Hindawi
Security and Communication Networks
Volume 2021, Article ID 5586959, 18 pages
https://doi.org/10.1155/2021/5586959

Research Article

An Image Encryption Scheme Based on Lorenz Hyperchaotic System and RSA Algorithm

Riguang Lin and Sheng Li

Faculty of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang 524088, China

Correspondence should be addressed to Sheng Li; lish_ls@sina.com

Received 27 January 2021; Revised 31 March 2021; Accepted 7 April 2021; Published 21 April 2021

Academic Editor: Zhiyuan Tan

This research proposes a new image encryption scheme based on Lorenz hyperchaotic system and Rivest–Shamir–Adleman (RSA) algorithm. Firstly, the initial values of the Lorenz hyperchaotic system are generated by RSA algorithm, and the key stream is produced iteratively. In order to change the position and gray value of the pixel, the image data are hidden by additive mode diffusion. Secondly, the diffusion image matrix is reshaped into a one-dimensional image matrix, which is confused without repetition to hide the image data again. Then, the finite field diffusion algorithm is executed to realize the third hiding of the image information. In order to diffuse the pixel information into the entire cipher image, the additive mode diffusion algorithm needs to be looped twice. Finally, the cipher image can be obtained. The experimental results prove that the image encryption scheme proposed in this research is effective and has strong antiattack and key sensitivity. Moreover, the security of this encryption scheme relies on the RSA algorithm, which has high security.

1. Introduction

With the rapid development and popularization of Internet technology, multimedia has become an important means of communication for people. Digital images, as a multimedia resource, are widely used in information communication because they can carry a large amount of information and express the information content intuitively and vividly. In the current big data era, digital images are widely used in various fields, such as business, education, medical research, aerospace, military, and politics. In order to share image information, we can easily transmit it on the Internet by computer or mobile equipment. However, people who are not authorized can also easily obtain the images, and the unauthorized cryptanalysis is a great threat to the information communication of images [1, 2]. More importantly, some images may involve national security and personal privacy, such as satellite reconnaissance or biometric passports. Therefore, the question of how to efficiently protect the security of image communication has attracted great attention from scholars and experts all over the world [2, 3]. Image data are generally different from text data. Classical cryptography provides good encryption algorithms and decryption algorithms for one-dimensional text data, such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard). However, due to the characteristics of digital images, such as large data volume and strong correlation between adjacent pixels, traditional ciphers are not suitable for encrypting images [2].

Accordingly, image encryption algorithms based on technologies such as DNA random coding [4], double random phase coding [5, 6], Arnold transform [7], and chaotic systems [8–10] have been proposed. The chaotic system has superior performance in the field of digital image encryption, which may be attributed to the basic characteristics of the chaotic system, such as sensitivity to initial conditions, pseudorandomness, nonlinearity, and nonperiodicity. As early as 1998, Fridrich [11] proposed a symmetric encryption scheme based on a two-dimensional chaotic map. In this scheme, permutation-diffusion architecture was suggested to encrypt image content, where the permutation operation is performed to alter the positions of

the image pixels, while the diffusion operation is performed to change gray values. Permutation-diffusion mechanism has been widely studied and used in chaotic encryption systems. For instance, a hyperchaos-based image encryption algorithm using pixel-level permutation and bit-level permutation was presented by Li et al. [12], which adopted a 5D multiwing hyperchaotic system, and the key stream generated by hyperchaotic system is related to the original. Ye et al. [2] proposed an efficient pixel-level image encryption algorithm that enhanced the connection between position shuffling for pixels and the change to gray values as compared to the traditional permutation-diffusion architecture. In [13], a novel approach that uses a hyperchaotic system, pixel-level filtering with kernels of variable shapes and parameters, and DNA-level diffusion was designed for image encryption. First, a hyperchaotic system is applied to generating hyperchaotic sequences. Second, dynamic filtering is performed on pixels to change the pixel values. Third, a global bit-level scrambling is conducted to change the values and positions of pixels. Finally, a novel DNA-level diffusion scheme is proposed to further change the image values simultaneously. A new permutation based on bit [14] was implemented into an image encryption algorithm. It is noted that the algorithm [14] employs a "Rubik's cube for bit permutation strategy" to replace the traditional permutation operation. In the diffusion stage, the chaotic map is iterated and bit streams are generated which are then used for diffusion and again chaotic map is used for confusion at pixel level. Unlike the above methods that mainly encrypt gray image, a new color image encryption algorithm was proposed in [15] with a new revised one-dimensional chaotic map. Compared with the traditional one-dimensional chaotic map, the revised one-dimensional chaotic map exhibits better chaotic performances and larger chaotic ranges. Firstly, the method [15] reshapes a color image matrix of size $M \times N$ into an image vector P, with length $3MN$. Then, it produces a permutation position matrix, X', from chaotic sequence X to shuffle pixel positions for P and obtain a permuted image, P'. After that, a diffusion operation for P', using a diffusion matrix D' from X, is taken to achieve C. A rotating function is applied to C in order to get C'. Finally, the cipher image is formed after reshaping C' into a R, G, and B color image.

There are also many other image encryption algorithms [16–23] that have been proposed to protect image information. For example, a parallel image encryption method based on compressive sensing was proposed in [16]. Memristive chaotic system, elementary cellular automata (ECA), and compressive sensing (CS) were designed for image encryption in [17]. To resist the chosen/known plaintext attacks, plaintext-related shuffling was designed for image encryption in [19]; the algorithm mainly includes two plaintext-unrelated diffusion operations and one plaintext-related shuffling. Moreover, generalized Arnold transform and double random phase encoding were introduced for quantum image encryption [20]. In [21], dynamic DNA encryption was used for color image cryptosystem. In order to improve security needs of image content, the method [23] of encryption scheme combines the techniques of chaotic image encryption and DNA (deoxyribonucleic acid) sequence operations. In [24, 25], matrix semitensor product and Boolean network are used in the encryption scheme. First, the pixels of the initial plaintext image are randomly divided into four blocks. The pixels in each block are then subjected to different numbers of rounds of Arnold transformation, and the four blocks are combined to generate a scrambled image. Then, a set of pseudosecret keys is given and filtered through a synchronously updating Boolean network to generate the real secret key, which is used as the initial value to generate a chaotic sequence. Finally, the matrix semitensor product (STP) operation is applied to the chaotic sequences and the scrambled image to generate an encrypted image. Compared with other encryption algorithms, the algorithm is more secure and effective, and it is also suitable for color image encryption. In [26], the fractal sorting matrix is irregular, self-similar, and infinitely iterative. And the scrambling images or information based on this new cluster of matrices can effectively improve encryption algorithm security. In addition, the data in the antidifferential attack test are closer to the theoretical values and smaller in data fluctuation. Therefore, the proposed algorithm shows better security and resistance to various attacks. An encrypted coverless information hiding method that transfers secret images between two different image domains using generative models was proposed in [27]. In the encryption stage, firstly, a secret image was embedded into a public image (one domain) to obtain a synthetic image; then, the image was utilized as the input to the first generative model F to obtain an encrypted image (another domain). Adversarial loss and an extraction module are added to improve the quality of the encrypted images generated in this stage. In the decryption stage, a second generative model G was designed to reconstruct the synthetic images from the encrypted images. Finally, the secret image is separated from the reconstructed synthetic image.

However, the methods mentioned above are types of symmetric cryptosystems, where encryption and decryption use the same key. This may cause problems related to key management [28] and image information leakage [1]. In order to overcome the shortcomings of symmetric cryptography in key management, many asymmetric encryption algorithms have been proposed [29–37]. For example, single-channel color image encryption based on asymmetric cryptosystem was proposed in [33]. Firstly, the color components, respectively, multiplied with three random phase encryption keys were combined into one gray image using convolution. Then, the gray image was encoded into a real-value gray ciphertext using the asymmetric cryptosystem. Moreover, the decryption key is generated during encryption process and is different from the encryption key. In [34], Hartley transform and gyrator transform were implemented into single-channel color image encryption with asymmetric cryptosystem. Due to the nonlinear operation of phase truncation, a one-way encryption scheme could be achieved and thus high robustness against existing attacks could be obtained. In addition, transformation angle of GT offers remarkably sensitive key, and thus the security of the system is greatly enhanced. A double-image

encryption method based on an asymmetric algorithm is proposed in [35]. The encryption process of the method [35] was different from the decryption, and the encrypting keys were also different from the decrypting keys. During the nonlinear encryption process, the images are encoded as amplitude ciphertext, and two phase-only masks generated based on phase truncation are retained as the decryption key. Chen et al. [36] proposed an enhanced asymmetric cryptosystem for color image, which uses equal modulus decomposition (EMD) in the gyrator transform domains, and created an effective one-way trapdoor function through EMD. To improve the security of the cryptosystem, the red-green-blue (RGB) components of color images were confused by using a Baker map. Rakheja et al. [37] proposed an asymmetric hybrid cipher scheme using a four-dimensional hyperchaotic structure by means of coherent superposition and random decomposition in hybrid multiresolution wavelet domain. The four-dimensional hyperchaotic framework's parameters and preliminary conditions together with the fractional order expand the key space and consequently give additional strength to the system.

The RSA encryption algorithm is a type of public-key cryptography. It has two different keys, one of which is a public key and the other a private key. The security of RSA is based on the difficulty of decomposing large integers into two prime factors. Consequently, the RSA algorithm is widely studied and applied in the field of image encryption [38, 39]. For example, in order to enhance the strength of the cryptosystem and provide higher security, a chaotic synchronization cryptosystem combined with RSA encryption algorithm was proposed in [40]. The scheme [40] uses the RSA algorithm to encrypt the plain image to produce a cipher image. To achieve double encryption, the cipher image is reencrypted by using chaotic synchronization.

2. Related Works

In recent years, digital image encryption algorithms based on asymmetric cryptosystems have attracted the attention of experts and scholars. More and more image encryption algorithms based on asymmetric cryptosystems have been proposed. For example, Liu et al. [41] proposed a digital image watermarking model based on the scrambling algorithm logistic and RSA asymmetric encryption algorithm to ensure the security of hidden data based on a large embedding amount, strong robustness, and high computing efficiency. The system [41] involved applying the encryption algorithms of logistic and RSA to the watermark image and performing the hybrid decomposition of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) on the host image, and the watermark was embedded into the low-frequency subband of the host. In [42], elliptic curve pseudorandom and Advanced Encryption System were introduced for image encryption scheme. The proposed scheme uses elliptic curve random generator to produce a sequence of arbitrary numbers based on curves; then, the Advanced Encryption System is applied to the sequence to acquire arbitrary keys for encrypting image. Jiao et al. [43] proposed an image encryption scheme based on a generalized Arnold map and RSA algorithm. In the scheme, RSA algorithm is used to generate the parameters of the generalized Arnold map. Then, the generalized Arnold map together with permutation and diffusion algorithms is performed on original image to obtain the cipher image. To reduce the burden of transmission, a scheme based on compressive sensing and RSA algorithm was proposed in [44], where the optical compressive image system is used to sample original image. During the process of encryption, the Walsh–Hadamard transform and a measurement matrix are designed for measuring the original image in order to reduce the redundant information in the original image. Then, a pseudorandom sequence generated by one-dimensional cascade chaotic system and deoxyribonucleic acid (DNA) sequence operations are utilized to change the pixel values. Finally, the cipher image can be obtained.

In order to efficiently and safely handle large volumes of encrypted data, chirp z-transform (CZT) was implemented into the asymmetric multi-image encryption system proposed in [45]. Since the system is asymmetric, decryption keys are different from encryption keys, which improves the system's ability to resist cryptanalysis attacks. To resist chosen-plaintext and chosen-ciphertext attacks, Henon Map, Dynamic S-Boxes, and Elliptic Curve Cryptography were introduced for an image encryption scheme [46], where encryption keys are produced by elliptic curve cryptography (ECC). Moreover, a hash verification step was utilized in decryption process to resist chosen-plaintext attacks. In order to improve the security of image transmission, RSA cryptosystem, reality preserving fractional discrete cosine transform, and Arnold transform were implemented into a novel approach [47] for security of multiple-color images. In the process of encryption, firstly, color images are divided into red, green, and blue components. Then, each component is encrypted by RSA cryptosystem. Moreover, the fractional discrete cosine transform is performed on the partially encrypted image. Finally, the cipher image can be obtained after Arnold transform dislocating the processed image. In [48], the scheme combined the advantages of hyperchaotic map and RSA algorithm. Firstly, encrypt the plain image into a cipher image by utilizing the row and column encryption algorithms. Second, the secret key of image is converted into ciphertext by using the RSA algorithm; then the ciphertext is transformed into an image and permuted by using the Arnold map to obtain the key cipher image. Finally, to obtain a visually secure image, the key cipher image and the cipher image are embedded into a carrier image.

Based on the analysis above, this paper combines Lorenz hyperchaotic system and RSA algorithm to solve the problem of key exchange by using permutation and finite field diffusion algorithms.

3. Preliminaries

3.1. RSA Algorithm. RSA is an asymmetric encryption algorithm. In 1978, three mathematicians, Rivest, Shamir, and Adleman, proposed the RSA encryption algorithm for the first time. Unlike the symmetric cryptosystem, RSA

algorithm has two different keys, one of which is a public key and the other is a private key. If the data are encrypted with a public key, only the corresponding private key can be used for decryption; if the data is encrypted with a private key, then only the corresponding public key can be used for decryption. Because encryption and decryption use two different keys, this algorithm is called an asymmetric encryption algorithm. Currently, RSA is the most widely used asymmetric encryption algorithm. It is based on Euler theorem in number theory, and its security depends on the difficulty of factoring large integers. RSA can be used to encrypt information and can also be used as a digital signature. The encryption and decryption process of the RSA algorithm is shown in Algorithm 1.

This algorithm can encrypt plaintext data by using the recipient's public key. After sending the ciphertext to the receiver, the receiver uses its private key to decrypt the ciphertext to obtain the plaintext data. Only the receiver knows the private key, which reduces the transmission of the key in the channel and improves the security of communication.

3.2. Lorenz Hyperchaotic System. The Lorenz hyperchaotic system is a classic chaotic system, which is defined as follows:

$$\begin{cases} \dfrac{\mathrm{d}x}{\mathrm{d}t} = a(y - x) + w, \\ \dfrac{\mathrm{d}y}{\mathrm{d}t} = cx - y - xz, \\ \dfrac{\mathrm{d}z}{\mathrm{d}t} = xy - bz, \\ \dfrac{\mathrm{d}w}{\mathrm{d}t} = -yz + rw. \end{cases} \tag{1}$$

A hyperchaotic system needs to satisfy the following conditions. Firstly, it has a phase space of dimension at least four. Secondly, it possesses at least two positive Lyapunov exponents [49].

In equation (1), r is the control parameter. Let $a = 10, b = 8/3, c = 28$; when $-1.52 \le r \le -0.06$, the system exhibits hyperchaotic behavior. According to the method proposed by Ramasubramanian et al. [50], when $r = -1$, the four Lyapunov exponents [51] can be obtained as follows: $\lambda_1 = 0.3381, \lambda_2 = 0.1586, \lambda_3 = 0, \lambda_4 = -15.1752$; obviously, the Lorenz hyperchaotic system exhibits hyperchaotic behavior. The fourth-order Runge–Kutta method is usually used to discretize continuous chaotic systems such as Lorenz hyperchaotic systems. For example, the first-order differential equation is defined as follows:

$$\frac{\mathrm{d}y}{\mathrm{d}x} = f(x, y), \quad x \in [a, b]. \tag{2}$$

The discrete form of Runge–Kutta method for equation (2) is defined as

$$\begin{cases} y_{i+1} = y_i + \dfrac{h}{6}(K_1 + 2K_2 + 2K_3 + K_4), \\ K_1 = f(x_i, y_i), \\ K_2 = f\left(x_i + \dfrac{h}{2}, y_i + \dfrac{h}{2}K_1\right), \\ K_3 = f\left(x_i + \dfrac{h}{2}, y_i + \dfrac{h}{2}K_2\right), \\ K_4 = f(x_i + h, y_i + hK_3). \end{cases} \tag{3}$$

The projections of Lorenz hyperchaotic system attractor drawn by equations (1) and (3) are shown in Figure 1. And the initial value range of Lorenz hyperchaotic system is as follows: $x_0 \in (-40, 40)$, $y_0 \in (-40, 40)$, $z_0 \in (1, 81)$, and $w_0 \in (-250, 250)$. Figure 1 shows the six strange attractors of the Lorenz hyperchaotic system, where the phase diagram of $x_n - z_n$ is butterfly like and is known as the butterfly attractor.

3.3. Chaotic Sequence Generator. The state values of chaotic systems are floating-point numbers, and the sequences composed of the state values of chaotic systems cannot be directly applied to image cryptosystems. In general, for images with a gray level of L, the chaotic state value needs to be converted to an integer of $0 \sim L - 1$. The transformed sequence can be applied to image cryptosystem, which is called chaotic pseudorandom sequence. Two methods of converting chaotic state values into integers are used in this study, as shown in the following equations:

$$d_i = \mathrm{floor}(x_i \times 10^m) \bmod L, \tag{4}$$

$$d_i = \mathrm{floor}(x_i \times 2^n) \bmod L. \tag{5}$$

3.4. Permutation without Repetition. Reshape the two-dimensional image matrix called P into a one-dimensional vector in rows or columns, which is denoted as A. Generate a pseudorandom sequence, X_i with the length of $M \times N$ by using the Lorenz hyperchaotic system, where $i = 1, 2, \ldots, MN$. Only the first one of the repeated pseudorandom numbers in X is preserved. Then, add the values in the set $\{1, 2, \ldots, MN\}$ that do not appear in X to the end of X in ascending order. Finally, swap $A(X_i)$ and $A(X_{MN-i+1})$.

3.5. Permutation Associated with Plaintext

Step 1. For a given pixel coordinate (x, y) in image A, we can use equations (6) and (7) to calculate a new coordinate of the pixel (m, n) in image B, as shown in the following equation:

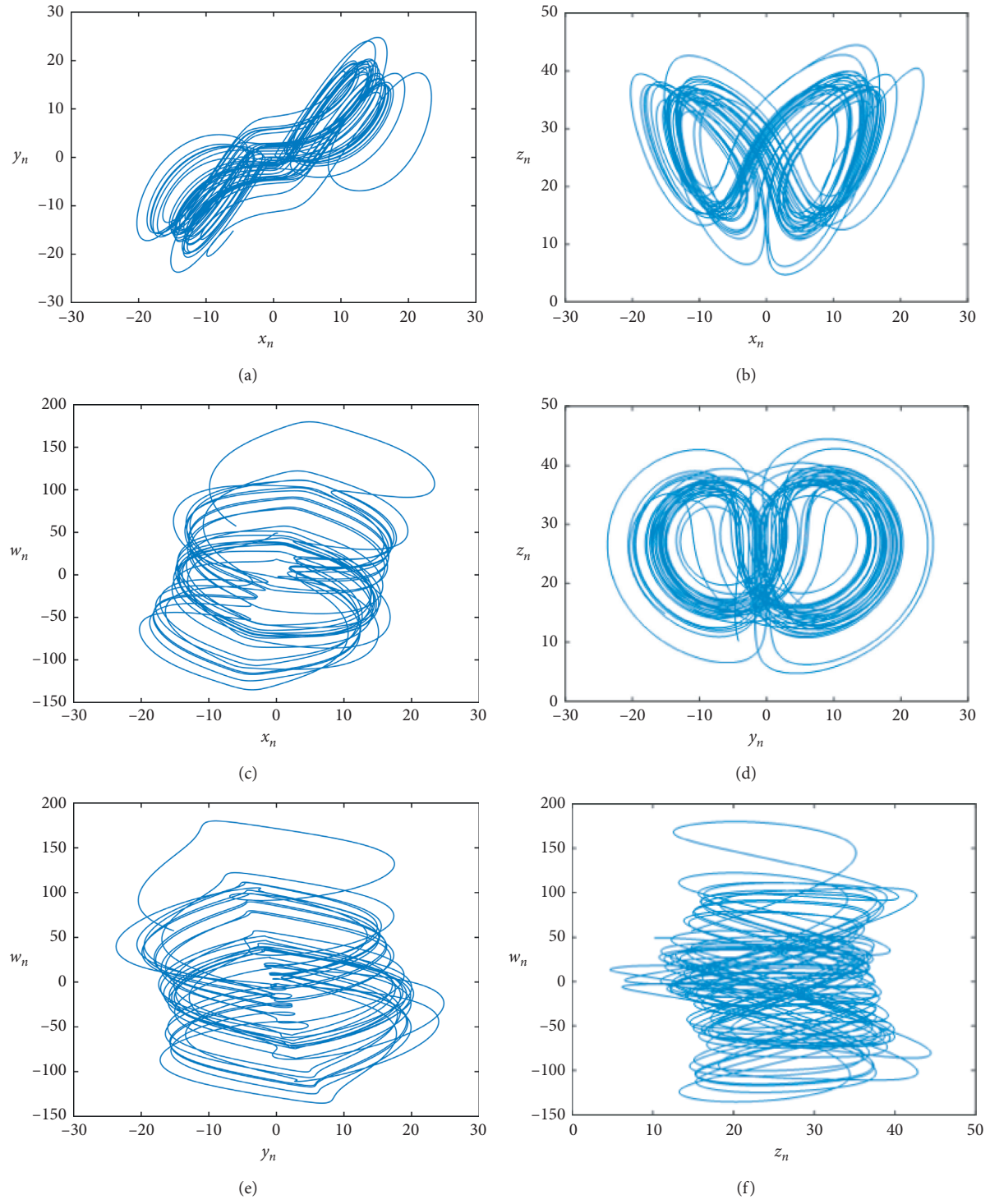

Figure 1: The projections of Lorenz attractor. (a) x-y plane. (b) x-z plane. (c) x-w plane. (d) y-z plane. (e) y-w plane. (f) z-w plane.

$$m = (U(i, j) + \text{sum}(A(Z(i, j), 1 \text{ to } N) \bmod M)) + 1, \tag{6}$$

$$n = (V(i, j) + \text{sum}(A(1 \text{ to } M, W(i, j)) \bmod N)) + 1, \tag{7}$$

where $k = 1, 2, \ldots, M$, $l = 1, 2, \ldots, N$, $\{x_i\}, \{y_i\}, \{z_i\}$, and $\{w_i\}$ $(i = 1, 2, \ldots, MN)$ are the four pseudorandom sequences generated by the Lorenz hyperchaotic system.

As for equations (6) and (7), if ($m = i$ or $m = Z(i, j)$), ($n = j$ or $n = W(i, j)$), or ($Z(i, j) = i$ or $W(i, j) = j$), then the position of $A(i, j)$ remains unchanged; otherwise, $A(i, j)$ and $A(m, n)$ swap positions.

Step 2. When coordinate (i, j) traverses all the pixels of image A in the scanning order from left to right and top to bottom, repeat step 1; we can convert image A into image B.

3.6. Diffusion Based on Finite Fields GF (257). Diffusion operation hides the information of any original image pixels in as many cipher image pixels as possible without changing the position of pixels. In cryptography, the finite field called GF (p) is an important field, where p is a prime number. It is a finite set of integers and uses mode operations to perform basic mathematical operations [52]. This study uses a finite field, $GF(257) = \{0, 1, \ldots, 256\}$, where 257 is a prime number. In the multiplication operation, in order to reduce the information loss caused by element 0, element 0 can be eliminated first, and then the remaining 255 elements are used for arithmetic operations.

Reshape the two-dimensional image matrix into a one-dimensional vector in rows or columns, which is denoted as P. Let C and S be the cipher vector; then the forward diffusion algorithm, i from 1 to MN, and its inverse operation are shown in equations (9) and (10), where M is the number of rows in the matrix and N is the number of columns in the matrix.

$$C_i = C_{i-1} \times S_i \times P_i, \tag{9}$$

$$P_i = C_i \div C_{i-1} \div S_i. \tag{10}$$

The reverse diffusion algorithm, i from MN to 1, and its inverse operation are shown in equations (11) and (12), respectively:

$$C_i = C_{i+1} \times S_i \times P_i, \tag{11}$$

$$P_i = C_i \div C_{i+1} \div S_i. \tag{12}$$

The multiplication and division used in the above four equations are arithmetic operations that satisfy the finite field of GF (257).

4. The Proposed Image Encryption Scheme

4.1. Image Encryption Process. This research uses Lorenz hyperchaotic system, RSA algorithm, nonrepetitive permutation, and finite field diffusion algorithm to realize a new asymmetric image encryption scheme. The flowchart of image encryption is shown in Figure 2, where the encryption process is described as follows:

Step 1: select prime numbers p and q; calculate $n = p \times q$ and $\varphi(n) = (p - 1)(q - 1)$.

Step 2: generate public key (e, n) and private key (d, n) by using RSA algorithm.

Step 3: four large positive integers (m_1, m_2, m_3, m_4) are randomly selected as confidential information; then the public key (e, n) is used to calculate $c_i = m_i^e \bmod n, i = 1, 2, 3, 4$, which is sent to the receiver.

Step 4: equation (13) is utilized to calculate the parameters x_0, y_0, z_0, w_0 of the Lorenz hyperchaotic system.

$$\begin{cases} x_0 = \text{sqrt}(\log(c_1 + m_1)), \\ y_0 = \text{sqrt}(\log(c_2 + m_2)), \\ z_0 = \text{sqrt}(\log(c_3 + m_3)), \\ w_0 = \text{sqrt}(\log(c_4 + m_4)). \end{cases} \tag{13}$$

Step 5: substitute parameters x_0, y_0, z_0, w_0 into equations (1) and (3) to generate pseudorandom sequence S, X, and R, and convert the generated values into the range of 0 to 255:

where Z, W, U, and V are four pseudorandom matrices generated by the hyperchaotic Lorenz system; the sizes of them are all $M \times N$, as shown in the following equation:

$$\begin{aligned} Z(k, l) &= \left(\text{floor}\left(z_{(k-1)\times N+l} \times 10^{13}\right) \bmod M\right) + 1, \\ W(k, l) &= \left(\text{floor}\left(\left(w_{(k-1)\times N+l} + 500 \bmod 1\right) \times 10^{12}\right) \bmod N\right) + 1, \\ U(k, l) &= \left(\text{floor}\left(\left(x_{(k-1)\times N+l} + y_{(k-1)\times N+l} + 500 \bmod 1\right) \times 10^{12}\right) \bmod M\right) + 1, \\ V(k, l) &= \left(\text{floor}\left(\left(z_{(k-1)\times N+l} + w_{(k-1)\times N+l} + 500 \bmod 1\right) \times 10^{12}\right) \bmod N\right) + 1, \end{aligned} \tag{8}$$

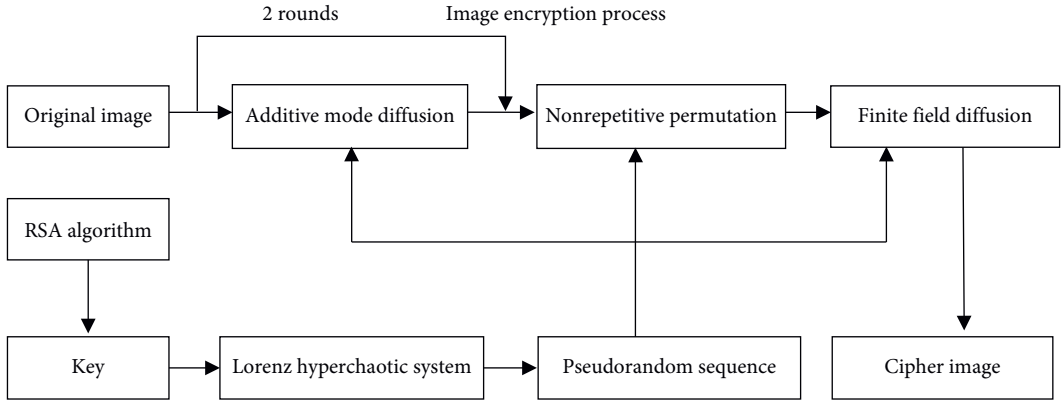

Figure 2: Encryption flowchart of Lorenz chaotic system.

$$\begin{cases} S = \mathrm{mod}\left(\mathrm{floor}\left((s+100)\times 10^{10}\right), 256\right), \\ X = \mathrm{mod}\left(\mathrm{floor}\left((s+100)\times 10^{14}\right), 256\right), \\ R = \mathrm{mod}\left(\mathrm{floor}\left((s+100)\times 2^{16}\right), 256\right). \end{cases} \tag{14}$$

Step 6: record the plain image as P and perform the following additive mode diffusion operation twice with the generated key stream S to obtain image A:

$$\begin{cases} A_i = (A_{i-1} + S_i + P_i) \bmod 256, \\ A_i = (A_{i+1} + S_i + P_i) \bmod 256, \end{cases} \tag{15}$$

where A_i, P_i, and S_i represent the elements of A, P, and S.

Step 7: use the key stream X and conduct nonrepetitive permutation of image A to obtain image B. Perform permutation associated with plaintext.

Step 8: according to equations (9) and (11), use the key stream R and conduct finite field diffusion of image B to obtain image C:

$$\begin{cases} C_i = C_{i-1} + R_i + B_i, \\ C_i = C_{i+1} + R_i + B_i, \end{cases} \tag{16}$$

where C_i, R_i, and B_i represent the elements of C, R, and B.

Step 9: finally, transform C to get an encrypted image matrix E.

As to the color image, it can be treated as three gray images by three channels R, G, and B. So, the encryption is the same for each channel.

4.2. Image Decryption Process. Image decryption is the reverse process of image encryption, as follows:

Step 1: the receiver decrypts the original image with a private key (d, n) based on the received ciphertext information $c_i, i = 1, 2, 3, 4$, calculate $m_i = c_i^d \bmod n, i = 1, 2, 3, 4$, and then equation (13) is used to calculate the parameters x_0, y_0, z_0, w_0 of the Lorenz hyperchaotic system.

Step 2: substitute parameters x_0, y_0, z_0, w_0 into equations (1) and (3) to generate pseudorandom sequence S', X', and R', and convert the generated values into the range of 0 to 255:

$$\begin{cases} S' = \mathrm{mod}\left(\mathrm{floor}\left((s'+100)\times 10^{10}\right), 256\right), \\ X' = \mathrm{mod}\left(\mathrm{floor}\left((s'+100)\times 10^{14}\right), 256\right), \\ R' = \mathrm{mod}\left(\mathrm{floor}\left((s'+100)\times 2^{16}\right), 256\right). \end{cases} \tag{17}$$

Step 3: according to equations (10) and (12), use the key stream R' and conduct finite field diffusion of image E to obtain image C':

$$\begin{cases} C'_i = E_i \div E_{i-1} \div R'_i, \\ C'_i = E_i \div E_{i+1} \div R'_i, \end{cases} \tag{18}$$

where C'_i, E'_i, and R'_i represent the elements of C', E', and R'.

Step 4: use the key stream X' and conduct nonrepetitive permutation of image C' to obtain image B'. Perform permutation associated with plaintext.

Step 5: perform the following additive mode diffusion operation twice on B' with the generated key stream S' to obtain image A':

$$\begin{cases} A'_i = (2\times 256 + B'_i - B'_{i-1} - S'_i) \bmod 256, \\ A'_i = (2\times 256 + B'_i - B'_{i+1} - S'_i) \bmod 256, \end{cases} \tag{19}$$

where A'_i, B'_i, and S'_i represent the elements of A', B', and S'.

Step 6: transform A'_i to get the original image matrix P'.

5. Analysis of Experimental Results

5.1. Random Tests for Chaotic Sequence. We used NIST SP800-22 to test the randomness of the Lorenz hyperchaotic system's sequences (see Table 1). NIST SP800-22 test gives a total of 15 test methods to test the random characteristics of the sequence. Each test produces a P value in [0, 1]. If the P value is higher than a preset threshold α, it means that the chaotic sequence passes the test [53]. In our tests, we set $\alpha = 0.01$, and the length of the chaotic sequence is 10^6.

Input: choose two different prime numbers p and q
(1) Calculate Euler function, $\varphi(n) = (p-1)(q-1)$
(2) $n = p \times q$
(3) Randomly select public key e, $1 < e < \varphi(n)$, and $\gcd(\varphi(n), e) = 1$
(4) Calculate the private key $d \cdot e \equiv 1 \bmod \varphi(n)$; $d = e^{-1} \pmod{\varphi(n)}$
(5) Encryption method: for each plaintext m, calculate $c = m^e \bmod n$
(6) Decryption method: for each ciphertext c, calculate $m = c^d \bmod n$

Algorithm 1: The encryption and decryption process of the RSA algorithm.

Table 1: Randomness test by NIST SP800-22 for the Lorenz hyperchaotic system's sequences.

Test name	P value	Result
The frequency test	0.8823	Pass
Frequency test within a block (block = 10000)	0.7208	Pass
The runs test	0.6031	Pass
Tests for the longest-run-of-ones in a block	0.0798	Pass
The binary matrix rank test	0.1220	Pass
The discrete Fourier transform test	0.8164	Pass
The nonoverlapping template matching test ($m = 10$)	0.2990	Pass
The overlapping template matching test ($m = 9$, template = 111111111)	0.4298	Pass
Maurer's "universal statistical" test	0.4561	Pass
The linear complexity test (block = 1000)	0.6040 [0.6013, 0.3395]	Pass
The serial test (test 1 and test 2)	0.1395	Pass
The approximate entropy test	[0.4992, 0.5407]	Pass
The cumulative sums test (forward and reverse test)	0.8008	Pass
The random excursions test ($x = -1$)	0.9104	Pass
The random excursions variant test ($x = 1$)	0.6031	Pass

5.2. Experimental Results. This paper selects some different images from the USC-SIPI database. And Windows 10 operating system was used with the MATLAB R2020a software. An Intel (R) Core (TM) i5-1035G processor was used, and 16 GB of RAM was required to simulate the work. For the experimental procedure, the private key consisted of large prime numbers $p = 3259, q = 3821$, and $d = 3385223$. Four positive integers were separately selected as $m_1 = 178334$, $m_2 = 38628$, $m_3 = 92873897$, and $m_4 = 829809$. And the public key consisted of $e = 1288367$, $c_1 = 11587151$, $c_2 = 1799483$, $c_3 = 12452638$, and $c_4 = 4198591$. The obtained results were as follows: $x_0 = 4.0349$, $y_0 = 3.7979$, $z_0 = 4.2980$, and $w_0 = 3.9282$. As it can be seen, the results of encryption and decryption for the test image are shown in Figure 3. The encrypted image in Figures 3(i)–3(p) reveals that no information could be obtained from it. The decrypted image (Figures 3(q)–3(x)) also shows that the plain image information could be correctly restored. This proves that the proposed scheme is effective for image encryption. Table 2 shows the time cost of encryption, which uses different size images. As it can be seen, the encryption time of our scheme is shorter than that of the other schemes. Therefore, the proposed scheme is efficient.

6. Analysis of System Performance

6.1. Histogram Analysis. A histogram is utilized to show the distribution of image pixel intensity. An ideal encrypted image usually has a uniform frequency distribution and will not provide any useful statistical information to the attacker. Figure 4 shows the histogram distribution of some images, showing the uniformity of gray values in the results. Simultaneously, a chi-squared test can be used to evaluate the uniformity of the histogram, which is calculated as

$$\chi^2 = \sum_{L=0}^{255} \frac{(O-E)^2}{E}, \tag{20}$$

where L is the intensity level and O and E represent the observed occurrence frequency and the expected occurrence frequency for each gray value, respectively. The uniformity of histogram is assessed with the help of the chi-squared test. Table 3 shows the histogram uniformity results of the χ^2 test for gray images by Lena, Baboon, and Peppers. In the table, at 255 degrees of freedom and 5% and 1% significance level, the chi-square test results are tested. At 5% and 1% significance level, the chi-square values are $\chi^2_{0.01}(255) = 310.457$ and $\chi^2_{0.05}(255) = 293.2478$, respectively [56]. It can be seen that, at both 5% and 1% significance levels, cipher images have fairly uniform distribution for gray values, different from that of their respective plain images. This means that it is difficult to apply histogram attacks.

For quantity analyses of each key, variances of histograms are employed to evaluate uniformity of ciphered images. The lower value of variances indicates the higher uniformity of ciphered images. We also calculate the two variances of ciphered images which are encrypted by different secret keys on the same plaintext image. The closer of

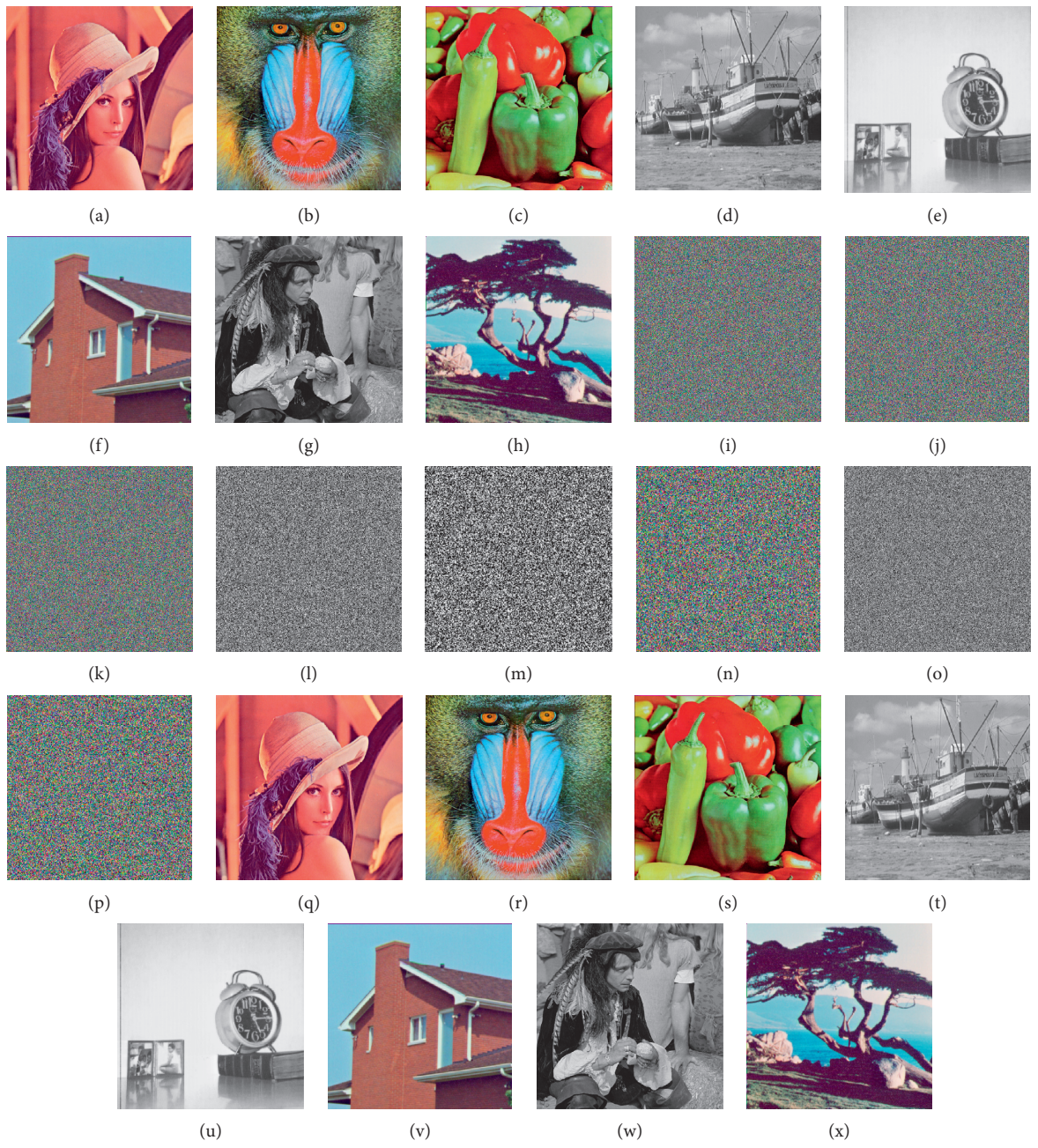

FIGURE 3: Plain image: (a) Lena; (b) Baboon; (c) Peppers; (d) Boat; (e) Clock; (f) House; (g) Male; (h) Tree. Encrypted: (i) Lena; (j) Baboon; (k) Peppers; (l) Boat; (m) Clock; (n) House; (o) Male; (p) Tree. Decrypted: (q) Lena; (r) Baboon; (s) Peppers; (t) Boat; (u) Clock; (v) House; (w) Male; (x) Tree.

TABLE 2: Time cost analysis.

Original image	Boat (512*512)	Lena (256*256)	Lena (256*256)	Lena (256*256)	Lena (256*256)
Algorithms	Proposed	Proposed	Ref. [54]	Ref. [55]	Ref. [17]
Encryption time (s)	0.269177	0.079054	0.132	0.417	0.580

the two values of variances indicates the higher uniformity of ciphered images when the secret keys are varying. The variance of histograms is presented as follows:

$$\operatorname{var}(Z) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}\left(z_i - z_j\right)^2, \tag{21}$$

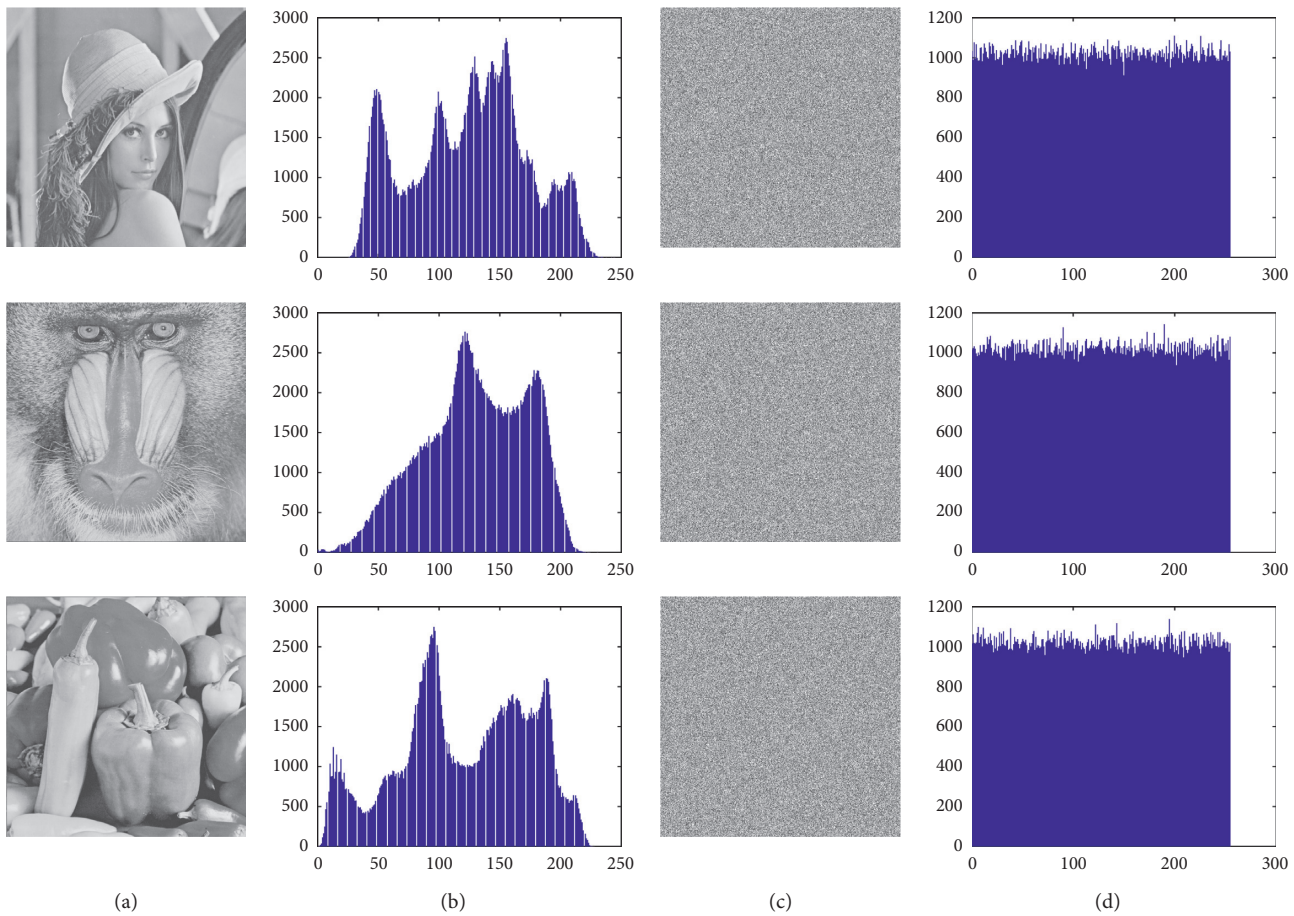

Figure 4: Histogram test: (a) plain images; (b) histograms of the plain images; (c) cipher images; (d) histograms of the cipher images.

Table 3: Histogram uniformity evaluation based on the chi-squared test.

Image	Lena	Baboon	Peppers	Boat	Clock
Plain image	158349.36	187356.57	120165.79	383969.69	217971.39
Cipher image	254.7051	246.5801	247.5566	246.5527	263.8195
Pass or not	Pass	Pass	Pass	Pass	Pass

where Z is the vector of the histogram values and $Z = \{z_1, z_2, \ldots, z_{256}\}$ and z_i and z_j are the numbers of pixels where gray values are equal to i and j, respectively. In simulating experiments, we calculate two variances of histograms of two ciphered images by equation (21) from the same plaintext image with different secret keys. Only one parameter of secret keys is changed in such different secret keys. Table 4 lists the variances of histograms of ciphered Lena, BARB, and Boat images. In Table 4, the variances in the first column are obtained by the secret key Key1 ($x_0 = 4.0349, y_0 = 3.7979, z_0 = 4.2980, w_0 = 3.9282$) ; the variances in next columns are obtained by only changing one parameter of x_0, y_0, z_0, and w_0, respectively, compared with the secret key Key1. The variance values are about 1000, which indicates that the average fluctuation of the number of pixels in each gray value is about 114 pixels. However, the variance value is 634576.2901 for histogram of the plaintext image Lena. And the variance value is 5335.8309 for histogram of ciphered image of Lena in Zhang's paper [57], which is greater than any of the variances in Table 4. Therefore, the proposed algorithm is efficient.

6.2. Correlation Coefficient. The correlation coefficient is a linear correlation between adjacent image pixels. In general, plain images have a strong correlation between adjacent pixels in horizontal, vertical, and diagonal directions, but there should be no correlation between adjacent pixels in cipher images. In the experiment, we randomly selected 2000 pairs of adjacent pixels from the original images and the encrypted images and analyzed the correlations at horizontal, vertical, and diagonal directions. The calculation formula is defined as

Table 4: Variances of histograms compared among all secret keys in the proposed algorithm.

Cipher image	Key 1	x_0	y_0	z_0	w_0
Lena	1047.6549	1038.0390	1044.2187	1030.9570	1094.3476
BARB	941.1686	970.0156	924.8242	961.7343	912.7245
Boat	990.0784	1005.9726	984.6914	1056.5585	971.8085
Average	992.9672	1004.6757	984.5781	1016.0976	992.9602

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}},$$
$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right),$$
$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{22}$$
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2,$$

where r_{xy} is the correlation coefficient, x and y are the gray values of two adjacent pixels, and N is the total quantities of (x_i, y_i). The correlation coefficient value is between −1 and +1. And the correlation coefficient of two independent and uncorrelated random sequences (adjacent pixels) is more close to zero [58]; the effect of encryption is better. The correlation coefficient between the original image (Male) and the encrypted image is shown in Figure 5. Table 5 calculates the correlation coefficients of some images from horizontal, vertical, and diagonal directions. Table 6 takes the color Lake image as an example to analyze the correlation coefficient between the plain image and the cipher image. Table 7 compares the correlation coefficient results of gray Boat image by different encryption algorithms. The results show that the proposed encryption algorithm breaks the strong correlation in the original image and can effectively resist statistical attacks.

6.3. Information Entropy. Information entropy reflects the uncertainty of image information; it is generally believed that the greater the value of information entropy, the greater the uncertainty (the more information). It can be used to measure the randomness of data series. It is mathematically defined as

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i), \tag{23}$$

where L is the grayscale of the image and $p(i)$ is the probability that the gray value i will appear. For digital images with 256 grayscale levels, the theoretical value of entropy H is 8. The higher the entropy value of the cipher image, the more uniform the distribution of pixel value. In addition, local Shannon entropy measures the randomness of image by calculating the sample mean of Shannon entropy on randomly selected image blocks and multiple nonoverlapping, so it can overcome the disadvantages of global information entropy, such as low efficiency, inconsistency, and inaccuracy [59]. Table 8 shows the local entropy of the cipher image and the information entropy of the image. And the average information entropy value of the three channels is calculated as the information entropy value of color image. It can be seen from the results that the entropy value of cipher image is very close to the theoretical value of 8, while the information entropy of plain image is significantly different from the theoretical value.

We make the comparison with some color images by information entropy [60, 61]. Table 9 shows the results. It can be seen that the proposed algorithm has good performance to resist differential attacks.

6.4. Differential Attack Analysis. In general, two encrypted images (the original cipher image and the new cipher image by changing one pixel in the original image) are compared to analyze the relationship between the original image and the corresponding cipher image in differential attack. The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are two common indicators of attack resistance [62–66]. NPCR measures the rate of change of pixel values in a cipher image by changing a pixel value in the original image, while UACI measures the average changing intensity between the original image and the corresponding cipher image. They can be defined as

$$\operatorname{NPCR}(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{D(i, j)}{M \times N} \times 100\%,$$
$$D(i, j) = \begin{cases} 0, & \text{if } C_1(i, j) = C_2(i, j), \\ 1, & \text{if } C_1(i, j) \neq C_2(i, j), \end{cases} \tag{24}$$
$$\operatorname{UACI}(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1(i, j) - C_2(i, j)\right|}{M \times N \times T} \times 100\%,$$

where M is the width of an image, N is the height of an image, and T is the grayscale of an image. Moreover, C_1 is the cipher image and C_2 is the modified cipher image after a pixel value of the original image is changed. Table 10 shows the NPCR and UACI values of some images. Table 11 lists the results of NPCR and UACI when the pixel values at different positions of Lena image are changed. All values of NPCR and UACI of our method are close to ideal values 99.6094% and 33.4635%, respectively.

6.5. Key Space Analysis. A key space is a collection of all valid keys. For the digital image cryptosystem proposed in this paper, the keys, $K = \{x_0, y_0, z_0, w_0\}$, are the initial value

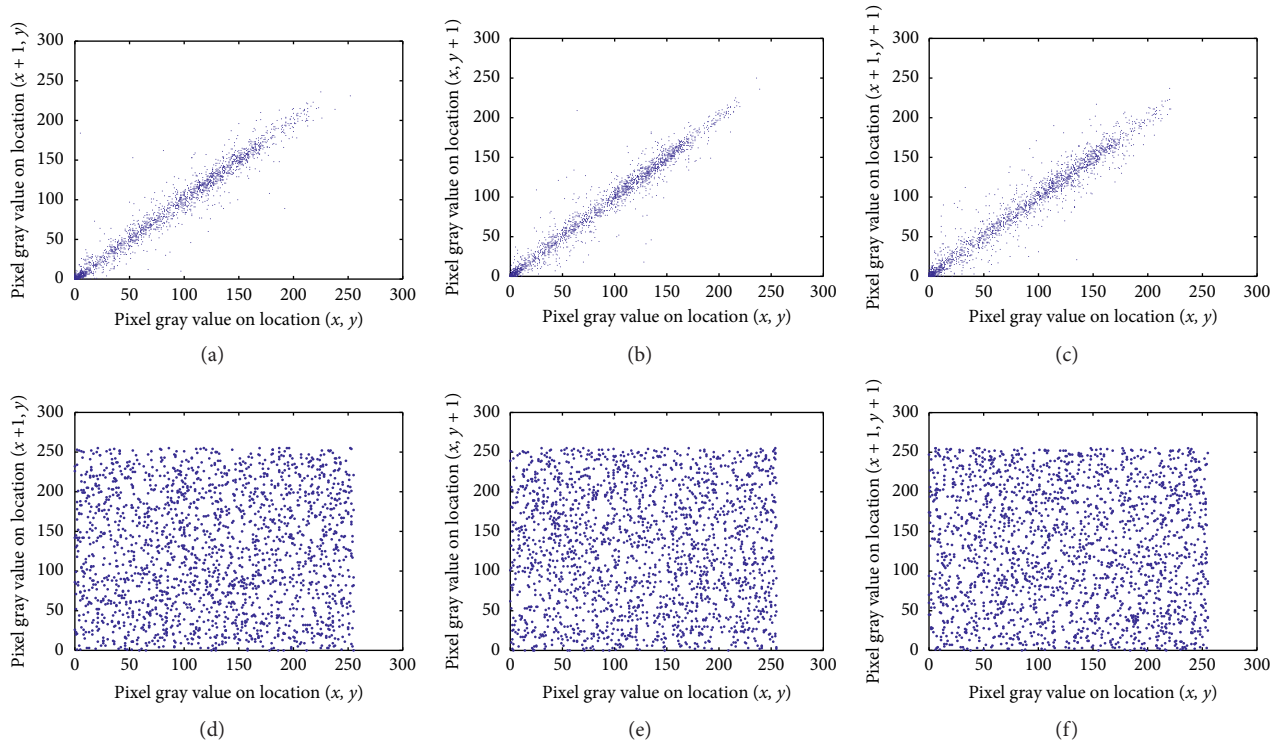

Figure 5: Correlation of two adjacent pixels in the plain image of 1024 × 1024 Male: (a) horizontal direction; (b) vertical direction; (c) diagonal direction. Correlation of two adjacent pixels in the cipher image: (d) horizontal direction; (e) vertical direction; (f) diagonal direction.

Table 5: Correlation coefficients of different images.

Original images	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9870	0.9690	0.9627	−0.0328	0.0105	−0.0330
Baboon	0.7794	0.8681	0.7497	−0.0179	−0.0060	0.0181
Peppers	0.9819	0.9747	0.9624	−0.0195	−0.0101	−0.0109
Boat	0.9719	0.9255	0.9268	0.0060	−0.0219	0.0211
Male	0.9790	0.9796	0.9726	0.0048	−0.0253	−0.0097

Table 6: Correlation coefficients of color Lake.

	Plain image			Cipher image		
	R (red)	G (green)	B (blue)	R (red)	G (green)	B (blue)
Horizontal	0.9533	0.9648	0.9682	0.0011	−0.0016	0.0062
Vertical	0.9594	0.9680	0.9659	−0.0365	0.0005	−0.0206
Diagonal	0.9440	0.9543	0.9517	−0.0235	0.0174	−0.0038

Table 7: Comparison of correlation coefficients of gray Boat image.

Encryption algorithm	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Proposed	0.9709	0.9353	0.9280	0.0035	−0.0006	−0.0074
Ref. [9]	0.9629	0.9672	0.9407	0.0071	0.0095	0.0140
Ref. [43]	0.9379	0.9383	0.8790	0.0146	0.0026	0.0013

Table 8: The information entropy and local entropy of some images.

Image	Plain image	Cipher image	Local Shannon
Lena	7.2719	7.9993	7.95806
Baboon	7.6444	7.9994	7.95425
Peppers	7.2978	7.9993	7.95268
Male	7.5237	7.9998	7.95709
Lake	7.3896	7.9993	7.95632
Boat	7.1914	7.9993	7.95559
Tree	7.1816	7.9975	7.95245
Clock	6.7057	7.9976	7.95367

Table 9: Information entropy comparison with color Peppers images.

Methods	R	G	B
Proposed	7.9993	7.9993	7.9994
Ref. [43]	7.9993	7.9992	7.9993
Ref. [60]	7.9989	7.9991	7.9989
Ref. [61]	7.9971	7.9975	7.9974

Table 10: UACI/NPCR scores of grayscale images for different image encryption algorithms.

Images	Wu et al. [65]	Zhou et al. [66]	Hua and Zhou [67]	Zhou et al. [68]	Lan et al. [69]	Proposed
5.1.09	33.51/99.61	33.48/99.60	33.60/99.61	33.14/99.60	33.42/99.60	33.3829/99.6185
5.1.10	33.56/99.60	33.51/99.61	33.54/99.62	33.24/99.61	33.45/99.64	33.4752/99.6140
5.1.11	33.43/99.61	33.35/99.61	33.44/99.62	33.72/99.64	33.40/99.61	33.4587/99.6140
5.1.12	33.62/99.61	33.45/99.63	33.42/99.57	33.56/99.60	33.41/99.60	33.5242/99.5941
5.1.13	33.46/99.61	33.36/99.59	33.42/99.61	33.77/99.63	33.42/99.59	33.3068/99.6506
5.1.14	33.46/99.66	33.37/99.67	33.47/99.64	33.21/99.62	33.44/99.63	33.5055/99.6231
5.2.08	33.43/99.61	33.43/99.60	33.47/99.63	33.31/99.61	33.45/99.62	33.4720/99.6197
5.2.09	33.34/99.60	33.42/99.60	33.49/99.63	33.62/99.60	33.57/99.63	33.5018/99.5884
5.3.01	33.45/99.61	33.43/99.61	33.45/99.59	33.42/99.60	33.47/99.61	33.5058/99.6149
5.3.02	33.48/99.60	33.47/99.61	33.49/99.59	33.29/99.60	33.49/99.61	33.4673/99.6212
7.1.01	33.54/99.58	33.44/99.61	33.52/99.60	33.25/99.59	33.47/99.59	33.5358/99.6063
7.1.02	33.49/99.61	33.45/99.60	33.48/99.61	33.53/99.59	33.46/99.62	33.4425/99.6082
7.1.03	33.56/99.62	33.46/99.59	33.46/99.61	33.27/99.62	33.41/99.62	33.4004/99.6078
7.1.04	33.48/99.62	33.46/99.62	33.52/99.60	33.21/99.59	33.49/99.59	33.3767/99.6059
7.1.05	33.40/99.62	33.38/99.59	33.54/99.62	33.21/99.62	33.45/99.60	33.5075/99.6063
7.1.06	33.57/99.63	33.50/99.60	33.53/99.63	33.30/99.61	33.48/99.61	33.5815/99.5991
7.1.07	33.44/99.59	33.47/99.59	33.52/99.59	33.15/99.61	33.51/99.63	33.4765/99.5972
.1.08	33.48/99.62	33.45/99.61	33.57/99.61	33.26/99.60	33.44/99.59	33.5333/99.5926
7.1.09	33.41/99.62	33.40/99.61	33.52/99.62	33.23/99.58	33.43/99.61	33.4785/99.6094
7.1.10	33.52/99.61	33.47/99.61	33.53/99.60	33.59/99.61	33.49/99.60	33.4756/99.6056
7.2.01	33.48/99.61	33.47/99.62	33.50/99.62	33.42/99.63	33.50/99.61	33.4988/99.6058
Elaine.512	33.49/99.58	33.52/99.62	33.51/99.62	33.37/99.61	33.51/99.61	33.4788/99.5987
Boat.512	33.44/99.61	33.38/99.63	33.55/99.62	33.37/99.61	33.47/99.61	33.4100/99.6021
Numbers.512	33.54/99.60	33.42/99.59	33.40/99.61	33.77/99.61	33.45/99.60	33.3944/99.6151
Ruler.512	33.42/99.61	33.40/99.62	33.51/99.61	33.43/99.61	33.44/99.59	33.4249/99.6086
Gray21.512	33.47/99.62	33.40/99.60	33.39/99.60	33.36/99.60	33.50/99.61	33.4812/99.6075
Mean	33.4827/99.6104	33.4362/99.6092	33.4938/99.6100	33.3846/99.6085	33.4623/99.6095	33.4654/99.6095

Table 11: Lena image sensitivity test in different position pixels.

Pixels	(1, 8)	(77, 184)	(14, 211)	(181, 43)	(233, 104)	(255, 255)
NPCR (%)	99.5823	99.6151	99.5991	99.6227	99.6159	99.6075
UACI (%)	33.4796	33.4255	33.4523	33.4580	33.4993	33.3801

of Lorenz hyperchaotic system, where $x_0 \in (-40, 40)$, $y_0 \in (-40, 40)$, $z_0 \in (1, 81)$, and $w_0 \in (-250, 250)$. The steps of x_0, y_0, and z_0 are all 10^{-13}, and the steps of w_0 are 10^{-12}. Therefore, the space size of the key is about $S \approx 2.56 \times 10^{59}$, which is equal to the length of the key $L = \log_2 S \approx 197$ bit.

If the eavesdropper uses an exhaustive search of the key to crack the encryption or decryption of the cryptosystem, it only needs to attempt half of the keys in the key space. Since the methods of encryption and decryption are reciprocal, it is sufficient to discuss the case of encryption. For the known plaintext and ciphertext pairs, if the ciphertext is exactly the same as the known ciphertext, the randomly selected key is the true key. And the time needed to crack it by an exhaustive search of the key can be approximated by the product of the number of keys in half of the key space and the time of a single encryption, which is about 4.4607×10^{51} years. That is to say, the key space of Lorenz chaotic system is large enough.

6.6. Key Sensitivity Analysis. Key sensitivity analysis is to analyze the difference between two cipher images obtained by encrypting the same plain image when the key changes slightly. If there are significant differences between the two cipher images, the key sensitivity of the image encryption system is strong; if there are small differences between the two cipher images, the key sensitivity is poor. A good image encryption system should have strong key sensitivity. The test process is as follows.

Suppose the initial set of keys is recorded as keys 1, denoted as

$$\text{keys1} = \{p, q, e, d, m_1, m_2, m_3, m_4, c_1, c_2, c_3, c_4\}, \quad (25)$$

where the values of $p, q, d, m_1, m_2, m_3, m_4$ represent the private key and e, c_1, c_2, c_3, c_4 are the public key. Keys 1 is used to encrypt the gray image (Lena). Figure 6(a) shows the gray Lena image, and Figure 6(b) shows the corresponding cipher image. Suppose a value in keys 1 changes slightly; then keys 2 is expressed as

$$\text{keys2} = \{p, q, e, d, m_1 - 1, m_2, m_3, m_4, c_1, c_2, c_3, c_4\}. \quad (26)$$

Keys 2 is used to encrypt the gray Lena image to obtain a new cipher image shown in Figure 6(c). Figure 6(d) is a different image of Figures 6(b) and 6(c). When the wrong decryption key, keys 2, is used to decrypt the image in Figure 6(b), the decrypted image can be obtained as shown in Figure 6(e). Figure 6(f) shows the correct decrypted image. And the NPCR and UACI values of Figures 6(b) and 6(c) were, respectively, 99.60785% and 33.50445%, which indicates that more than 99% of the pixels could be changed with just a single key change. Therefore, the proposed algorithm is highly sensitive to the key.

6.7. Security Analysis. Currently, a method that involves an exhaustive search of the key is used to crack a password, which attempts all possible key combinations. However, the RSA algorithm uses exponential calculations in both the encryption and decryption processes, which has a huge computational workload. Therefore, it is impossible to decipher by using an exhaustive search. Cryptographic analysis is the only means to decipher the RSA algorithm. However, cracking RSA cryptography needs to factor two large integers, which is difficult. Moreover, Lorenz hyperchaotic system is sensitive to initial conditions, pseudorandomness, nonlinearity, and nonperiodicity. Therefore, the proposed encryption scheme can safely and effectively hide information.

6.8. Chosen-Plaintext Attacks or Chosen-Ciphertext Attacks. The capacity of resisting chosen-plaintext attack or chosen-ciphertext attacks is a significant standard to measure security of image encryption [70–72]. Plaintext sensitivity analysis refers to using the same key to encrypt two original images with little difference with the help of the image encryption system to obtain two corresponding cipher images and then compare the differences between the two cipher images. If the difference between the two cipher images is relatively large, it is said that the image encryption system has good plaintext sensitivity, which means that the cryptographic system can resist chosen-plaintext attacks. The general process of plaintext sensitivity is as follows:

(1) For a certain original image P_1, with the help of a given key, use the image encryption system to encrypt P_1 to obtain the corresponding cipher image, denoted as C_1

(2) Randomly select a pixel from P_1, change the value of the selected pixel, the amount of change is 1, the changed image is marked as P_2, and the same key is used to encrypt P_2 to obtain the corresponding cipher image, denoted as C_2

(3) Compare the difference between C_1 and C_2; calculate the values of NPCR and UACI

(4) Repeat steps (2) and (3) 200 times, calculate the value of a group of NPCR and UACI each time, and finally calculate the average value of 200 groups

Table 12 shows that the NPCR and UACI of test images are approximately equal to the ideal values. In other words, the digital image encryption system proposed in this paper has good plaintext sensitivity; it can resist chosen-plaintext attacks. Chosen-ciphertext attacks are the same as chosen-plaintext attacks because the image encryption system adds permutation associated with the plaintext, which can enhance the ability of the image encryption scheme to resist chosen-plaintext attacks or chosen-ciphertext attacks.

Table 13 shows that the cryptosystem can resist chosen-ciphertext attacks.

6.9. Noise and Data Loss Attacks. It is inevitable that the digital signal may be corrupted by noise or data loss during the transmission. In this situation, we hope to acquire the content of the original images as much as possible so it is not necessary to transmit the encrypted images again. When the image information is tampered or destroyed by others after being attacked by noise (such as Gaussian noise and salt and pepper noises), the algorithm proposed in this paper can detect that the image has been tampered or destroyed by others. However, the algorithm cannot reconstruct the cipher images, because the algorithm is actually very sensitive to the ciphertext; if the ciphertext changes slightly, the

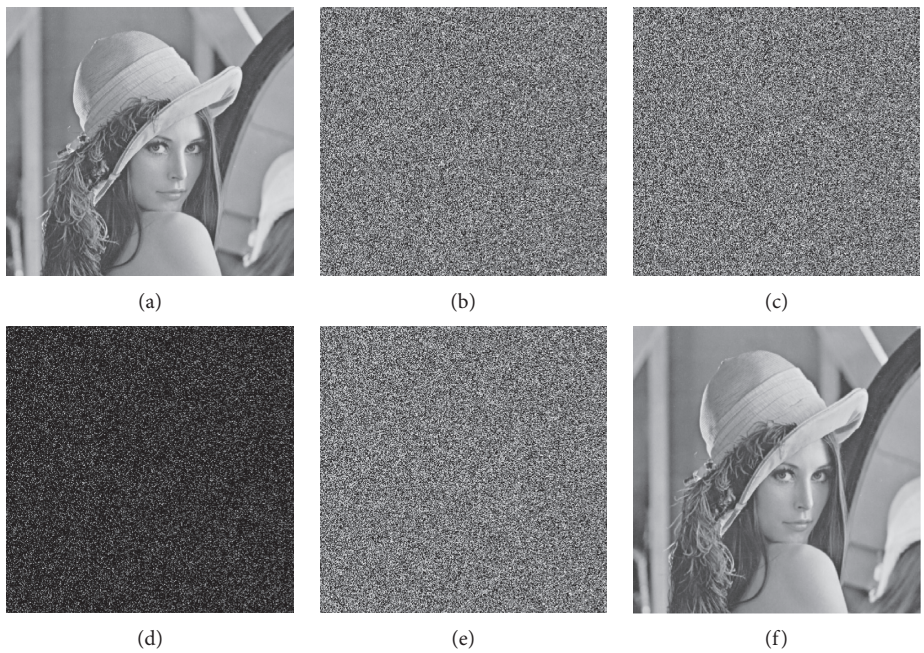

Figure 6: Key sensitivity analysis: (a) original image; (b) encrypted image using keys 1; (c) encrypted image using keys 2; (d) difference image of (b) and (c); (e) decrypted image (b) using wrong keys 2; (f) decrypted image using correct key.

Table 12: Analysis results of chosen-plaintext attacks.

Index	Lena	Baboon	Pepper	Ideal values
NPCR (%)	99.6087	99.6072	99.6109	99.6094
UACI (%)	33.4586	33.4572	33.4592	33.4635

Table 13: Analysis results of chosen-plaintext attacks.

	Lena		Baboon		Pepper	
	Experimental value	Ideal value	Experimental value	Ideal value	Experimental value	Ideal value
NPCR (%)	99.6046	99.6094	99.6065	99.6094	99.6057	99.6094
UACI (%)	28.6226	28.6242	27.8532	27.8472	29.6281	29.6259

decrypted image will also change greatly. If the cipher image is artificially destroyed or tampered with during transmission, the algorithm cannot reconstruct the cipher images to obtain the content of the original images as much as possible. As for data loss attacks, the algorithm cannot also reconstruct the cipher images well. In the future, I will study the impact of noise attacks on image encryption and improve the robustness of the algorithm.

7. Conclusions

This study proposes a new image encryption scheme based on Lorenz hyperchaotic system and Rivest–Shamir–Adleman (RSA) algorithm. Firstly, the initial values of the Lorenz hyperchaotic system are generated by RSA algorithm, and the key stream is produced iteratively. Then, the image data are hidden by performing additive mode diffusion. Secondly, the diffusion image matrix is confused without repetition to hide the image data again. Then, the finite field diffusion algorithm is executed. In order to diffuse the pixel information into the entire ciphertext image, the additive mode diffusion algorithm needs to be looped twice. Finally, the ciphertext image can be obtained. The experimental results prove that the image encryption scheme proposed in this research is effective and has strong antiattack and key sensitivity. In the future, we will study how to improve the efficiency of the scheme for color images.

Data Availability

This paper uses some different images from the USC-SIPI database through http://sipi.usc.edu/database/.

Conflicts of Interest

The authors declare no conflicts of interest.

Authors' Contributions

Riguang Lin and Sheng Li contributed to methodology, validation, data curation, and review and editing; Riguang Lin contributed to software, formal analysis, resources, and original draft preparation; Sheng Li contributed to investigation, supervision, and funding acquisition. All authors have read and agreed to the published version of the paper.

Acknowledgments

This work was supported by the Natural Science Foundation of Guangdong Province (2018A030307062) and the Fund of Southern Marine Science and Engineering Guangdong Laboratory (Zhanjiang) (ZJW-2019-04).

References

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

[2] G. Ye, C. Pan, X. Huang, and Q. Mei, "An efficient pixel-level chaotic image encryption algorithm," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 745–756, 2018.

[3] Y.-G. Yang, J. Tian, H. Lei, Y.-H. Zhou, and W.-M. Shi, "Novel quantum image encryption using one-dimensional quantum cellular automata," *Information Sciences*, vol. 345, pp. 257–270, 2016.

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

[5] D. Huo, D.-f. Zhou, S. Yuan, S. Yi, L. Zhang, and X. Zhou, "Image encryption using exclusive-OR with DNA complementary rules and double random phase encoding," *Physics Letters A*, vol. 383, no. 9, pp. 915–922, 2019.

[6] F. Yi, Y. Kim, and I. Moon, "Secure image-authentication schemes with hidden double random-phase encoding," *IEEE Access*, vol. 6, pp. 70113–70121, 2018.

[7] 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.

[8] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps," *Signal Processing: Image Communication*, vol. 29, no. 5, pp. 618–627, 2014.

[9] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Optics and Lasers in Engineering*, vol. 90, pp. 146–154, 2017.

[10] X. Huang and G. Ye, "An image encryption algorithm based on irregular wave representation," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 2611–2628, 2018.

[11] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[12] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, 2017.

[13] J. Wu, J. Shi, and T. Li, "A novel image encryption approach based on a hyperchaotic system, pixel-level filtering with variable kernels, and DNA-level diffusion," *Entropy*, vol. 22, no. 5, 2020.

[14] S. F. Raza and V. Satpute, "A novel bit permutation-based image encryption algorithm," *Nonlinear Dynamics*, vol. 95, no. 2, pp. 859–873, 2019.

[15] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017.

[16] R. Huang, K. H. Rhee, and S. Uchida, "A parallel image encryption method based on compressive sensing," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 71–93, 2014.

[17] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, 2018.

[18] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding," *Optics and Lasers in Engineering*, vol. 124, p. 105837, 2020.

[19] Y. Zhang, "The image encryption algorithm with plaintext-related shuffling," *IETE Technical Review*, vol. 33, no. 3, pp. 310–322, 2016.

[20] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, and Q. H. Liao, "Quantum image encryption based on generalized Arnold transform and double random-phase encoding," *Quantum Information Processing*, vol. 14, no. 4, pp. 1193–1213, 2015.

[21] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[22] Z.-j. Huang, S. Cheng, L.-H. Gong, and N.-R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform," *Optics and Lasers in Engineering*, vol. 124, p. 105821, 2020.

[23] K. C. Jithin and S. Sankar, "Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set," *Journal of Information Security and Applications*, vol. 50, p. 102428, 2020.

[24] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Information Sciences*, vol. 539, pp. 195–214, 2020.

[25] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Information Sciences*, vol. 507, pp. 16–36, 2020.

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

[27] Q. Li, X. Wang, X. Wang, B. Ma, C. Wang, and Y. Shi, "An encrypted coverless information hiding method based on generative models," *Information Sciences*, vol. 553, pp. 19–30, 2021.

[28] C. Wu, K.-Y. Hu, Y. Wang, J. Wang, and Q.-H. Wang, "Scalable asymmetric image encryption based on phase-truncation in cylindrical diffraction domain," *Optics Communications*, vol. 448, pp. 26–32, 2019.

[29] X.-D. Chen, Q. Liu, J. Wang, and Q.-H. Wang, "Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality image reconstruction," *Optics & Laser Technology*, vol. 107, pp. 302–312, 2018.

[30] A. Sinha, "Nonlinear optical cryptosystem resistant to standard and hybrid attacks," *Optics and Lasers in Engineering*, vol. 81, pp. 79–86, 2016.

[31] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Processing*, vol. 113, pp. 104–112, 2015.

[32] S. K. Rajput and N. K. Nishchal, "Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask," *Applied Optics*, vol. 51, no. 22, pp. 5377–5786, 2012.

[33] X. Deng and D. Zhao, "Single-channel color image encryption based on asymmetric cryptosystem," *Optics & Laser Technology*, vol. 44, no. 1, pp. 136–140, 2012.

[34] M. R. Abuturab, "An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform," *Optics and Lasers in Engineering*, vol. 69, pp. 49–57, 2015.

[35] X. Wang and D. Zhao, "Double images encryption method with resistance against the specific attack based on an asymmetric algorithm," *Optics Express*, vol. 20, no. 11, pp. 11994–12003, 2012.

[36] H. Chen, C. Tanougast, Z. Liu, and L. Sieler, "Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains," *Optics and Lasers in Engineering*, vol. 93, pp. 1–8, 2017.

[37] P. Rakheja, R. Vig, and P. Singh, "An asymmetric hybrid cryptosystem using hyperchaotic system and random decomposition in hybrid multi resolution wavelet domain," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 20809–20834, 2019.

[38] T. Zhao, Q. Ran, and Y. Chi, "Image encryption based on nonlinear encryption system and public-key cryptography," *Optics Communications*, vol. 338, pp. 64–72, 2015.

[39] S. E. El-Khamy, N. O. Korany, and M. H. El-Sherif, "A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption," *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 24091–24106, 2017.

[40] F.-H. Hsiao, "Chaotic synchronization cryptosystems combined with RSA encryption algorithm," *Fuzzy Sets and Systems*, vol. 342, pp. 109–137, 2018.

[41] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert Systems with Applications*, vol. 97, pp. 95–105, 2018.

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

[43] 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, Article ID 9721675,, 14 pages, 2020.

[44] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," *Optics and Lasers in Engineering*, vol. 121, pp. 169–180, 2019.

[45] E. Mosso, O. Suárez, and N. Bolognini, "Asymmetric multiple-image encryption system based on a chirp z-transform," *Applied Optics*, vol. 58, no. 21, pp. 5674–5680, 2019.

[46] S. Ibrahim and A. Alharbi, "Efficient image encryption scheme using Henon map, dynamic S-boxes and ellipticurve cryptography," *IEEE Access*, vol. 8, no. c, pp. 194289–194302, 2020.

[47] V. Guleria, S. Sabir, and D. C. Mishra, "Security of multiple RGB images by RSA cryptosystem combined with FrDCT and Arnold transform," *Journal of Information Security and Applications*, vol. 54, p. 102524, 2020.

[48] Q. Xu, K. Sun, and C. Zhu, "A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map," *Physica Scripta*, vol. 95, Article ID 035223, 2020.

[49] A. Al-khedhairi, A. Elsonbaty, A. H. Abdel Kader, and A. A. Elsadany, "Dynamic analysis and circuit implementation of a new 4D lorenz-type hyperchaotic system," *Mathematical Problems in Engineering*, vol. 2019, Article ID 6581586, 17 pages, 2019.

[50] F. Zhang, "Analysis of a lorenz-like chaotic system by Lyapunov functions," *Complexity*, vol. 2019, Article ID 7812769, 6 pages, 2019.

[51] X. Wang and M. Wang, "A hyperchaos generated from Lorenz system," *Physica A: Statistical Mechanics and Its Applications*, vol. 387, no. 14, pp. 3751–3758, 2008.

[52] J. M. Vilardy O., L. Barba J., and C. O. Torres M., "Image encryption and decryption systems using the jigsaw transform and the iterative finite field cosine transform," *Photonics*, Photonics, vol. 6, no. 4, p. 121, 2019.

[53] L. Bassham, A. Rukhin, J. Soto et al., *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, National Institute of Standards and Technology, Gaithersburg, MA, USA, 2010.

[54] C. Xu, J. Sun, and C. Wang, "An image encryption algorithm based on random walk and hyperchaotic systems," *International Journal of Bifurcation and Chaos*, vol. 30, no. 04, p. 2050060, 2020.

[55] Q. Yin and C. Wang, "A new chaotic image encryption scheme using breadth-first search and dynamic diffusion," *International Journal of Bifurcation and Chaos*, vol. 28, no. 4, 2018.

[56] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," *Journal of Information Security and Applications*, vol. 52, p. 102470, 2020.

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

[58] T. Hu, Y. Liu, L.-H. Gong, and C.-J. Ouyang, "An image encryption scheme combining chaos with cycle operation for DNA sequences," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 51–66, 2017.

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

[60] B. Y. Irani, P. Ayubi, F. A. Jabalkandi, M. Y. Valandar, and M. J. Barani, "Digital image scrambling based on a new one-dimensional coupled Sine map," *Nonlinear Dynamics*, vol. 97, pp. 2693–2721, 2019.

[61] M. Y. Valandar, M. J. Barani, and P. Ayubi, "A fast color image encryption technique based on three dimensional chaotic map," *Optik*, vol. 193, p. 162921, 2019.

[62] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Transactions on NanoBioscience*, vol. 16, no. 8, pp. 850–858, 2017.

[63] X. Wang, Ü. Çavuşoğlu, S. Kacar et al., "S-box based image encryption application using a chaotic system without equilibrium," *Applied Sciences*, vol. 9, no. 4, p. 781, 2019.

[64] K. A. K. Patro and B. Acharya, "An efficient colour image encryption scheme based on 1-D chaotic maps," *Journal of*

Information Security and Applications, vol. 46, pp. 23–41, 2019.

[65] Y. Wu, J. P. Noonan, and S. Agaian, "A Wheel-Switch Chaotic System for Image Encryption," in *Proceedings 2011 International Conference on System Science and Engineering*, pp. 23–27, Macau, China, December 2011.

[66] Y. Zhou, Z. Hua, C. M. Pun, and C. L. Chen, "Cascade chaotic system with applications," *IEEE Transactions on Cybernetics*, vol. 45, no. 9, pp. 2001–2012, 2015.

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

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

[69] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated chaotic systems for image encryption," *Signal Processing*, vol. 147, pp. 133–145, 2018.

[70] Y. Liu, L. Y. Zhang, J. Wang, Y. Zhang, and K.-w. Wong, "Chosen-plaintext attack of an image encryption scheme based on modified permutation-diffusion structure," *Nonlinear Dynamics*, vol. 84, no. 4, pp. 2241–2250, 2016.

[71] Y. Zhang, D. Xiao, W. Wen, and H. Nan, "Cryptanalysis of image scrambling based on chaotic sequences and Vigenère cipher," *Nonlinear Dynamics*, vol. 78, no. 1, pp. 235–240, 2014.

[72] L. Y. Zhang, Y. Liu, C. Wang, J. Zhou, Y. Zhang, and G. Chen, "Improved known-plaintext attack to permutation-only multimedia ciphers," *Information Sciences*, vol. 430-431, pp. 228–239, 2018.