656	Success
	$X = -2$	0.434521	Success
	$X = -1$	0.429843	Success
	$X = 1$	0.512344	Success
	$X = 2$	0.576545	Success
	$X = 3$	0.496565	Success
	$X = 4$	0.486632	Success

Table 7: Result of DIEHARD tests suite.

Test name	Average value	Result
Birthday spacing	0.524546	Success
Overlapping permutation	0.486766	Success
Binary rank 31×31	0.823667	Success
Binary rank 32×32	0.456273	Success
Binary rank 6×8	0.686388	Success
Bitstream	0.423876	Success
OPSO	0.4601	Success
OQSO	0.5243	Success
DNA	0.5561	Success
Count the ones 01	0.480243	Success
Count the ones 02	0.256778	Success
Parking lot	0.638823	Success
Minimum distance	0.467348	Success
3DS spheres	0.327673	Success
Squeeze	0.536561	Success
Overlapping sum	0.476538	Success
Runs	0.426565	Success
Craps	0.387243	Success

and 4. As can be observed, NPCR is over 99% whereas UACI is over 33%. These results infer the high sensitivity of the proposed calculation towards the miniature modification made to the plain image; the decrypted images will be completely different even if there is only one bit of change between the two plain images. In our test, the results of four encrypted images and the average value UACI and NPCR are 33.6248% and 99.6472%, individually. By differentiation, the values of UACI and NPCR in our plot are closer to the perfect esteem, which proves that it is exceedingly sensitive for the proposed encryption for resisting differential attacks.

5.4. Correlation of Two Adjacent Pixels. Using the sample images above, we compute the correlation coefficients of adjacent pixels for the original and the encrypted image, and this is done through estimating the correlation among two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in the original and the corresponding encrypted images [22]. We randomly select 5000 pairs of two adjacent pixels from the image.

$$\begin{aligned} r_{xy} &= \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \\ \operatorname{cov}(x, y) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right), \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2, \\ E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \end{aligned} \tag{15}$$

where $\operatorname{cov}(x, y)$ represents the covariance of x and y, $D(x)$ represents the variance of the vector x, $E\,\text{vector or}\,(x)$ represents the main value of vector x, and N means the length of the vector x.

As can be seen from Table 5 and Figure 18, the correlation coefficients of the plain images are close to 1, while the correlation coefficients of the cipher images are close to 0. So, the plain images have strong correlations for the adjacent pixels, while the cipher images have hardly any correlations for the adjacent pixels. These demonstrate that our proposed scheme can fight against attacks based on statistical properties of the images.

5.5. Randomness Tests for the Ciphered Image. To guarantee the security of the cryptosystem, the figured picture must have properties to segregate designs for additional measurable investigation, for example, great dispersion (i.e., arrangement's connection gets feeble), extensive stretch (i.e., long key period), and high multifaceted nature and productivity (i.e., disarray and dissemination) [39]. A few tests are ordinarily used to test the haphazardness of the figured picture. These tests incorporate DIEHARD and NIST (SP800) measurable test suites. DIEHARD test is significant on the grounds that it is by all accounts the most remarkable and troublesome test suite to pass [40]. The P estimation of each test must be inside the achievement scope of $0.01 < P$ esteem < 0.99. NIST is a measurable bundle comprising a lot of tests. These tests were created to test the haphazardness of the ciphered image dependent on the pseudorandom number generators. Tables 6 and 7 show the consequences of the NIST and DIEHARD; the outcomes show that ciphered images have passed all the assessments, which implies that they exhibit highly random behavior.

6. Conclusion

A set of novel chaotic maps based on DWT and double chaotic function have been proposed in an effort to improve encryption quality and execution. In such a way, the proposed pipeline was able to avoid many existing cryptanalysis methodologies and cryptography attacks. This has been documented using the NPCR and UACI metrics with values of 99.6472% and 33.6248%, individually. The dynamical analysis and sample entropy algorithms showed that the proposed map is overall hyperchaotic with the high sensitivity and high complexity. Thus, the proposed chaos-based image cipher can be seen as reasonable tool for applications like wireless communications. There are a few research focuses that can follow after this investigation. The key choice handle can be randomized. The number of offers superimposed can be expanded to increase the layers of security. Different sorts of chaotic maps can be connected to the same image to improve the encryption handle. The proposed chaotic maps for multimedia security algorithms can be applied based on chaotic system for fog computing.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Al, S. Najim, and E. Hato, "A speech encryption based on chaotic maps," *International Journal of Computer Applications*, vol. 93, no. 4, pp. 19–28, 2014.

[2] A. S. Menon and K. S. Sarila, "Image encryption based on chaotic algorithms: an overview," *International Journal of Science, Engineering and Technology Research*, vol. 2, no. 6, pp. 1328–1332, 2013.

[3] C. Li, G. Luo, and C. Li, "An image encryption scheme based on the three-dimensional chaotic logistic map," *IJ Network Security*, vol. 21, no. 1, pp. 22–29, 2019.

[4] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new beta chaotic maps," *Optics and Lasers in Engineering*, vol. 96, pp. 39–49, 2017.

[5] 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.

[6] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-box," *Information Sciences*, vol. 450, pp. 361–377, 2018.

[7] X. L. Aqeel-ur-Rehman, X. Liao, and M. A. R. Hahsmi, "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.

[8] C.-Y. Song, Y.-L. Qiao, and X.-Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3329–3334, 2013.

[9] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Applied Soft Computing*, vol. 11, no. 1, pp. 514–522, 2011.

[10] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Optics & Laser Technology*, vol. 101, pp. 30–41, 2018.

[11] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, 2018.

[12] N. B. Slimane, N. Aouf, K. Bouallegue, and M. Machhout, "An efficient nested chaotic image encryption algorithm based on DNA sequence," *International Journal of Modern Physics C*, vol. 29, no. 7, Article ID 1850058, 2018.

[13] N. Ben Slimane, K. Bouallegue, and M. Machhout, "Designing a multi-scroll chaotic system by operating logistic map with fractal process," *Nonlinear Dynamics*, vol. 88, no. 3, pp. 1655–1675, 2017.

[14] S. Su, Y. Su, and M. Xu, "Comparisons of firefly algorithm with chaotic maps," *Computer Modelling & New Technologies*, vol. 18, no. 12, pp. 326–332, 2014.

[15] N. Ramadan, "Chaos-based image encryption using an improved quadratic chaotic map," *American Journal of Signal Processing*, vol. 6, no. 1, pp. 1–13, 2016.

[16] A. Kenfack, "Bifurcation structure of two coupled periodically driven double-well duffing oscillators," *Chaos, Solitons & Fractals*, vol. 15, no. 2, pp. 205–218, 2003.

[17] L. Wang and H. Cheng, "Pseudo-random number generator based on logistic chaotic system," *Entropy*, vol. 21, no. 10, p. 960, 2019.

[18] M. Ausloos and M. Dirickx, Eds., *The Logistic Map and the Route to Chaos: From the Beginnings to Modern Applications*, Springer, Berlin, Germany, 2006.

[19] M. Ahmad, M. N. Doja, and M. M. S. Beg, "A new chaotic map based secure and efficient pseudo-random bit sequence generation," *International Symposium on Security in Computing and Communication*, Springer, Berlin, Germany, 2018.

[20] B. Toufik and N. Mokhtar, "The wavelet transform for image processing applications," *Advances in Wavelet Theory and Their Applications in Engineering, Physics and Technology*, vol. 17, pp. 395–422, 2012.

[21] E. A. Albahrani and T. Karam Alshekly, "New chaotic substation and permutation method for image encryption," *International Journal of Applied Information Systems*, vol. 12, no. 4, pp. 34–39, 2017.

[22] G. Hanchinamani and L. Kulakarni, "Image encryption based on 2-D zaslavskii chaotic map and pseudo Hadmard transform," *International Journal of Hybrid Information Technology*, vol. 7, no. 4, pp. 185–200, 2014.

[23] M. A. Mohamed, A. S. Samrah, A. M. Abu Taleb, and M. G. Abdel-Fattah, "Development of hybrid encryption-watermarking techniques of multimedia," Master thesis, Faculty of Engineering, Mansoura University, Mansoura, Egypt, 2015.

[24] J. D. Dieu, "A fast image encryption algorithm based on chaotic maps and the linear diophantine equation," *Computer Science and Applications*, vol. 1, no. 4, pp. 232–243, 2014.

[25] W. Pratt, *Digital Image Processing*, John Wiley & Sons Inc., New York, NY, USA, 3rd edition, 2001.

[26] V. Aslantas, L. A. Dog¢an, and S. Ozturk, "DWT-SVD based image watermarking using particle swarm optimizer," in *Proceedings of the IEEE International Conference on Multimedia Expo*, pp. 241–244, Hannover, Germany, April 2008.

[27] R. Enayatifar, "Image encryption via logistic map function and heap tree," *International Journal of the Physical Sciences*, vol. 6, no. 2, pp. 221–228, 2011.

[28] K. Gupta and S. Silakari, "Efficient hybrid image cryptosystem using ECC and chaotic map," *International Journal of Computer Applications*, vol. 29, no. 3, pp. 1–13, 2011.

[29] O. Boubaker and S. Jafari, *Recent Advances in Chaotic Systems and Synchronization: From Theory to Real World Applications*, Academic Press, Cambridge, MA, USA, 2018.

[30] J. Wang and X. Li, "A chaotic system with one line equilibria and image encryption with avalanche effects," in *Proceedings of the 2015 International Conference on Electronics, Electrical Engineering and Information Science-EEEIS2015*, World Scientific Publishing Co., Inc., Guangzhou, China, 2016.

[31] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons & Fractals*, vol. 26, no. 1, pp. 117–129, 2005.

[32] Y. Feng, L. Li, and F. Huang, "A symmetric image encryption approach based on line maps," in *Proceedings of the 2006 1st International Symposium on Systems and Control in Aerospace and Astronautics*, IEEE, Harbin, China, January 2006.

[33] A. Akshahani, S. Behnia, A. Akhavan, S. C. Lim, and Z. Hassan, "An image encryption approach using quantum chaotic map," in *Proceedings of the Second International Conference on Advances in Computer and Information Technology-ACIT 2013*, Kuala Lumpur, Malaysia, 2013.

[34] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on hash function with only two-round diffusion process," *Multimedia Systems*, vol. 20, no. 1, pp. 45–64, 2014.

[35] X. Wang, S. Wang, N. Wei, and Y. Zhang, "A novel chaotic image encryption scheme based on hash function and cyclic shift," *IETE Technical Review*, vol. 36, no. 1, pp. 39–48, 2019.

[36] H. Luo and B. Ge, "Image encryption based on Henon chaotic system with nonlinear term," *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 34323–34352, 2019.

[37] 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.

[38] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.

[39] O. M. Al-Hazaimeh, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Computing and Applications*, vol. 31, no. 7, pp. 2395–2405, 2017.

[40] T. Sobh, *Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics*, Springer, Berlin, Germany, 2008.