Hindawi
Complexity
Volume 2022, Article ID 3676265, 20 pages
https://doi.org/10.1155/2022/3676265

Research Article

Fast and Robust Image Encryption Scheme Based on Quantum Logistic Map and Hyperchaotic System

Nehal Abd El-Salam Mohamed,[1] **Aliaa Youssif**,[2] **and Hala Abdel-Galil El-Sayed**[3]

[1]*College of Information Technology, Misr University for Science & Technology (MUST), 6th of October City 77, Egypt*
[2]*College of Computing and Information Technology, Arab Academy for Science, Technology and Maritime Transport, Smart Village 12577, Egypt*
[3]*College of Computers and Artificial Intelligence, Helwan University, Ain Helwan (Helwan University Building), Helwan 11795, Egypt*

Correspondence should be addressed to Nehal Abd El-Salam Mohamed; nehal.mohamed@must.edu.eg

Received 7 October 2021; Revised 9 February 2022; Accepted 14 February 2022; Published 29 March 2022

Academic Editor: Ahmed A. Abd El-Latif

Topic of quantum chaos has begun to draw increasing attention in recent years. So, to ensure the security of digital image, an image encryption algorithm based on combining a hyperchaotic system and quantum 3D logistic map is proposed. This algorithm is applied in four stages. Initially, the key generator builds upon the foundation of mean for any row or column of the edges of the plain image. Its output value is used to yield initial conditions and parameters of the proposed image encryption scheme. Next, it diffuses the plain image by the random sequences generated by 3D hyperchaotic system, and the diffusion process is realized by implementing XOR operation. Then, the diffused image and chaotic sequences are produced by the 3D quantum chaotic logistic map, expressed as a quantum superposition state using density matrix which is a representation of the state of a quantum system, and finally the resulting quantum image is then confused and diffused simultaneously by a unitary matrix generated by logistic chaos using XNOR operation to obtain the final cipher image. Because of the dependence on the plain image, the algorithm can frustrate the chosen-plaintext and known-plaintext attacks. Simulation results and theoretical analysis verify that the presented scheme has high safety performance, a good encryption effect, and a large key space. The method can effectively resist exhaustive, statistical, and differential attacks. Moreover, the encryption time of the proposed method is satisfactory, and the method can be efficiently used in practice for the secure transmission of image information.

1. Introduction

In today's era [1–6], with the fast development of electronic technology and the scale of the communication network, a lot happens over a time of one minute. Along with this rapid development of Internet and multimedia, usage of digital media has increased tremendously in past decades. In this period of digital data technology, today, we are in the sphere of digitally advanced era, where most of the private data and secure digital information is being exchanged by the help of electronic media such as television, smartphones, personal computers, tablets, facsimiles, satellites, and so forth to all corners of the world over just one minute to facilitate the daily needs of people where digital information is being applied in all the fields in the society.

Images originated in some scenarios such as any social media servers, business, personal privacy, healthcare or military systems, organizations, banks, and other private sectors contain private information which is placed and maintained in very big databases, since it can be transmitted, shared, and stored on the Internet, so if this information is stolen or an unauthorized person accesses it, this may cause a serious damage and serious consequences to any organization [7–9].

With the widespread application of a digital image, providing digital image information security in the

transmission channel has become an increasingly serious issue to be urgently solved because the data can be intercepted, cracked, or destroyed [10, 11]. Hence, the security of the important and valuable image information has become a hot recent topic of the field of information security.

Image encryption [5, 12, 13] is one of the possible effective solutions used to protect these images from this threat where it is extensively recognized as a useful technique for secure transmission and its objective is to accomplish privacy and integrity of data. It converts images into noise-like encrypted images with key by disrupting pixel positions or changing pixel values and decryption will reveal the original message or information by utilizing same key utilized for encryption.

To satisfy the emerging demand, a lot of useful image encryption algorithms based on optical transformation, DNA sequence operations, wave motion, Brownian motion, cellular automata, compressive sensing, and chaotic system [6, 14] were developed in literature to secure these digital images.

Since the chaos theory was first proposed by Lorenz, many chaotic phenomena were found in many fields, such as physics, astronomy, chemistry, biology, and medicine. In 1998, Fridrich firstly proposed a chaos-based image encryption algorithm composed of two stages: permutation and diffusion. After that, many scholars have designed numerous efficient algorithms for chaotic systems and chaos-based image encryption to be applied for the secure communications [3, 4, 8, 11].

Chaotic systems [2, 4] have many noteworthy features which satisfy the requirements of image encryption, such as random-like behaviors, high sensitivity to initial conditions and control parameters where the wrong initial condition will lead to nonchaotic behavior, nonperiodicity, and ergodicity, and low cost in the computer operation system and microprocessor [8–10]. Therefore, these systems can be rapidly applied to cryptographic systems which achieve superior performance with respect to the trade-offs between the security and efficiency. However, the appearance of quantum computing brought a great challenge to classic encryption methods [15, 16].

Additionally, with the advancement in technology in the modern era of computer world, brute-force attack [4, 6] will be quite easily performed in quantum computers which are based on quantum information theory. This vulnerability gives potential danger to idealized security required at national security and protected innovation level. To beat this threat, it is necessary to study novel and safer cryptosystem to meet the current safety requirements in image encryption, and, therefore, quantum encryption can be applied in the image encryption process as it gives us a secure encryption method.

Quantum computation [7, 17, 18] has shown great potential for improving information processing speed and enhancing communication security. Combining quantum computing and image encryption is a secure and effective approach to design the encryption algorithms. The essence task of quantum image encryption is to store the images into quantum computers, and then quantum encryption techniques can be exploited to process these images. Due to the promising prospect of quantum image encryption, more and more researchers devoted their attention to developing quantum image representation models and designing image encryption algorithms.

For example, Li et al. [3] proposed an efficient chaos-based image encryption scheme, which uses the imitating jigsaw method containing revolving and shifting operations and shows good performance in both security and speed. Liu et al. [7] proposed a quantum image encryption algorithm based on bit-plane permutation and sine logistic map which has good performance in the aspect of security and the computational complexity is superior to its classical counterpart. Dong et al. [9] proposed a self-adaptive image encryption algorithm based on the quantum logistic map, which can achieve secure communications and frustrate the chosen-plaintext and known-plaintext attacks. In [15], an innovative quantum color image encryption method focused on the Lucas series-based substitution box is suggested to enhance the competence of encryption. This cryptosystem has more excellent key space and significant confidentiality. In [19], an image encryption algorithm based on 3D DNA level permutation and substitution scheme is proposed, where the proposed encryption scheme has large key space and high key sensitivity and may resist some typical attacks, and it may effectively secure the secret image information. El-Latif et al. [20] presented a new method for constructing substitution boxes (S-boxes) based on cascaded quantum-inspired quantum walks and chaos inducement, which will offer gains in many cryptographic applications where the performance of the proposed S-box scheme is investigated via established S-box evaluation criterion and outcomes suggest that the constructed S-box has significant qualities for viable applications information security. In [21], a new method for the encryption by utilizing quantum chaotic maps and continuous chaotic dynamical systems is designed which contributes to achieving the security of data with the minimum time of encryption. Sridevi and Philominathan [22] presented a quantum encryption technique which is built by adopting Haar Integer Wavelet Transform (HIWT), RC6 (Rivest Cipher) block cipher, and DNA (deoxyribonucleic acid) sequences. In addition, a Unified Chaotic Logistic Tent Map (ULTM) has been employed in the permutation phase to produce the pseudorandom sequence for shuffling the RGB planes of the quantum represented source image in spatial and transform domains. This cryptosystem has confirmed the significant immune level of the quantum cryptosystem. In [23], an enhanced quantum scheme is proposed for generalized novel enhanced quantum image representation which has good visual effects and high security. Wen et al. [24] proposed an image cryptosystem adopting a quantum chaotic map and the certain security-enhanced mechanisms where the cryptosystem has excellent performance and can resist various cryptographic attacks. Moreover, the feasibility and effectiveness of the image cryptosystem are verified on the Internet of Things secure communication experimental platform. It proves that the proposed image cryptosystem is a preferred and promising secure communication technology solution.

After conducting a detailed analysis of the breaking methods, it was found that some chaos-based image encryption schemes have security vulnerabilities, which are as follows: (1) key dependence and fixed key; (2) one cycle of permutation-diffusion architecture; (3) low-dimensional systems used for image encryption; (4) single chaotic system still used for encryption operation, which leads to inability to resist brute-force attack; and (5) low sensitivity to all the chaotic secret keys.

To overcome these security shortcomings and design secure and effective image encryption, an image encryption algorithm based on integrating a hyperchaotic system and quantum 3D logistic map is presented in this paper. The essence goals of the proposed scheme are listed as follows:

(i) First, it can fight against the chosen-/known-plaintext attacks due to the use of symmetric key image cryptosystem based on original image.

(ii) Second, the generated key cryptosystem based on the plain image is used to determine the number of cycles of composite chaotic algorithms.

(iii) Third, multidimensional chaotic maps like hyperchaos and 3D quantum logistic map are used which have more chaotic attractors, so the high-dimensional chaotic system has stronger randomness, better confidentiality, greater amount of information, and higher communication efficiency, providing sufficiently large key space and having high security.

(iv) Fourth, two different chaotic systems (quantum logistic map and hyperchaotic Chen's system) are combined, which have the advantage of excellent random sequence to expand the key space, enhance the performance of resisting brute-force attack, and achieve better encryption effect and high level of security.

(v) Fifth, high sensitivity with respect to all secret keys is achieved, which leads to creating a completely different cipher image when applied to the same plain image whenever flipping one bit in a key.

Based on the above literature, it is evident that, for generating excellent encryption effects and producing a highly secure encryption scheme, it is needed to design a combination of hyper- and multidimensional chaotic systems through density matrix which describes the quantum state of a system.

2. Preliminary Knowledge

2.1. Chen's Hyperchaotic System. In order to improve the security and efficiency performance, many image encryption methods based on three-dimensional chaotic systems, hyperchaos, and even spatiotemporal chaos have been presented in recent years [25].

In 1963, Lorenz [26] found the first chaotic attractor in a three-dimensional autonomous system:

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = cx - xz - y, \\ \dot{z} = xy - bz, \end{cases} \tag{1}$$

where a, b, and c are constant parameters of the system. Typically, when $a = 10$, $b = 8/3$, and $c = 28$, the system is in a chaotic state.

In 1999, Chen [27] discovered another chaotic system with more complex dynamic behaviors than Lorenz system when studying chaotic feedback control. Chen's hyperchaotic system is defined as follows:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1), \\ \dot{x}_2 = -x_1x_3 + dx_1 + cx_2 - x_4, \\ \dot{x}_3 = x_1x_2 - bx_3, \\ \dot{x}_4 = x_1 + k, \end{cases} \tag{2}$$

where a, b, c, d, and k are the system parameters. In this system, when the values of the parameters $(a, b, c, d, k) = (36, 3, 28, -16, -0.7 < k < 0.7)$, the system is hyperchaotic in a very wide parameter range in this case and has many more interesting complex dynamical behaviors than those of Lorenz system. The hyperchaos attractors of this system are shown in Figure 1, while the corresponding bifurcation diagram of state x with respect to k is given in Figure 2.

Its Lyapunov exponents are $\lambda_1 = 1.552$, $\lambda_2 = 0.023, \lambda_3 = 0, \lambda_4 = -12.573$; Lyapunov exponents for this system are depicted in Figure 3. As the hyperchaos has four positive Lyapunov exponents, the prediction time of a hyperchaotic system is shorter than that of a chaotic system [28]; as a result, it is safer than chaos in security algorithm.

2.2. 3D Quantum Logistic Chaotic Map. Quantum chaotic systems are the quantized of classical chaotic system, such as quantum logistic map which [1, 29, 30] is constructed by the classical logistic system and that is a perfect example of complex chaotic maps which arises from nonlinear dynamical equations. Classical chaotic maps have a small range for key space as they suffer from low control parameters which in turn lead to a limited chaotic range, whereas the chaotic maps with higher dimensional as the used one in the proposed scheme can be lead to increase the key space range, have excessive complexity, high degree of randomness, and high sensitivity to initial conditions and control parameters. Therefore, quantum logistic system is suitable as seed system in encryption algorithm.

Based on the classical logistic map and the effect of quantum correlations on a dissipative system [31], the proposed quantum logistic map was applied to image encryption, which can be defined as follows:

$$\begin{aligned} x_{n+1} &= r\left(x_n - |x_n|^2\right) - ry_n, \\ y_{n+1} &= -y_n e^{-2\beta} + e^{-\beta} r\left[\left(2 - x_n - x_n^*\right)y_n - x_n z_n^* - x_n^* z_n\right], \\ z_{n+1} &= -z_n e^{-2\beta} + e^{-\beta} r\left[2\left(1 - x_n^*\right)z_n - 2x_n y_n - x_n\right], \end{aligned} \tag{3}$$

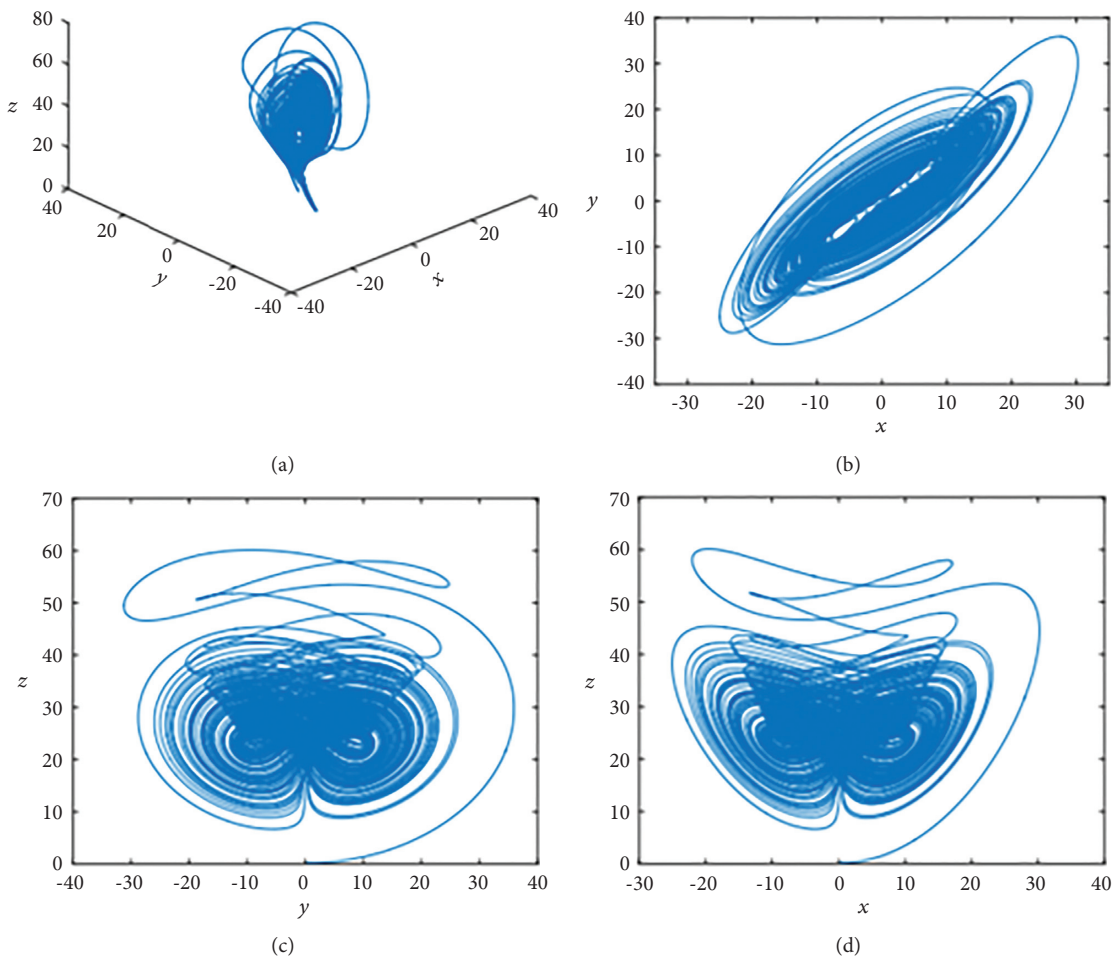

Figure 1: $x - yx - z$Figure 1Hyperchaos attractors of Chen's chaotic system: (a) Distribution in the direction of x-y-z. (b) Plane graph of x-y. (c) Plane graph of y-z. (d) Plane graph of x-z.

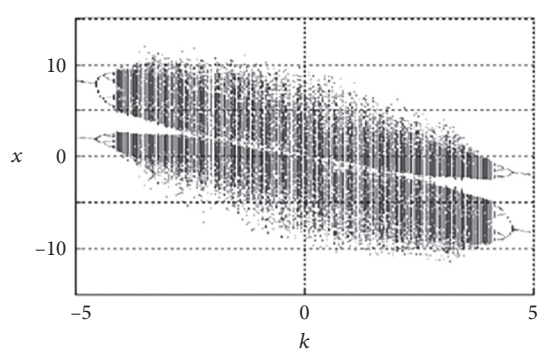

Figure 2: Bifurcation diagram of Chen's chaotic system with parameter k.

where β is dissipation parameter and γ represents control parameter. However, the initial conditions (x_n, y_n, z_n) are set as real numbers to meet the requirement of communication. Figure 3 shows the phase diagram of quantum logistic map, and its bifurcation diagram is displayed in Figure 4.

3. The Proposed Image Encryption and Decryption Scheme

3.1. Image Encryption Process. This section presents the details of the design of the proposed method based on the adopted fundamental Fridrich's permutation-diffusion model,

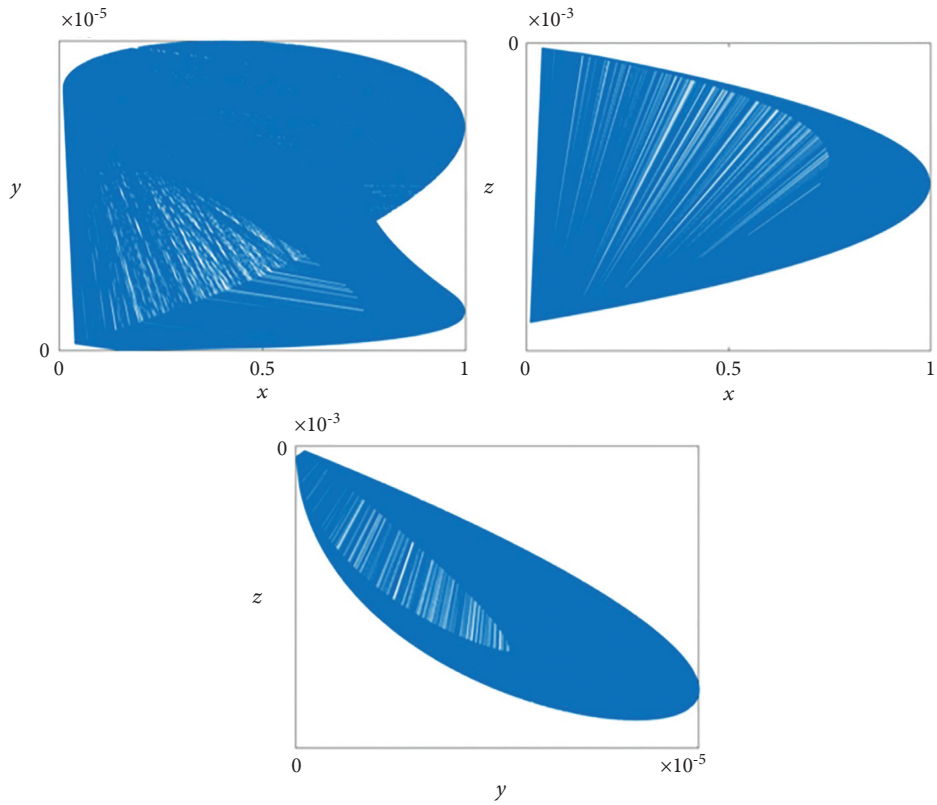

Figure 3: Phase diagram of quantum logistic map.

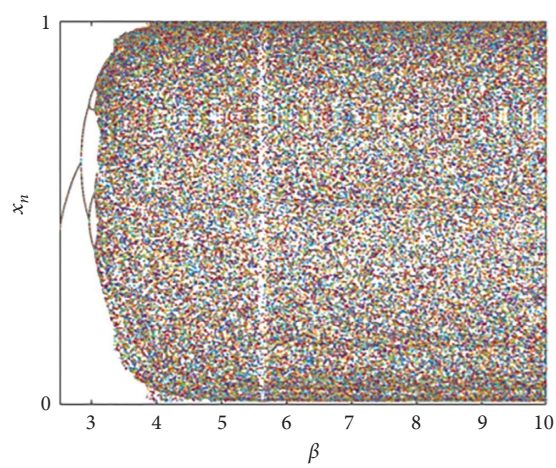

Figure 4: Bifurcation diagram of quantum logistic map.

hyperchaotic system, and a 3D quantum logistic mapping. The proposed algorithm is designed in the context of sensitive information of digital color and gray images. Consider a color image I with size $W \times H$, where W and H represent the image's rows and columns, respectively. The R, G, and B components of I are denoted as R, G, and B, respectively. The proposed framework consists of four main phases, and the details of these phases are presented as follows:

(i) The first phase is key extraction from a plain image through computing the mean of any of the four edges of the plain image and then utilizing that mean to make a number of iterations for both Chen's hyperchaotic system and the quantum logistic map in order to modify the initial seeds and control parameters for them.

(ii) Iterate continuously Chen's hyperchaotic system $W \times H$ times to generate a random sequence of integers E_I whose values range from [0...255], where the length of sequence E_I, that is, n, will be equal to the number of pixels in the image. Then split it into three chaotic sequences E_i^R, E_i^G, E_i^B which are computed using the following equations:

$$\begin{aligned} E_i^R(i,j) &= \text{unit8}\Big(\text{round}\Big(\text{mod}\Big((abs(x) - \text{floor}(abs(x))) * 10^{(14)}, 256\Big)\Big)\Big), \\ E_i^G(i,j) &= \text{unit8}\Big(\text{round}\Big(\text{mod}\Big((abs(y) - \text{floor}(abs(y))) * 10^{(14)}, 256\Big)\Big)\Big), \\ E_i^B(i,j) &= \text{unit8}\Big(\text{round}\Big(\text{mod}\Big((abs(z) - \text{floor}(abs(z))) * 10^{(14)}, 256\Big)\Big)\Big), \end{aligned} \tag{4}$$

where $i = 1, 2, \ldots, W \times H$.

(iii) Diffuse three components of the plain image by the random sequences generated by 3D hyperchaotic system to obtain their corresponding cipher sequences. The diffusion process is performed by implementing XOR operation as follows:

$$\begin{aligned} C_i^R &= P_i^R \oplus E_i^R, \\ C_i^G &= P_i^G \oplus E_i^G, \\ C_i^B &= P_i^B \oplus E_i^B. \end{aligned} \tag{5}$$

(iv) Perform quantum logistic map to produce a chaotic sequence Q_i; after that separate it into three channels Q_i^R, Q_i^G, Q_i^B which can be calculated as follows:

$$\begin{aligned} Q_i^R &= \text{mod}(\text{floor}(\varepsilon_1 * x_{i+1} + \varepsilon_2), 256), \quad i = 1, 2, \ldots, W \times H, \\ Q_i^G &= \text{mod}(\text{floor}(\varepsilon_1 * y_{i+1} + \varepsilon_2), 256), \quad i = 1, 2, \ldots, W \times H, \\ Q_i^B &= \text{mod}(\text{floor}(\varepsilon_1 * z_{i+1} + \varepsilon_2), 256), \quad i = 1, 2, \ldots, W \times H, \end{aligned} \tag{6}$$

where $(\varepsilon_1, \varepsilon_2)$ are two large prime numbers and $(x_{i+1}, y_{i+1}, \text{and}\, z_{i+1})$ are random sequences which are generated by 3D quantum logistic map (3).

(v) Generate density matrix H using the following equations:

$$\begin{aligned} H_{11} &= (p + (1-p)) * \left(\cos\left(\frac{a}{2}\right)^2\right), \\ H_{12} &= (1-p) * \left(\sin\left(\frac{a}{2}\right) * * \cos\left(\frac{a}{2}\right)\right), \\ H_{21} &= (1-p) * \left(\sin\left(\frac{a}{2}\right) * \cos\left(\frac{a}{2}\right)\right), \\ H_{22} &= (1-p) * \left(\sin\left(\frac{a}{2}\right)^2\right), \end{aligned} \tag{7}$$

where p is probability and a is angle.

(vi) The diffused layers (C_i^R, C_i^G, C_i^B) and chaotic sequences are produced by the 3D chaotic logistic map (Q_i^R, Q_i^G, Q_i^B) which are expressed as a quantum superposition state, using the XNOR function as follows:

$$\begin{aligned} \text{SC}_i^R &= \overline{C_i^R \oplus H}, \\ \text{SC}_i^G &= \overline{C_i^G \oplus H}, \\ \text{SC}_i^B &= \overline{C_i^B \oplus H}, \\ \text{SQ}_i^B &= \overline{Q_i^B \oplus H}, \\ \text{SQ}_i^B &= \overline{Q_i^B \oplus H}, \\ \text{SQ}_i^B &= \overline{Q_i^B \oplus H}, \end{aligned} \tag{8}$$

where operator $\overline{\oplus}$ denotes bitwise exclusive NOR.

(vii) Finally, the final cipher channels $\text{FC}_i^R, \text{FC}_i^G, \text{FC}_i^B$ are obtained by applying XNOR function on both a unitary matrix generated by logistic chaos $(\text{SQ}_i^R, \text{SQ}_i^G, \text{SQ}_i^B)$ and the diffused components $(\text{SC}_i^R, \text{SC}_i^G, \text{SC}_i^B)$ generated density matrix to confuse and diffuse pixels simultaneously, which can be expressed as follows:

$$\begin{aligned} \text{FC}_i^R &= \overline{\text{SC}_i^R \oplus \text{SQ}_i^R}, \\ \text{FC}_i^G &= \overline{\text{SC}_i^G \oplus \text{SQ}_i^G}, \\ \text{FC}_i^B &= \overline{\text{SC}_i^B \oplus \text{SQ}_i^B}. \end{aligned} \tag{9}$$

(viii) Combine (FC_i^R, FC_i^G, and FC_i^B) into a chaotic matrix FC_i with transpose rows and columns of the border of the image to get the final cipher image $C_{W\times H}$.

The sketch of the proposed encryption scheme is exhibited in Figure 5 with a succinct explanation of each phase presented herewith while the specific implementation process of the proposed image encryption scheme is presented in Algorithm 1.

3.2. Decryption Method. The architecture of the proposed decryption algorithm is shown in Figure 6, which is applied on a cipher image to produce a plain image.

4. Experimental Results and Numerical Analysis

Due to the absence of a practical and functional quantum computer, the experimental results are performed with MATLAB R2017b platform on a classical computer to verify the security and effectiveness of the proposed quantum image encryption algorithm. The operation system used is Windows 10 Professional operating system with the specific configuration being i7-8550U applied as the central processing unit (CPU) and the random-access memory (RAM) adopted is 8 GB.

For simulation, the control parameters and initial values of Chen's hyperchaotic system, given in (2), are set as $a = 36$, $b = 3$, $c = 28$, and $d = -16$, and $x_0 = 0.3$, $y_0 = -0.4$, $z_0 = 1.2$, and $q = 1$, we carry out the encryption scheme. The keys for this proposed cryptosystem include the iteration times of Chen's hyperchaotic system and quantum logistic chaotic map M, where the discarded number M is set according to the mean of plain image. For color images, the encryption key is the same in RGB channels.

To demonstrate the practical benefits of the proposed image encryption scheme, a number of experiments were performed based on the USC-SIPI (the University of Southern California Signal and Image Processing Institute) Image Database [32]. This database is divided into four groups of images: Textures (64 images), Aerials (38 images), Miscellaneous (39 images), and Sequences (69 images). Each group contains images of various sizes $m \times m$, $m = 256$, 512, 1024. Different sample images (gray and color) are chosen as test images from the USC-SIPI "Miscellaneous" dataset and the simulation results of these encryption and decryption images are presented in Figure 7, where the plain images of "Aerial," "Boat," "Male," "Airplane," "Lena," and "Baboon" are shown in Figures 7(a)–7(f), their corresponding cipher images are shown in Figures 7(g)–7(l), and the recovery images from decryption process with correct secret keys are shown in Figures 7(m)–7(r) which are identical to the original images, and their detailed information is listed in Table 1.

As illustrated in Figures 7(g)–7(l) that the proposed encryption scheme can encrypt different size images, besides that it destroys the obvious pattern of the plain image and makes the ciphered image display a space filling with a noise-like pattern which makes the ciphered image seem random to the intruder. Therefore, the proposed encryption algorithm has good encryption and decryption effect; it can attain the image data security and appearance security. The quantitative performance of the newly resulted image encryption algorithm could be measured through different evaluation parameters, including statistical, differential, sensitivity, and key space metrics. Each of these measures is discussed in detail in the accompanying subsections.

4.1. Key Space Analysis. The key space of a cryptosystem is the very important factor on security when brute-force attack is happening. For high-security cryptosystem, it should be highly sensitive to a tiny change in the cryptographic keys and the key space is suggested to be much larger than 2^{100} to resist exhaustive attack effectively [33–36]. Moreover, the keys should be easy to establish and exchange for practical communication. The key space is the total number of different keys that can be used in the encryption/decryption procedure. According to the algorithm structure, the secret key format should consist of the following: (1) The parameters of Chen's hyperchaotic system are a, b, c, d, and k and each of the original variables (x_1, x_2, x_3, x_4) has 2 decimal places; there exist 10^2 possible values for each value. This contributes to 6 possible guesses of value. This applies to (a, b, c, d, k, x_1, x_2, x_3, x_4) as well. Thus, there are 2^{54} possible values of (a, b, c, d, k, x_1, x_2, x_3, x_4). (2) The initial values of hyperchaotic system (x_1, x_2, x_3) are obtained by iterating system; each has 14 decimal places with the range between 0 and 1, and there exist 10^{14} possible values for each value. This contributes to $2^{46.5}$ possible guesses of value. This applies to (x_1, x_2, x_3) as well. Thus, there are $2^{139.5}$ possible values of (x_1, x_2, x_3). (3) Parameters β and r are used in the quantum logistic chaotic map, where β consists of 4 decimal places; there exist 10^4 possible values for each value. This contributes to 2^{12} possible guesses of its value and r consists of 2 decimal places, and there exist 10^2 possible values for each value. This contributes to 2^6 possible guesses of its value. Thus, there are 2^{18} possible values of β and r. (4) Each initial value of quantum map consists of 12 decimal places with the range between 0 and 1; there exist 10^{12} possible values for each value. This contributes to 2^{40} possible guesses of value. This applies to (x_0, y_0, z_0) as well. Thus, there are 2^{120} possible values of x_0, y_0, and z_0. (5) Two large prime numbers are of 8 decimal places with the range between 0 and 1; there exist 10^8 possible values for each value. This contributes to 2^{26} possible guesses of value. This applies to $(\varepsilon_1, \varepsilon_2)$ as well. Thus, there are 2^{52} possible values of $(\varepsilon_1, \varepsilon_2)$. (6) Density matrix has probability p and an angle a, where p has only one decimal place with the range between 0 and 1, and a has 2 decimal places; thus there exist 10^1 possible values for p; this contributes to 2^3 possible guesses of value, whereas there exist 10^2 possible values for a; this contributes to 2^6 possible guesses of value. This contributes to 2^{10} possible guesses of value. Thus, there are 2^9 possible values of (p, a).

Consequently, the overall key space of the proposed image encryption scheme is

$$\begin{aligned}\text{TOTAL KEY SPACE} &= 2^{54} * 2^{18} * 2^{139.5} * 2^{120} * 2^{52} * 2^{9}\\ &= 2^{54+139.5+120+52+20}\\ &= 2^{392.5}.\end{aligned} \tag{10}$$

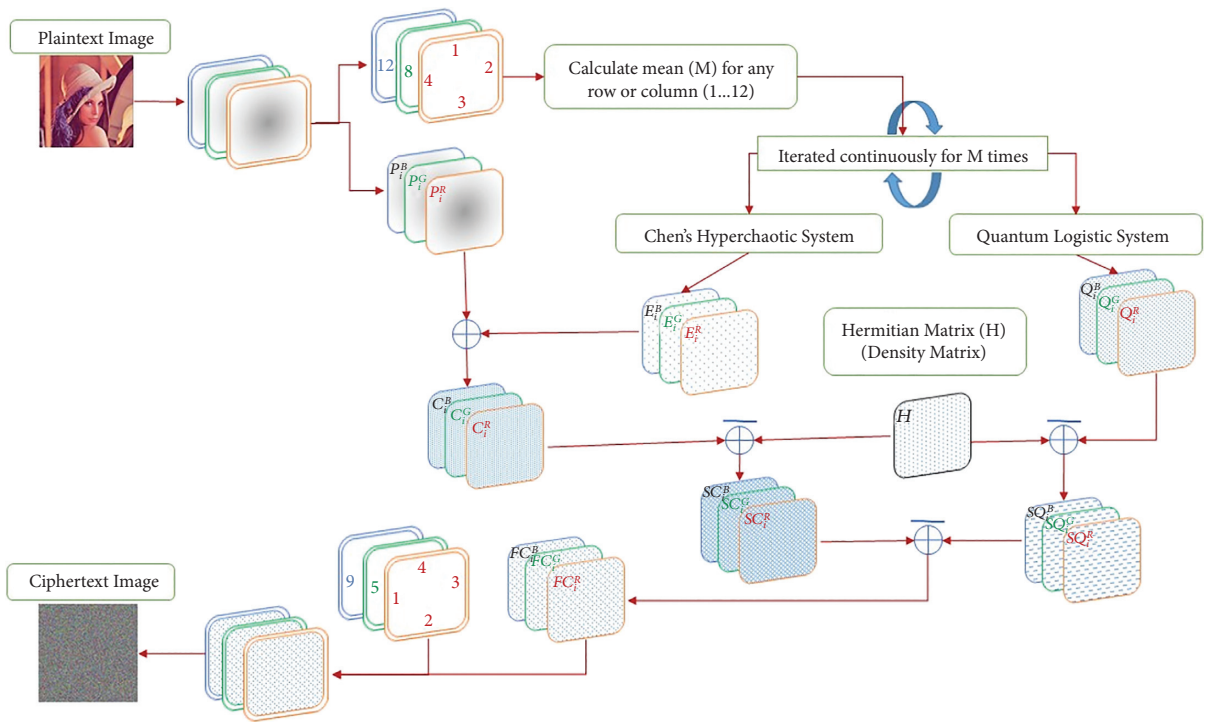

Figure 5: Block diagram of the proposed image encryption algorithm.

Input: Plain Image P of size $W \times H$, initial conditions and control parameters for hyperchaotic system (3D Chen's system), and seeds for the chaotic generator.
Output: Cipher Image C of size $W \times H$
Step 1: Plain image P is resized to a dimension of $((W-2) \times (H-2))$ pixels and is stored as P_2, and compute the mean M of any of the edges of the plain image P.
Step 2: Iterate both Chen's hyperchaotic system (equation (2)) and quantum logistic map (equation (3)) M times according to the computed mean M.
Step 3: Generate three chaotic sequences E_i^R, E_i^G, E_i^B by using a hyperchaotic system with given parameters and initial state values as secret keys.
Step 4: Separate each of the color pixel $P_i \in P_2$ of the resized image P_2 into its three grayscale components of P_i^R, P_i^G, P_i^B, then apply XOR function between three components P_i^R, P_i^G, P_i^B of the resized image P_2 and three chaotic sequences E_i^R, E_i^G, E_i^B produced by chen's hyperchaotic system. The result is considered as diffused R, G, and B components, which are C_i^R, C_i^G, C_i^B.
Step 5: Quantum logistic map is initiated and utilized to generate a chaotic keystream sequence Q_i, after that split it into R, G, and B components Q_i^R, Q_i^G, Q_i^B.
Step 6: Generate Density matrix which is described as Hermitian matrix $H_{W-2\times H-2}$.
Step 7: Employ Density matrix on the diffusion components (C_i^R, C_i^G, C_i^B), as well as the output of quantum logistic map (Q_i^R, Q_i^G, Q_i^B) using XNOR function to put each of them in a superposition environment.
Step 8: The three components of the cipher image FC_i^R, FC_i^G, FC_i^B are generated by XNORing the output of applying density matrix on the diffused components (SC_i^R, SC_i^G, SC_i^B), and quantum logistic map (SQ_i^R, SQ_i^G, SQ_i^B).
Step 9: Take transpose of the edges of the plain image P in order to increase the randomness within the plain image by shuffling the pixels.
Step 10: Recombine the cipher image FC with the shuffled edges of the plain image P to obtain the final cipher image C.

Algorithm 1: Image encryption method.

As a result, the key space is reasonably large enough for the cryptosystem to withstand exhaustive attacks and even quantum computer attacks. Table 2 shows the key space comparison of similar recent algorithms. Obviously, the proposed encryption algorithm has larger key compared to the existing works [4, 15, 24, 35, 37], which is sufficiently large to resist all presently known brute-force attacks.

4.2. Key Sensitivity Analysis. To resist violent attacks, a password system should be highly sensitive. Hence, key sensitivity [37–40] is an important index to measure the strength of encryption algorithm. The key sensitivity of an image cryptosystem can be evaluated in two aspects: First, the cipher image will be completely different when encrypting the same plain image with slightly different keys,

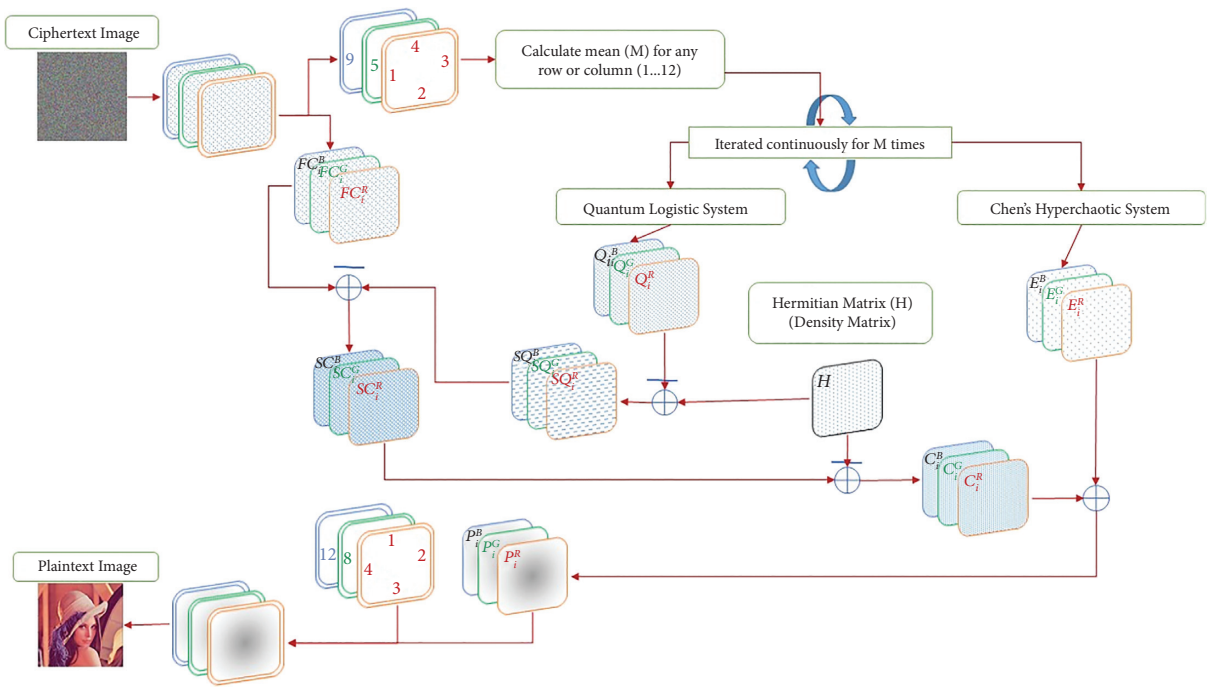

Figure 6: Block diagram of the proposed image decryption algorithm.

Input: Cipher Image C of size $W \times H$
Output: Decrypted Image P of size $W \times H$
Steps: Inverse steps of image encryption routine are carried out in the reverse order using the same encryption keys.

Algorithm 2: Image decryption method.

which is measured by the change rate t of the cipher image. Second, a small change in the decryption key makes a huge difference to the result, and the original image will not be decrypted correctly, indicating that the algorithm has a high sensitivity. The Lena color image with size 512×512 is utilized to verify the sensitivity of the suggested image encryption scheme. During the test process, one of the keys has undergone a tiny change, while other keys were kept untouched. Suppose that K_1 and K_2 are the two keys that are slightly different from each other, which gives encrypted outputs of E_1 and E_2, respectively, where K_1 is the correct key and K_2 is the wrong one. In the proposed cryptosystem, the control parameters of Chen's hyperchaos system are set as $a = 36$, $b = 3$, $c = 28$, and $d = -16$, and the initial values of the system are $x_0 = 0.3$, $y_0 = -0.4$, $z_0 = 1.2$, and $q = 1$, which are denoted as K_1, to obtain encrypted image E_1. Another encrypted image E_2 is generated with a tiny change in only x_0 ($x_0 = 0.4$, $y_0 = -0.4$, $z_0 = 1.2$, and $q = 1$), which are denoted as K_2. As shown in Figures 8(b) and 8(c), the image encrypted using K_1 is completely different from the image encrypted using K_2. From the result, as shown in Figures 8(e) and 8(f), it is clear that decryption of the encrypted image is possible only when we use the same key. Therefore, it can be seen that only a subtle difference in the secret key can have a huge effect which guarantees the security against brute-force attacks and known plain-text attacks.

4.3. Statistical Attack Analysis. To verify the security performance of the proposed algorithm, the statistical analyses including histogram, correlation, and entropy analysis are demonstrated in this subsection.

4.3.1. Histogram Statistical Analysis. Histogram statistical analysis is a kind of statistical attack, and the histogram can characterize the image. It has been widely used in image retrieval, classification, and other fields [41–47]. Image histogram is probability density function of discrete gray level, plotted by gray level on horizontal axis and the corresponding frequency on the vertical. The more uniform the histogram distribution for the encrypted image, the stronger the ability of antistatistical analysis. Therefore, the elimination of correlation among pixels was necessary, and pixels of the encrypted image had to be distributed evenly to prevent the opponent from extracting any useful information from the fluctuating histogram. In addition, comparing cipher image histogram with the original image histogram, there is a significant difference.

We have analyzed the histograms of two original images as well as their encryptions using the proposed approach. The histogram of the original grayscale image of "Boat" with dimensions 512×512 pixels and the histogram of its cipher image are shown in Figure 9, while Figure 10 illustrates the

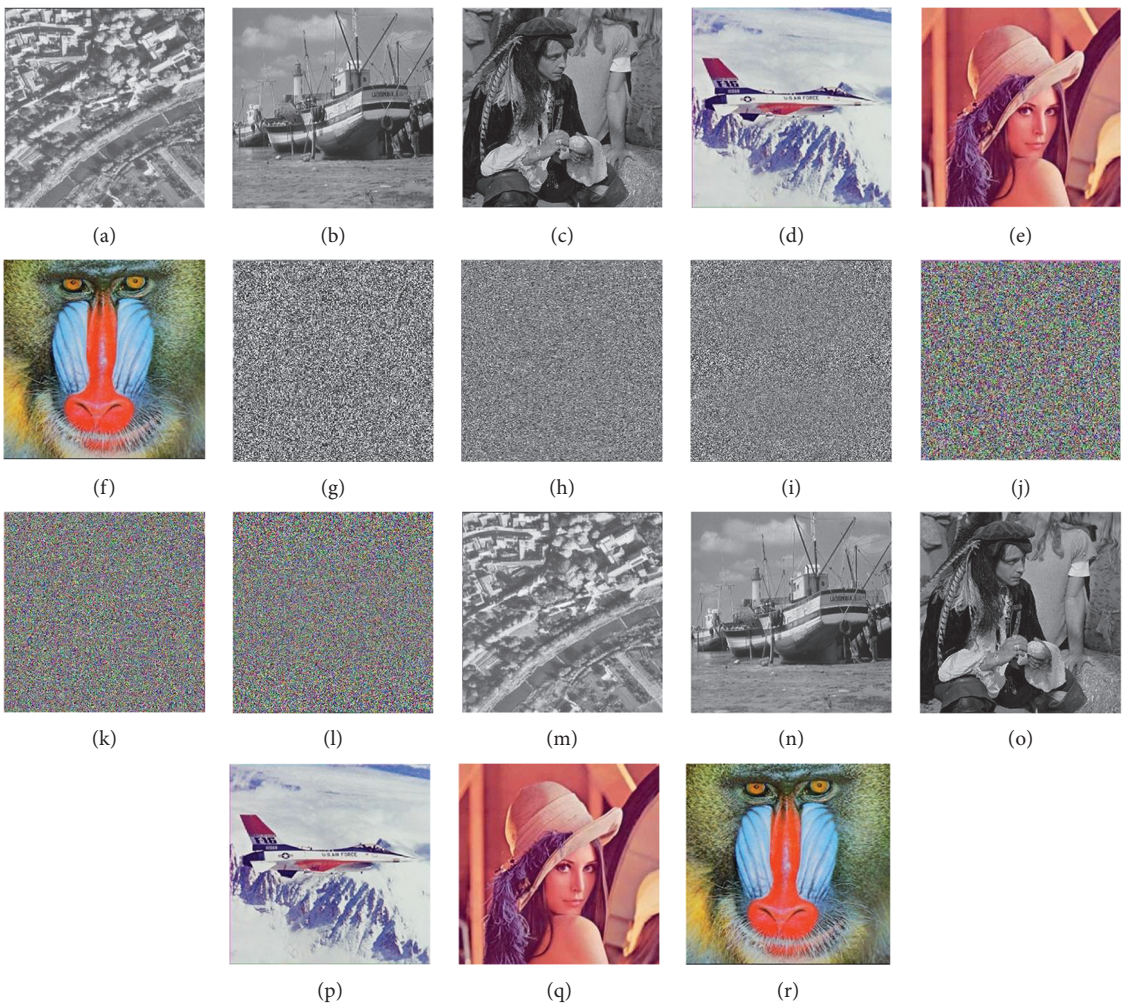

Figure 7: Encryption and decryption results: ((a)–(f)) plain images of "Aerial," "Boat," "Male," "Airplane," "Lena," and "Baboon"; ((g)–(l)) the corresponding encrypted images; and ((m)–(r)) decrypted images.

Table 1: Selected test images.

Image	Aerial	Boat	Male	Airplane	Lena	Baboon
Size	256×256	512×512	1024×1024	256×256	512×512	1024×1024
Type	Grayscale	Grayscale	Grayscale	Color	Color	Color

Table 2: Key space comparative analysis.

Encryption scheme	Key space
Ref. [4]	2^{256}
Ref. [15]	2^{125}
Ref. [24]	$10^{15\times 3} + 2^{256}$
Ref. [35]	2^{186}
Ref. [37]	2^{364}
Proposed algorithm	$2^{392.5}$

histograms of the R, G, and B channels of the color plain image "Lena" alongside its encrypted counterparts with the size 512×512, respectively.

Clearly, it can be seen from Figures 9 and 10 that the histograms of the original images have obvious peaks, and the gray value and RGB component histogram of cipher images are very uniform and flat distribution, which indicates that the attack based on histogram analysis is difficult as attackers cannot use a statistical attack to obtain any useful information by analyzing the histogram of the encrypted image. Thus, the proposed scheme is strong enough to withstand statistical attacks.

Consequently, it is concluded that the proposed image encryption scheme can achieve good performance and meet the requirements of image encryption.

Furthermore, for quantity analyses of the image histogram, a metric called variance of the histogram (var) is measured to evaluate and guarantee the uniformity of pixels values of the encrypted images. The higher the uniformity of ciphered images, the lower the value of variances of

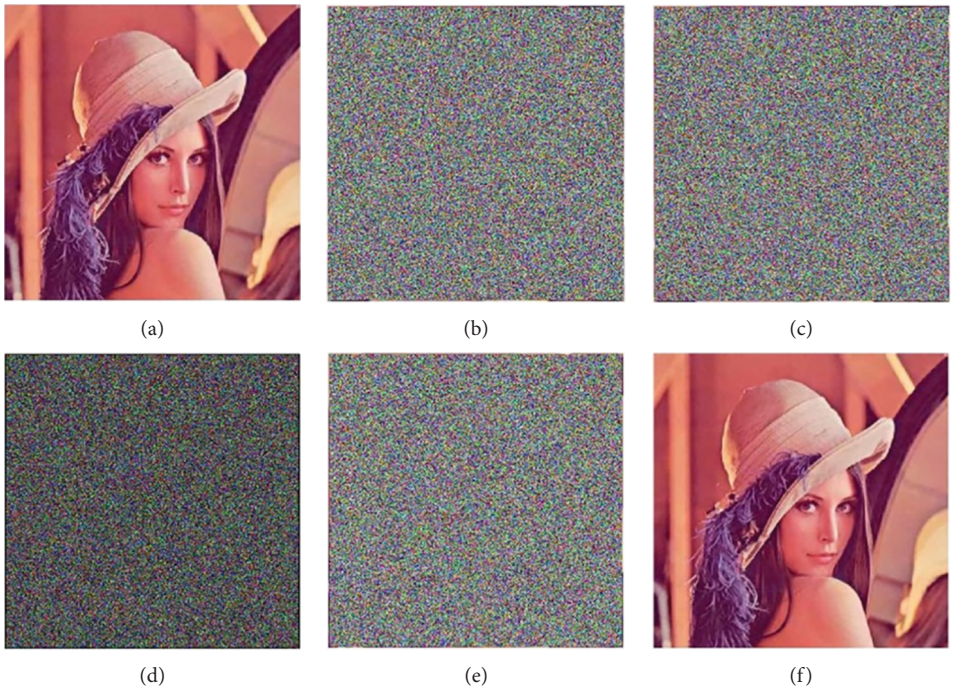

Figure 8: Key sensitivity analysis. (a) Plain image, (b) correctly encrypted image (E_1), (c) incorrectly encrypted image (E_2), (d) difference of E_1 and E_2, (e) incorrectly decrypted image, and (f) correctly decrypted image.

histogram [48]. The variance of histogram can be computed as follows:

$$\operatorname{var}(H) = \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{2} \left(h_i - h_j\right)^2, \tag{11}$$

where $H = \{h_1, h_2, \ldots, h_{256}\}$ is a one-dimensional array of the histogram values; h_i and h_j are considered as the numbers of pixels where gray values are equal to i and j, respectively. Tables 3 and 4 display the values of histogram variance for the experimented grayscale and color images, respectively, and illustrate that the variance of images after encryption is greatly reduced when compared with the variance of those images prior to encryption.

The simulation results indicate that the difference in variance value shows that the histogram depends on the plain image; in addition, the proposed algorithm can strongly withstand statistical analysis attack as it is efficient to prevent attackers from obtaining any useful statistical information to decrypt the cipher image.

4.3.2. Correlation Coefficient Analysis. It is known that some algorithm was broken by using correlation analysis between the adjacent pixels. So, correlation coefficient analysis [49–52] is performed to evaluate the statistical relationship between image pixels, and its value is in the range of [−1, 1]. This type of analysis visually shows the distribution between the neighborhood pixels of both the original and encrypted images.

Due to the intrinsic features of the digital image [53], there is a strong correlation between the adjacent pixels, namely, the gray value of one pixel of the plaintext image is very close to the gray value of the surrounding pixels. Therefore, attackers could try to infer adjacent pixel values based on probability theory. Conversely, in order to resist the statistical attack and achieve better security of the encrypted image, an excellent image encryption algorithm should be able to break high correlation between adjacent pixels of the plain image and produce a very small correlation value near the optimal value of zero.

Normally, three different types of correlation are performed to ensure the strength of the encrypted image: the horizontal, the vertical, and the diagonal correlation [54]. To evaluate the proposed encryption scheme, 3000 pairs of adjacent pixels are selected randomly in the three different adjacent directions in both original and encrypted images of the different sample images to calculate the correlation coefficient. Then, the correlation coefficient r_{xy} of each pair, defined in (12), is calculated as follows:

$$\begin{cases} r_{xy} = \dfrac{\operatorname{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}}, \\[2ex] \operatorname{cov}(x, y) = \dfrac{1}{N} \displaystyle\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right), \\[2ex] D(x) = \dfrac{1}{N} \displaystyle\sum_{i=1}^{N} \left(x_i - E(x)\right)^2, \\[2ex] E(x) = \dfrac{1}{N} \displaystyle\sum_{i=1}^{N} x_i, \end{cases} \tag{12}$$

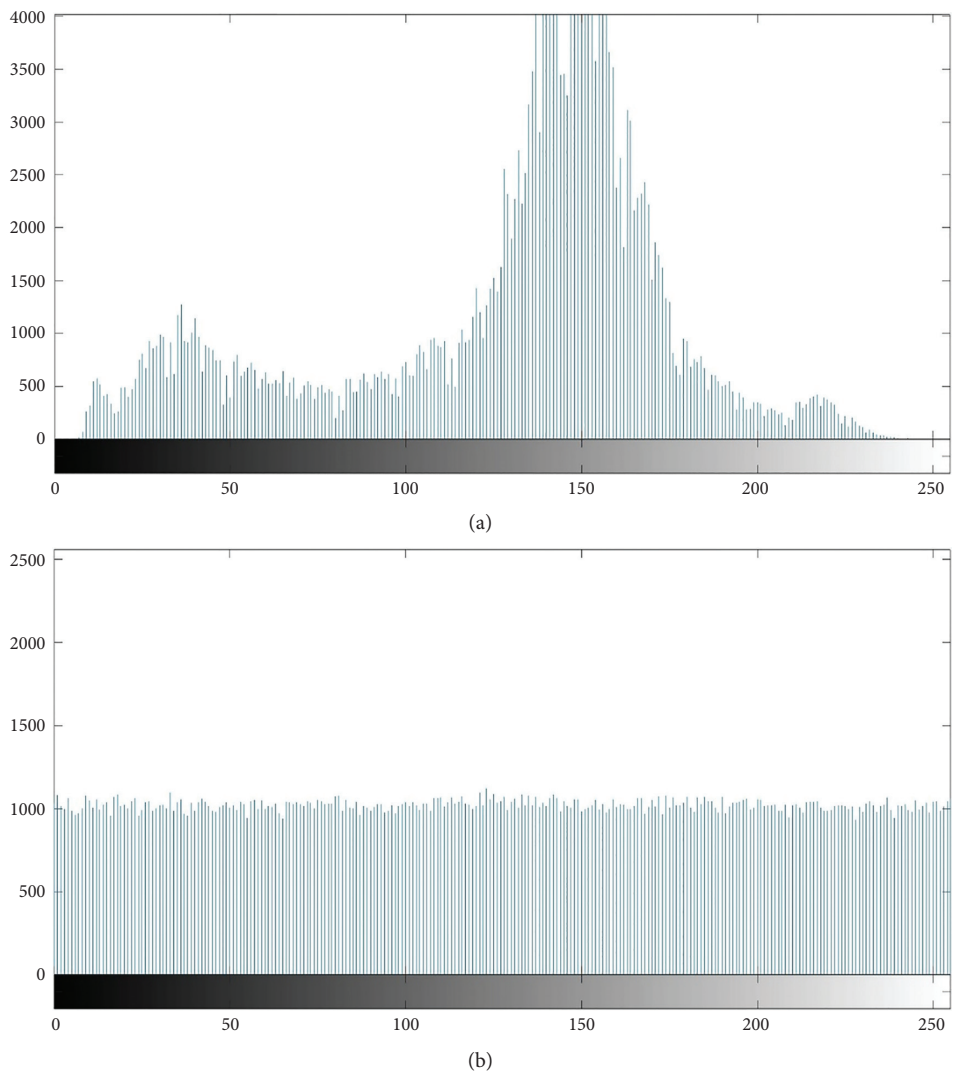

Figure 9: Histogram distribution analysis of plain and encrypted grayscale image. (a) Plain grayscale "Boat" image; (b) encrypted grayscale "Boat" image.

where x_i and y_i are the grayscale pixel values of the ith pair of the selected adjacent pixels in the tested image, N is the total number of the randomized chosen samples, $\mathrm{cov}(x, y)$ is the covariance of x and y, and $E(x)$ and $D(x)$ represent the mean value and the variance of vector x, respectively.

Figures 11 and 12 show the correlation distribution between neighborhood pixels in the three directions of the grayscale "Boat" image and color "Lena" image with size 512×512 before and after image encryption. It is obvious that the correlation of adjacent pixel pairs of the plain image is distributed intensively, but those of encrypted image are scattered randomly which looks very uniform, and the correlation is greatly reduced.

Numerically, Table 5 demonstrates values of correlation coefficient parameter for the proposed technique in different test images with diverse sizes. According to the quantitative results, it can be concluded that the correlation degrees between adjacent pixels in the plain images are close to 1, while those of the encrypted images are very small and are close to 0, which means that the plain image has strong relationships, but weakness exists in the encrypted image. Therefore, these results show that the proposed image encryption scheme has a good performance in fighting against attacks based on statistical properties of the images.

4.3.3. Information Entropy Analysis. Information entropy [55–57] is the most important criterion to evaluate the efficiency of an image encryption algorithm. In information theory, the entropy parameter is considered as the standard to test randomness. For a digital image, information entropy (IE) is one of the outstanding criteria that is usually utilized to evaluate the degree of disorder or randomness of each gray value in the encrypted image and measure the amount of information hidden in an image. The color-level distribution values in an image can also be determined via entropy analysis. Ideally, in the case of 8-bit grayscale image, a robust encryption scheme has an entropy value of 8; otherwise, it

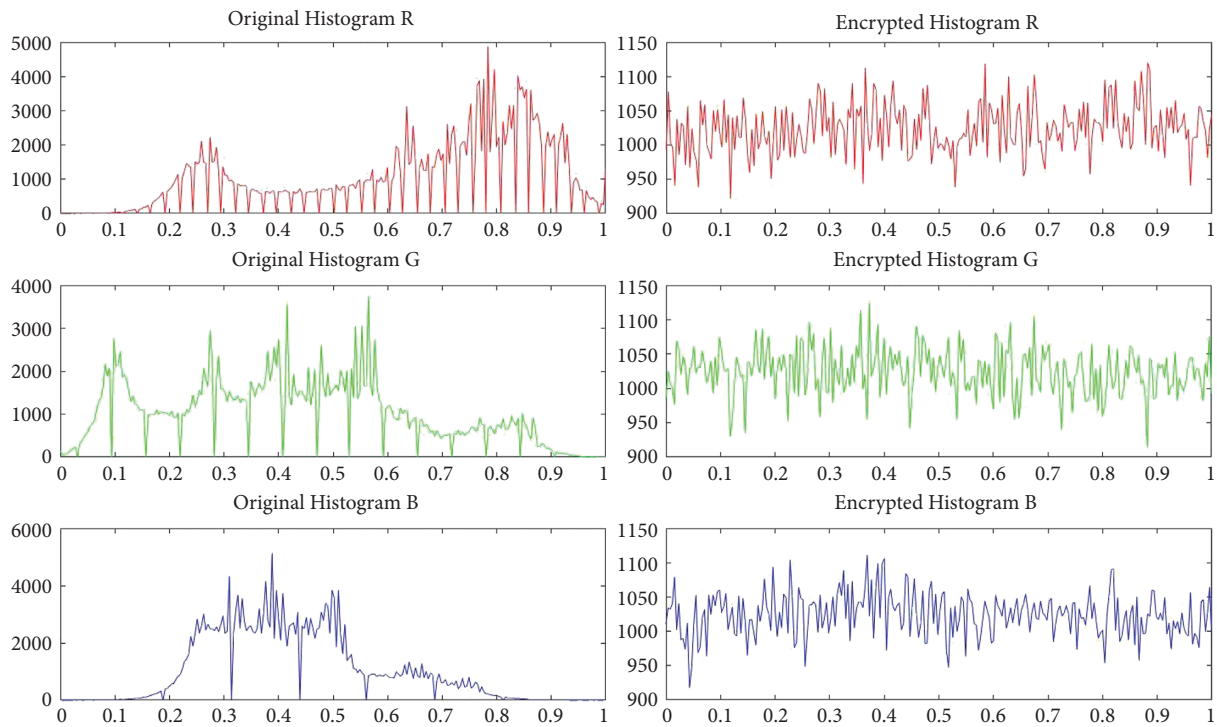

Figure 10: RGB color histogram of original "Lena" image and its corresponding cipher image.

Table 3: Variance of histogram for encrypted grayscale images.

Image name	Variance value	
	Plain image	Cipher image
Aerial	51062	780.8235
Boat	1541901.8039	9791.7098
Male	11393958.6980	138136.8627

Table 4: Variance of histogram for encrypted color images.

Image name	Variance value					
	Plain image			Cipher image		
	R	G	B	R	G	B
Airplane	165621.8980	163801.6941	274155.3333	783.1607	765.4039	796.7137
Lena	1021383.0980	457505.9372	1382757.2627	8929.4431	8930.2823	9570.1019
Baboon	6346579.1843	10106060.6980	5938608.9490	133133.6470	135706.9490	136423.2078

causes a plausibility of consistency which undermines its security. The closer the value is to 8, the greater the uncertainty is and the stronger the randomness of image is, which leads to better-secured encryption where the less visual information can be obtained from the image. The most famous entropy formula is Shannon's entropy equation, calculated in terms of the probability of each available data value, which can be defined as follows:

$$\mathrm{IE} = -\sum_{i=0}^{255} P(i)\log_2 P(i), \tag{13}$$

where $P(i)$ denotes the probability of occurrence of gray level i in an image, that is, the proportion of the number of pixels with gray value i to all pixels in an image. Besides, to verify the randomness, local Shannon entropy should be applied. It can be calculated by the following operations: ① divide the image into noninterlocked K blocks containing a certain fixed number of pixels; ② compute Shannon entropy $\mathrm{IE}(K_i)$ using the former equation (12); ③ calculate the sample mean of global Shannon entropy over all these K image blocks as local Shannon entropy.

Table 6 presents the simulation results of information entropy and local Shannon entropy values, where $K = 16$, on some standard original images and their respective encrypted images, which were encrypted by the proposed image encryption algorithm. It can be seen that the results reveal that the entropy values of each cipher image are very close to the ideal value of 8, while the information entropy of

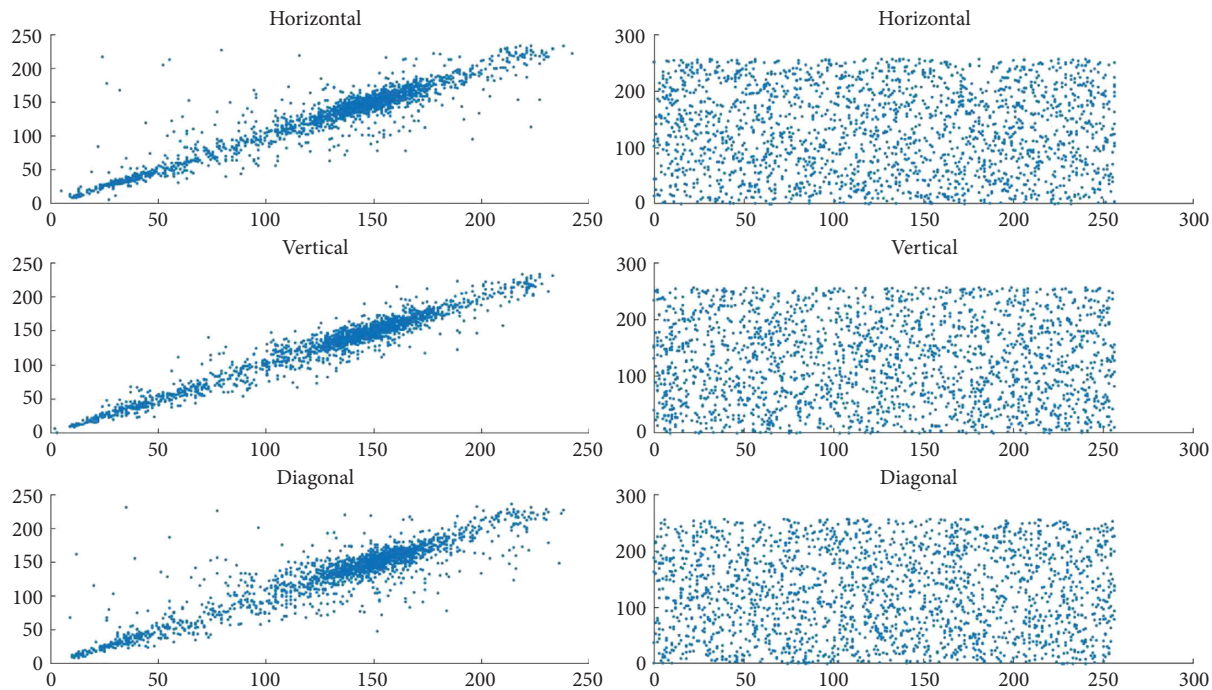

Figure 11: Adjacent pixel correlation test for plain grayscale "Boat" image (a) and the corresponding encrypted image (b) for horizontal, vertical, and diagonal directions.

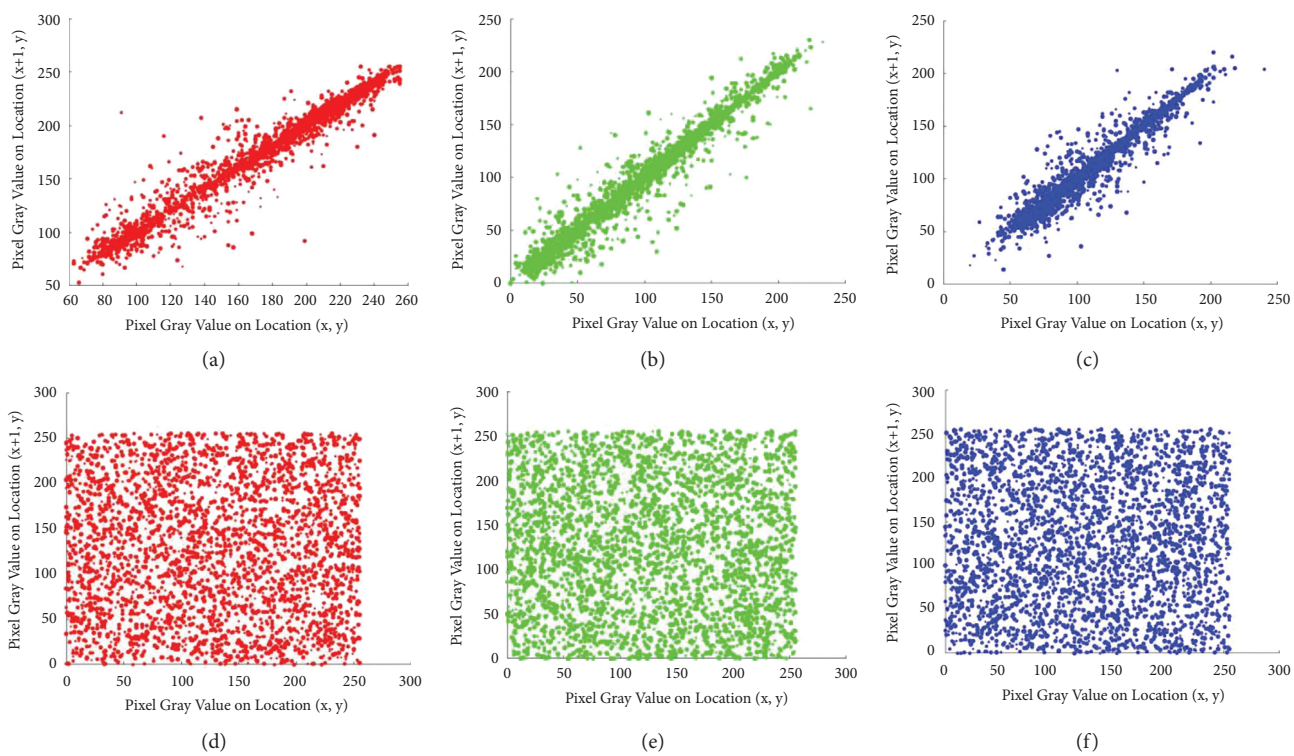

Figure 12: Correlation distribution of color "Lena" image: (a)–(c) show RGB layers of plain image; (d)–(f) show RGB layers of cipher image for vertical, horizontal, and diagonal directions, respectively.

each plain image is much less than the ideal one. This result makes obtaining image information by analyzing this information difficult for attackers. This indicates that the encrypted images have a good randomness. As a conclusion, the proposed scheme is safe against the perspective of information entropy attack.

Table 5: Correlation coefficients results.

Image name	Plain image			Cipher image		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Aerial	0.8602	0.9050	0.8213	0.0062	−0.0017	0.0031
Boat	0.9713	0.9381	0.9222	−0.0012	0.0007	0.0004
Male	0.9813	0.9774	0.9671	0.0001	0.0002	0.0023
Airplane	0.9174	0.9314	0.8643	0.0061	0.0109	0.0012
Lena	0.9902	0.9804	0.9695	0.0040	−0.0003	−0.0012
Baboon	0.9765	0.9877	0.9671	0.0023	0.0012	0.0001

Table 7 presents the values of information entropy of the proposed scheme as compared with the values which resulted from other recent schemes. It can be seen that the information entropy of the different cipher images is very close to 8 bits and the proposed algorithm has greater superiority or in the same range.

4.4. Differential Attack Analysis. Differential attacks are another effective and commonly used cryptanalysis technique. A differential attack is attempted to learn the key and figure out the encryption scheme by tracing differences. An Assailant may make a trivial change in the plain image, encrypt two plain images, and then carry out cryptanalysis by tracing the meaningful relationship between two cipher images. According to the principles of cryptography, the encryption algorithm should be sufficiently sensitive to the changes of plaintext image or secrete key in order to keep high security, such that a minor change in the plaintext image or the initial key parameters causes a significant change in the ciphertext image [59–64]; then differential analysis may become useless. The high sensitivity of the system shows that the generated algorithm is sturdy against any probable attack, since it would indicate no meaningful relationship between the plain image and the cipher image. In this test, the number of pixels changing rate (NPCR) and unified average changing intensity (UACI) become two widely used security analyses in the image encryption community for differential attacks. The tests signify the chance of occurrence of the attack and its sensitivity towards the source image by changing the value.

Considering C_1 and C_2 as the two cipher images obtained from encrypting two one-pixel different images with $M \times N$ size or encrypting same plain image with two secret keys of only 1-bit difference, introduce a bipolar array, D, with the sizes similar to images C_1 and C_2 as follows:

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j), \\ 1, & C_1(i,j) \neq C_2(i,j). \end{cases} \tag{14}$$

The NPCR reflects the change rate of the gray value of different pixels at the same position between two corresponding encrypted images which are obtained by two original images with one-bit difference. In other words, NPCR helps us to understand the effect of change of single pixel over an image, while the UACI reflects the average change of the gray value within the two paired cipher images (C_1 and C_2). Then, the formula used to calculate UACI and NPCR is shown in the two following equations:

$$\text{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\%, \tag{15}$$

$$\text{UACI} = \frac{1}{M \times N}\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1(i,j) - C_2(i,j)\right|}{255}\right) \times 100\%. \tag{16}$$

Taking the images that are listed in Table 1 as examples and experimenting on them for 100 times, the theoretical ideal values of the NPCR and UACI for a gray image are 99.6094% and 33.4635%, respectively. Table 8 lists the test results of NPCR and UACI of grayscale encrypted images, whereas the theoretical values of NPCR and UACI for different color images in three channels are shown in Table 9. It can be observed from the former tables that the proposed image encryption algorithm can achieve better performances against differential attacks, since the values of NPCR and UACI are close to their theoretical values. Thus, the system has guaranteed that the designed system is applicable for real-time communication.

4.5. Known-Plaintext Attack and Chosen-Plaintext Attack Analysis. A cryptosystem is supposed to be secure if it resists all known types of cryptographic attacks. In cryptanalysis, the fundamental assumption enunciated by Kerckhoffs's principle is that encryption and decryption algorithms are known or transparent in a cryptosystem [65–68]. Therefore, the security of the cryptosystem depends on the key rather than the encryption algorithm itself. In the cryptanalysis, there are four traditional cryptanalysis attacks: (1) ciphertext-only attack, (2) known-plaintext attack, (3) chosen-plaintext attack, and (4) chosen-ciphertext attack. Among these attacks, chosen-plaintext attack is the most threatening attack. Therefore, it is claimed that the cryptosystem can resist the other three types of attacks if it can resist the chosen-plaintext attack. In order to assess the resistance of encryption algorithms against the main attacks, two tests are generally used, namely, the known-plaintext attack (KPA) and chosen-plaintext attack (CPA). In known-plaintext attack and chosen-plaintext attack, the attackers usually choose special plaintext and make minor changes to observe the changes of ciphertext. Or they choose some plaintext with linear relationship to observe the characteristics of ciphertext. By using this method, they can obtain secret key. By using this method, they can obtain secret key.

Table 6: Results of information entropy and local Shannon entropy.

Image name	Dimension	Information entropy		Local Shannon entropy	
		Plain image	Cipher image	Plain image	Cipher image
Aerial	256×256	3.3556	7.9970	3.2893	7.9556
Boat	512×512	3.3153	7.9993	3.1037	7.9880
Male	1024×1024	3.3540	7.9998	3.2127	7.9971
Airplane	$256 \times 256 \times 3$	6.6906	7.9987	6.1280	7.9834
Lena	$512 \times 512 \times 3$	7.7495	7.9997	7.3136	7.9959
Baboon	$1024 \times 1024 \times 3$	7.7208	7.9999	7.4281	7.9990

Table 7: Information entropy comparison.

Image name	Dimension	Information entropy				
		Proposed Scheme	Ref. [6]	Ref. [39]	Ref. [58]	Ref. [59]
Aerial	256×256	7.9970	—	—	7.9024	—
Boat	512×512	7.9993	—	7.9993	—	—
Male	1024×1024	7.9998	—	7.9998	—	—
Airplane	$512 \times 512 \times 3$	7.9997	—	—	—	7.9994
Lena	$512 \times 512 \times 3$	7.9997	7.9988	—	—	7.9994
Baboon	$512 \times 512 \times 3$	7.9997	—	—	—	7.9993

Table 8: NPCR and UACI results for cipher grayscale images.

Image name	Image size	NPCR (%)	UACI (%)
Aerial	256×256	99.6458	33.5243
Boat	512×512	99.6517	33.4416
Male	1024×1024	99.6300	33.4864

Table 9: NPCR and UACI scores on color images of different sizes.

Image name	Dimension	NPCR (%)			UACI (%)		
		Red	Green	Blue	Red	Green	Blue
Airplane	$256 \times 256 \times 3$	99.6892	99.6380	99.64113	33.3572	33.5681	33.6369
Lena	$512 \times 512 \times 3$	99.6394	99.6417	99.6574	33.4980	33.4593	33.5460
Baboon	$1024 \times 1024 \times 3$	99.6241	99.6168	99.6238	33.4607	33.4702	33.4707

In the presented encryption scheme, the mean (M) value of the plaintext image is computed to generate the number of preiterations, which is related chaotic sequences generation, and the initial value of diffusion process. In other words, the generated random sequences are related to the plaintext, and the chaotic systems are sensitive to the initial value. Consequently, the keystream used in the proposed algorithm has a high connection with the plain image, which means that a small change in the plaintext image produces a completely different key, as detailed in the "Key Sensitivity Analysis" section. That means the attacker cannot extract any useful information by encrypting certain selected images because the encrypted image is only relevant to the selected image, which implies the excellent performance in withstanding the known-plaintext attack and chosen-plaintext attack.

Besides, to test the ability of defending this kind of attack, both plain images with "pure white" and "pure black" images, their encrypted images, and the corresponding histograms are derived, which are shown in Figure 13. From the results, it can be seen that the pixels in the cipher image are uniformly distributed with random noise, and the attacker cannot decrypt other cipher images by using the same keys. By observing the resulting encrypted images, we can find that it is impossible to extract any information from the encrypted images. Therefore, the proposed encryption scheme is sufficiently robust to resist all forms of potential attacks.

4.6. Time Complexity Analysis. Apart from security analysis of the image encryption scheme, performance analysis is also an important aspect to evaluate the encryption/decryption time and time complexity of the algorithm [69, 70]. A good encryption algorithm needs to have a fast encryption time and low computation complexity.

The encryption/decryption time can be calculated manually where it is mainly analyzed into six parts as follows: (a) mean for any row column of R, G, and B channels, so its complexity is $O(1)$; (b) the cyclic process N times for Chen's hyperchaotic system quantum logistic chaotic map, so it has complexity of $O(n)$; (c) the generation of three chaotic sequences (E^R, E^G, E^G), which are produced by Chen's hyperchaotic system with length $M \times N$ and hence

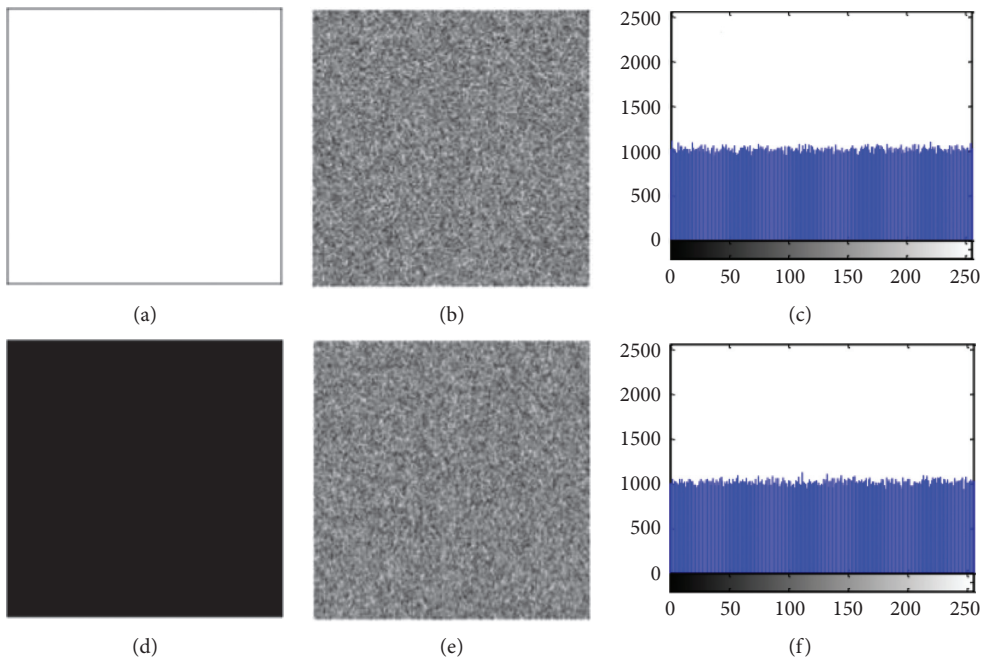

Figure 13: Simulation result of cryptanalysis tests: (a) all white image; (b) cipher image of (a); (c) histogram of (b); (d) all black image; (e) cipher image of (d); (f) histogram of (e).

Table 10: Running time analysis.

Image name	Image size	Encryption/decryption time (s)
Grayscale Aerial	256×256	0.4844
Color Airplane	256×256	0.8125
Grayscale Boat	512×512	1.4375
Color Lena	512×512	3.2969
Grayscale Male	1024×1024	5.7500
Color Baboon	1024×1024	13.6250

Table 11: Speed performance analysis (seconds).

Encryption scheme	Encryption time (s)	Processor speed	RAM	Platform
Ref. [71]	3.45	3 GHz	4 GB	Python 3.6
Ref. [22]	13.90	—	—	MATLAB R2016b
Ref. [72]	1.67	—	—	MATLAB
Ref. [73]	9.36	3.60 GHz	32 GB	MATLAB R2019b
Proposed algorithm	1.11	1.80 GHz	8 GB	MATLAB R2017b

the time cost is $(3 \times M \times N)$; (c) XOR operation having time complexity of $O(1)$; (d) time cost of chaotic map sequences and the generation of random matric being $O(n^2) = \max\{O(1), O(n^2)\}$; (e) the computational cost of density matrix being $O(1)$; and (f) the computational cost of XNOR operation being $O(1)$. From the above analyses, the total time cost of the proposed scheme is $O(n^2)$, so that the time consumption of proposed scheme hinges on t representing the number of code loops.

It can be calculated by using the in-built operations of the software used for implementation. Here, the elapsed time was measured by the tic and toc functions of MATLAB. The running speed of the proposed encryption scheme for a number of standard images with diverse sizes $(M \times M)$ is presented in Table 10. As a result, the proposed scheme reflects the efficiency to be used in practical cases.

Taking the 256×256 "Lena" image as an example, comparative analyses of the execution time among different encryption algorithms are illustrated in Table 11. It is observed that the proposed algorithm runs faster than the referenced algorithms [71–73]. In addition, it has less computational complexity.

5. Conclusion

Complex nonlinearity was preserved by choosing suitable chaotic maps. By choosing a high-dimensional chaotic system, the key space is increased. This study employed a

chaotic quantum logistic map, combining with both confusion and diffusion operations, to propose a new symmetric image encryption algorithm. This algorithm is based on Chen's hyperchaotic system to diffuse image pixels. Among them, the keystreams extracted are different for the same secret key associated with the plain image, which are true random numbers generated from noise arrays. Thus, the presented approach can achieve high resistance to the known-plaintext attack and chosen-plaintext attack as well as high level of sensitivity where the randomness of the random sequence displayed better behavior. At last, to confuse the relationship between original and encrypted images, the transpose process is applied to rows and columns of image. Through the results of extensive experiments and corresponding security analysis, it can be found that the salient features of the proposed symmetric image encryption algorithm can be summarized as follows: (a) large enough key space to resist brute-force attacks, (b) high level of security and being quite worthy of being called a good security system, (c) less computational complexity, and (d) being suitable for applications like wireless communications due to its fast implementation. An actual implementation of different kinds of operations in the scrambling stage to increase the security without affecting drastically the processing time is concerned and more detailed analysis on the chaotic or hyperchaotic dynamical systems deserves further investigation in the near future.

Data Availability

The data that support the findings of this study are openly available in [USC-SIPI Image Database] at [http://sipi.usc.edu/ database/], reference number [32].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] B. Sinha, S. Kumar, and C. Pradhan, "Comparative analysis of color image encryption using 3D chaotic maps," in *Proceedings of the International Conference on Communication and Signal Processing (ICCSP)*, pp. 332–335, Melmaruvathur, India, April 2016.

[2] J. Xu, P. Li, F. Yang, and H. Yan, "High intensity image encryption scheme based on quantum logistic chaotic map and complex hyperchaotic system," *IEEE Access*, vol. 7, pp. 167904–167918, 2019.

[3] Z. Li, C. Peng, W. Tan, and L. Li, "An effective chaos-based image encryption scheme using imitating jigsaw method," *Complexity*, vol. 2021, Article ID 88249115, 18 pages, 2021.

[4] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Scientific Reports*, vol. 10, no. 1, 2020.

[5] R. K. Singh, B. Kumar, D. K. Shaw, and D. A. Khan, "Level by level image compression-encryption algorithm based on quantum chaos map," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 7, pp. 844–851, 2021.

[6] M. Khan and H. M. Waseem, "A novel image encryption scheme based on quantum dynamical spinning and rotations," *PLoS ONE*, vol. 13, no. 11, Article ID e0206460, 2018.

[7] X. Liu, D. Xiao, and C. Liu, "Quantum image encryption algorithm based on bit-plane permutation and sine logistic map," *Quantum Information Processing*, vol. 19, no. 8, pp. 1–23, 2020.

[8] M. Ge and R. Ye, "A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties," *Egyptian Informatics Journal*, vol. 20, no. 1, pp. 45–54, 2019.

[9] Y. Dong, X. Huang, Q. Mei, and Y. Gan, "Self-adaptive image encryption algorithm based on quantum logistic map," *Security and Communication Networks*, vol. 2021, Article ID 66749448, 12 pages, 2021.

[10] H. Liu, B. Zhao, and L. Huang, "Quantum image encryption scheme using arnold transform and S-box scrambling," *Entropy*, vol. 21, no. 4, p. 343, 2019.

[11] Y. Luo, R. Zhou, J. Liu, Y. Cao, and X. Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," *Nonlinear Dynamics*, vol. 93, no. 3, pp. 1165–1181, 2018.

[12] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, vol. 23, no. 3, p. 341, 2021.

[13] Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, "Image encryption with double spiral scans and chaotic maps," *Security and Communication Networks*, vol. 2019, Article ID 8694678, 15 pages, 2019.

[14] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Processing: Image Communication*, vol. 52, pp. 6–19, 2017.

[15] K. K. Butt, G. Li, F. Masood, and S. Khan, "A digital image confidentiality scheme based on pseudo-quantum chaos and Lucas sequence," *Entropy*, vol. 22, no. 11, p. 1276, 2020.

[16] Y. Liu, B. Zhou, Z. Li, J. Deng, and Z. Cai, "An image encryption method based on quantum fourier transformation," *International Journal of Intelligence Science*, vol. 8, no. 3, pp. 75–87, 2018.

[17] X. Liu, D. Xiao, and C. Liu, "Double quantum image encryption based on arnold transform and qubit random rotation," *Entropy*, vol. 20, no. 11, pp. 1–16, 2018.

[18] N. Zhou, X. Yan, H. Liang, X. Tao, and G. Li, "Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system," *Quantum Information Processing*, vol. 17, no. 12, pp. 1–36, 2018.

[19] C. Zhu, Z. Gan, Y. Lu, and X. Chai, "An image encryption algorithm based on 3-D DNA level permutation and substitution scheme," *Multimedia Tools and Applications International Journal*, vol. 17, no. 12, pp. 7227–7258, 2019.

[20] A. A. El-Latif, B. A. El-Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Scientific Reports*, vol. 10, p. 1, 2020.

[21] A. Alghafis, N. Munir, M. Khan, and I. Hussain, "An encryption scheme based on discrete quantum map and continuous chaotic system," *International Journal of Theoretical Physics*, vol. 59, no. 4, pp. 1227–1240, 2020.

[22] R. Sridevi and P. Philominathan, "Quantum colour image encryption algorithm based on DNA and unified logistic tent map," *Information Sciences Letters*, vol. 9, no. 3, pp. 219–231, 2020.

[23] W.-W. Hu, R.-G. Zhou, S. Jiang, X. Liu, and J. Luo, "Quantum image encryption algorithm based on generalized Arnold transform and Logistic map," *CCF Transactions on High Performance Computing*, vol. 2, no. 3, pp. 228–253, 2020.

[24] H. Wen, C. Zhang, P. Chen et al., "A quantum chaotic image cryptosystem and its application in IoT secure communication," *IEEE Access*, vol. 9, pp. 20481–20492, 2021.

[25] X. Wu, Y. Li, and J. Kurths, "A new color image encryption scheme using CML and a fractional-order chaotic system," *PLoS ONE*, vol. 10, no. 3, Article ID e0119660, 2015.

[26] J. Lü and G. Chen, "A new chaotic attractor coined," *International Journal of Bifurcation and Chaos*, vol. 12, no. 3, pp. 659–661, 2002.

[27] R. Zhang, L. Yu, D. Jiang et al., "A novel plaintext-related color image encryption scheme based on cellular neural network and chen's chaotic system," *Symmetry*, vol. 13, no. 3, p. 393, 2021.

[28] A. Z. Mahmoud, *On some new approaches for multimedia content encryption*, Ph.D. dissertation, Dept. Comp. Science, Menoufia Univ., Al Minufya, Egypt, 2015.

[29] X. Liu, D. Xiao, and Y. Xiang, "Quantum image encryption using intra and inter bit permutation based on logistic map," *IEEE Access*, vol. 7, pp. 6937–6946, 2019.

[30] G. Ye, K. Jiao, C. Pan, and X. Huang, "An effective framework for chaotic image encryption based on 3D logistic map," *Security and Communication Networks*, vol. 2018, no. 11, 11 pages, Article ID 8402578, 2018.

[31] Y. He, Y.-Q. Zhang, X. He, and X.-Y. Wang, "A new image encryption algorithm based on the OF-LSTMS and chaotic sequences," *Scientific Reports*, vol. 11, no. 1, pp. 1–22, 2021.

[32] SIPIUSC, "The USC-SIPI image database," 2021, http://sipi.usc.edu/database/.

[33] Y. Zhou, C. Li, W. Li, H. Li, W. Feng, and K. Qian, "Image encryption algorithm with circle index table scrambling and partition diffusion," *Nonlinear Dynamics*, vol. 103, no. 2, pp. 2043–2061, 2021.

[34] X. Yan, X. Wang, and Y. Xian, "Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10949–10983, 2021.

[35] M. Liu and G. Ye, "A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm," *Mathematical Biosciences and Engineering*, vol. 18, no. 4, pp. 3887–3906, 2021.

[36] C. Fu, J.-j. Chen, H. Zou, W.-h. Meng, Y.-f. Zhan, and Y.-w. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," *Optics Express*, vol. 20, no. 3, pp. 2363–2378, 2012.

[37] Y. Wan, S. Gu, and B. Du, "A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding," *Entropy*, vol. 22, no. 2, pp. 1–19, 2020.

[38] K. Jiao, G. Ye, Y. Dong, X. Huang, and J. He, "Image encryption scheme based on a generalized arnold map and RSA algorithm," *Security and Communication Networks*, vol. 2020, pp. 1–14, 2020.

[39] J. Ge, "ALCencryption: A secure and efficient algorithm for medical image encryption," *Computer Modeling in Engineering and Sciences*, vol. 125, no. 3, pp. 1083–1100, 2020.

[40] S. Zhu, C. Zhu, and W. Wang, "A new image encryption algorithm based on chaos and secure hash SHA-256," *Entropy*, vol. 20, no. 9, p. 716, 2018.

[41] X. Zhang, L. Wang, Y. Niu, G. Cui, and S. Geng, "Image encryption algorithm based on the H-fractal and dynamic self-invertible matrix," *Computational Intelligence and Neuroscience*, vol. 2019, no. 12, 12 pages, Article ID 9524080, 2019.

[42] C. Li, F. Zhao, C. Liu, L. Lei, and J. Zhang, "A hyperchaotic color image encryption algorithm and security analysis," *Security and Communication Networks*, vol. 2019, Article ID 8132547, 8 pages, 2019.

[43] H. Fan, K. Zhou, E. Zhang, W. Wen, and M. Li, "Subdata image encryption scheme based on compressive sensing and vector quantization," *Neural Computing & Applications*, vol. 32, no. 16, pp. 12771–12787, 2020.

[44] X. Xue, H. Jin, D. Zhou, and C. Zhou, "Medical image protection algorithm based on deoxyribonucleic acid chain of dynamic length," *Frontiers in Genetics*, vol. 12, pp. 1–18, Article ID 654663, 2021.

[45] S. Zhou, P. He, and N. Kasabov, "A dynamic DNA color image encryption method based on SHA-512," *Entropy*, vol. 22, no. 10, p. 1091, 2020.

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

[47] F. Yang, J. Mou, J. Liu, C. Ma, and H. Yan, "Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application," *Signal Processing*, vol. 169, pp. 1–19, Article ID 107373, 2020.

[48] N. Tsafack, A. M. Iliyasu, N. J. De Dieu et al., "A memristive RLC oscillator dynamics applied to image encryption," *Journal of Information Security and Applications*, vol. 61, Article ID 102944, 2021.

[49] Z. Deng and S. Zhong, "A digital image encryption algorithm based on chaotic mapping," *Journal of Algorithms & Computational Technology*, vol. 13, pp. 1–11, 2019.

[50] J. Zeng and C. Wang, "A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata," *Security and Communication Networks*, vol. 2021, Article ID 6675565, 15 pages, 2021.

[51] L. Ding and Q. Ding, "A novel image encryption scheme based on 2D fractional chaotic map, DWT and 4D hyperchaos," *Electronics*, vol. 9, no. 8, p. 1280, 2020.

[52] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A chaotic-based encryption/decryption framework for secure multimedia communications," *Entropy*, vol. 22, no. 11, p. 1253, 2020.

[53] H. Liu, B. Zhao, J. Zou, L. Huang, and Y. Liu, "A lightweight image encryption algorithm based on message passing and chaotic map," *Security and Communication Networks*, vol. 2020, pp. 1–12, 2020.

[54] N. Sanam, A. Ali, T. Shah, and G. Farooq, "Non-associative algebra redesigning block cipher with color image encryption," *Computers, Materials & Continua*, vol. 67, no. 1, pp. 1–21, 2021.

[55] F. Naz, I. A. Shoukat, R. Ashraf, U. Iqbal, and A. Rauf, "An ASCII based effective and multi-operation image encryption method," *Multimedia Tools and Applications*, vol. 79, no. 31-32, pp. 22107–22129, 2020.

[56] D. W. Ahmed, T. M. Jawad, and L. M. Jawad, "An effective color image encryption scheme based on double piecewise linear chaotic map method and RC4 algorithm," *Journal of Engineering Science & Technology*, vol. 16, no. 2, pp. 1319–1341, 2021.

[57] S. Zhu and C. Zhu, "Security analysis and improvement of an image encryption cryptosystem based on bit plane extraction and multi chaos," *Entropy*, vol. 23, no. 5, p. 505, 2021.

[58] Y. Chen, C. Tang, and Z. Yi, "A novel image encryption scheme based on PWLCM and standard map," *Complexity*, vol. 2020, Article ID 3026972, 23 pages, 2020.
[59] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map," *Entropy*, vol. 22, no. 3, p. 274, 2020.
[60] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Information Sciences*, vol. 546, pp. 1063–1083, 2021.
[61] U. Erkan, A. Toktas, S. Enginoglu, E. Akbacak, and D. N. H. Thanh, "An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN," *Multimedia Tools and Applications*, vol. 81, no. 78, pp. 7365–7391, 2022.
[62] C. Xu, J. Sun, and C. Wang, "A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems," *Multimedia Tools and Applications*, vol. 79, no. 9-10, pp. 5573–5593, 2020.
[63] G. Ye, K. Jiao, X. Huang, B.-M. Goi, and W.-S. Yap, "An image encryption scheme based on public key cryptosystem and quantum logistic map," *Scientific Reports*, vol. 10, no. 1, p. 19, 2020.
[64] M. A. A.-J. A. Mizher, R. Sulaiman, A. M. A. Abdalla, and M. A. A. Mizher, "A simple flexible cryptosystem for meshed 3D objects and images," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 6, pp. 844–851, 2019.
[65] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.
[66] H.-Y. Gu, W.-Q. Yan, and J.-H. Zhang, "A novel image encryption scheme based on hyperchaotic cellular automaton," *Journal of Computers*, vol. 31, no. 6, pp. 155–168, 2020.
[67] Y. Dong, X. Huang, and G. Ye, "Visually meaningful image encryption scheme based on DWT and schur decomposition," *Security and Communication Networks*, vol. 2021, Article ID 6677325, 16 pages, 2021.
[68] L. M. Heucheun Yepdia, A. Tiedeu, and G. Kom, "A robust and fast image encryption scheme based on a mixing technique," *Security and Communication Networks*, vol. 2021, Article ID 6615708, 17 pages, 2021.
[69] B. Mondal, P. K. Behera, and S. Gangopadhyay, "A secure image encryption scheme based on a novel 2D sine-cosine cross-chaotic (SC3) map," *Journal of Real-Time Image Processing*, vol. 18, no. 1, pp. 1–18, 2021.
[70] R. I. Abdelfattah, H. Mohamed, and M. E. Nasr, "Secure image encryption scheme based on DNA and new multi chaotic map," *Journal of Physics: Conference Series*, vol. 1447, no. 1, pp. 1–11, Article ID 012053, 2020.
[71] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12452–12466, 2020.
[72] X. Wang and Y. Su, "Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform," *Scientific Reports*, vol. 10, pp. 1–19, Article ID 18556, 2020.
[73] D. Zhang, L. Chen, and T. Li, "Hyper-chaotic color image encryption based on transformed zigzag diffusion and RNA operation," *Entropy*, vol. 23, no. 3, p. 361, 2021.