IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON EMERGING APPROACHES TO CYBER SECURITY

Received December 18, 2019, accepted January 8, 2020, date of publication January 13, 2020, date of current version January 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2966264

Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz

TAO LI, BAOXIANG DU, AND XIAOWEN LIANG
Electronic Engineering College, Heilongjiang University, Harbin 150080, China

Corresponding author: Baoxiang Du (dubaoxiang@hlju.edu.cn)

This work was supported by the Another Special Science and Technology Innovation Project of the Heilongjiang Province Basic Research Basic Research Project in 2019 under Grant KJCX201906.

ABSTRACT In recent years, experts and scholars in the field of information security have attached great importance to the security of image information. They have proposed many image encryption algorithms with higher security. In order to further improve the security level of image encryption algorithm, this paper proposes a new image encryption algorithm based on two-dimensional Lorenz and Logistic. The encryption test of several classic images proves that the algorithm has high security and strong robustness. This paper also analyzes the security of encryption algorithms, such as analysis of the histogram, entropy process of information, examination of correlation, differential attack, key sensitivity test, secret key space analysis, noise attacks, contrast analysis. By comparing the image encryption algorithm proposed in this paper with some existing image encryption algorithms, the encryption algorithm has the characteristics of large secret key space, sensitivity to the key, small correlation coefficient and high contrast. In addition, the encryption algorithm is used. It can also resist noise attacks.

INDEX TERMS Encryption, image decryption, logistic, two-dimensional Lorenz, security analysis.

I. INTRODUCTION

With the increasing demand for multimedia information technology, The security of multimedia is also concerned by us. Image multimedia contains a lot of information, and the image is open in the process of communication, The security of image information will be threatened in the process of transmission, especially in the low security channel. Therefore, improving the security of image information in the process of storage and transmission, and avoiding the leakage of image multimedia information is an urgent problem to be solved.

Some traditional encryption algorithms, such as DES, AES, and RSA, are used in image encryption [1]–[3]. However, the traditional encryption algorithm is less efficient when applied to the system that encrypts a large number of pictures or encrypts video. The chaotic system has superior properties in the field of information encryption. It has sensitivity to initial value conditions, unpredictability and bifurcation complexity. [4], [5] proposes an image encryption algorithm based on chaos theory. Chaos has some complex properties that contribute to the generation of more secure and robust encryption algorithms. Chaotic models include Arnold Cat map, Logistic map, Lorenz, Henon map, and some other models [6]. This complex nature of chaotic mapping can be reflected in the characteristics of certain encryption processes similar to ideal ciphers, such as diffusion, aliasing, balancing, and avalanche [7].

In order to ensure the security of image information in the process of transmission and storage, some encryption algorithms based on chaos theory are proposed and applied to image encryption. Since Matthews [8] published his first chaotic theory-based encryption algorithm in 1989, many image encryption algorithms based on chaos theory have been published. In [9], the author proposes a bit-level encryption system based on one-dimensional chaos theory, which converts the pixel values of images into binary, and uses a Logistic map to generate chaotic sequences to scramble and encrypt them. In [10], chaotic sequence generated by Logistic map was used to scramble pixel positions of the segmented images, so as to achieve the purpose of image encryption. [11] proposed an image encryption algorithm based on Logistic mapping, which mainly used ''scrambling-diffusion'' and multiple iterations to encrypt the image. [12] proposed an image encryption scheme based on double Logistic chaotic map. [13] Using YRBS coding with one-dimensional

The associate editor coordinating the review of this manuscript and approving it for publication was Vincenzo Piuri.

Logistic mapping for image encryption. [14] proposed an image encryption algorithm based on interleaved logic diagram (ILM) and deoxyribonucleic acid (DNA) for simultaneous replacement and diffusion of color images. [15] Use pseudo-random sequence generator and improved Logistic mapping to encrypt images. [16] Block image encryption using four-dimensional Logistic mapping and DNA sequence algorithm. [17] proposed a combination of baker map and Logistic map into a two-dimensional chaotic system, and used this algorithm to encrypt the image. [18] proposed an image block encryption algorithm based on Lorenz map and Logistic map. [19] proposed an image encryption algorithm based on improved Logistic mapping. [20] proposed the use of a hyperchaotic system to scramble and diffuse images to achieve the purpose of image encryption. [21] proposed a discrete Lorenz map applied to compressed data, and applied the algorithm in the field of image encryption. [22] Utilizing the characteristics of quaternions, a new S-box was constructed based on the Lorenz system. It is applied in the field of image watermarking. [23] proposed a digital image encryption scheme based on Lorenz chaotic system. [24] proposed an image encryption algorithm based on DNA random coding and Lorenz chaotic mapping. [25] proposed an image encryption algorithm based on multiple chaotic maps. This algorithm uses different keys for four rounds of encryption, which can be used to encrypt grayscale images and color images. In [26], the author proposes an image encryption algorithm based on the optimized Arnold scrambling algorithm and diffusion algorithm, which improves the speed of image encryption and decryption. [27] proposed a fast and secure image encryption algorithm based on a new one-dimensional chaotic system. Multiple chaotic system models were combined to generate pseudo-random sequences, which improved the secret key space and increased the security of the algorithm. In [28], Rossler system is included in an encryption algorithm, which is used to change the pixel value and position of the image, so that the encrypted image has a high uncertainty. Some encryption algorithms combining chaos theory and other theories have been proposed. [29] proposed an image encryption algorithm combining DNA coding and chaos theory. The encryption algorithm has the characteristics of large key space, good cryptographic image statistics, high sensitivity of key and common image, and large information entropy. [30] proposed an image encryption system combining chaotic system and S-box. The system uses segmented linear chaotic map and cubic S-box to generate key stream with excellent statistical features for image encryption. A new index called BACI (Barrier Mean Change Intensity) was proposed as an indicator for sensitivity analysis. [31] proposed a new image encryption algorithm based on chaos and hash SHA-256, which used confusion and diffusion methods to encrypt images. In [32], Sivakumar et al. introduced a new image encryption algorithm based on pixel position displacement and random key flow. In [33], an image encryption algorithm is proposed by combining DNA sequence with chaotic mapping. [34] proposed an image processing algorithm based on discrete wavelet transform and multiple chaos. In [35], the Arnold transform is used to encrypt images with high security. [35] is to randomly divide the image into several parts, and then encode each part by Arnold transform to improve security. [36] Based on the classical confusion-diffusion structure, an image encryption algorithm based on two-dimensional logic-sinusoidal coupling mapping is proposed. In [37], a bit-level image encryption algorithm is constructed using a simple piecewise linear chaotic map.

The structure of this paper is as follows. In the second part, the two-dimensional Lorenz used in the algorithm is briefly introduced. The third part introduces the implementation steps of the algorithm in detail. The fourth part shows the encryption effect of the algorithm on several classical images. In the fifth part, the results obtained by applying the algorithm to some classical images are discussed and compared with those obtained by existing algorithms in literature. In the sixth part, we give some conclusions.

II. TWO-DIMENSIONAL LORENZ CHAOTIC

In recent years, the application of chaotic systems in image encryption has attracted widespread attention. Chaotic systems have many parameters that affect the behavior of the system and are suitable for image encryption algorithms. These parameters have some important uses because they are used as a security key during the encryption process. Small changes in system parameter values may cause the system to enter a chaotic state. The chaotic behavior of such systems is an important basis for constructing cryptographic algorithms. In the encryption algorithm mentioned in this paper, we use two-dimensional Lorenz chaotic system and Logistic chaotic system. These two chaotic mapping algorithms have low complexity. The encryption and decryption scheme proposed in this paper can improve the security of image encryption.

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

$$\begin{cases} x_{1,n+1} = (1 + ah)x_{1,n} - hx_{1,n}x_{2,n} \\ x_{2,n+1} = (1 - h)x_{1,n} + h(x_{1,n})^2 \end{cases} \tag{2}$$

Equation (1) is the Logistic mapping equation, When $3.569945672\cdots\cdots < \mu \leq 4$, the system is in a chaotic state.

Equation (2) is the mapping equation of the two-dimensional discrete Lorenz chaotic system. When the parameters a $\in$ [0.9, 1] and h $\in$ [0.9, 1], the complexity of the system reaches 0.9. In other words, when we use a two-dimensional discrete Lorenz chaotic system for encryption, the parameters can be selected in this parameter range, which is difficult to crack [38].

Figure 1 is a bifurcation diagram of Logistic mapping and two-dimensional Lorenz mapping.

III. THE ALGORITHM

This chapter will introduce in detail the encryption and decryption steps of image encryption using the image encryption algorithm proposed in this article, and show the

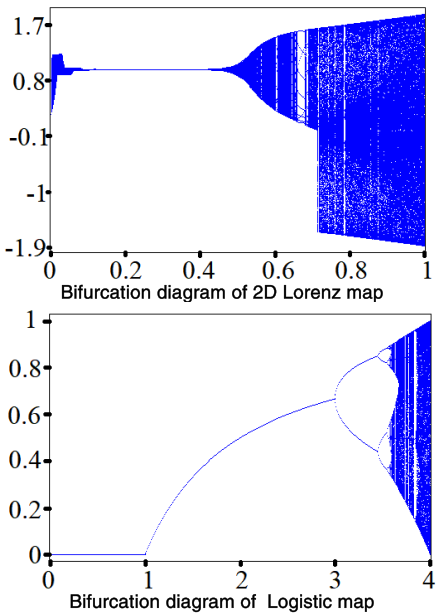

FIGURE 1. Bifurcation diagram of Logistic map and two-dimensional Lorenz map.

TABLE 1. Key scheme 1.

Logistic mapping key		2D Lorenz mapping key					
μ	x_0	μ	x_0	$x_{1,0}$	$x_{2,0}$	a	h
3.9985	0.02	3.9995	0.3	0.11	0.12	0.95	1

encryption and decryption process in detail by setting the key by way of example. Set key scheme 1 as shown in Table 1.

The steps to encrypt the image using this encryption and decryption algorithm are as follows:

Step 1: Read the original image and convert the color image P_{Color} into a grayscale image P_{Gray}. P_{Gray} can be expressed as:

$$P_{Color} = \begin{pmatrix} P_{i1,j1} & P_{i1,j2} & \cdots & P_{i1,jn} \\ P_{i2,j1} & P_{i2,j2} & \cdots & P_{i2,jn} \\ \cdots & \cdots & \cdots & \cdots \\ P_{im,j1} & P_{im,j2} & \cdots & P_{im,jn} \end{pmatrix}$$

Step 2: Convert the pixel value of P_{Gray} from decimal to binary representation, that is, $P_{GrayBin}$.

Step 3: Use Logistic to generate two sets of chaotic sequences X_H and X_V, $X_H = \{X_{H1}, X_{H2}, X_{H3}, \ldots, X_{Hm}\}$, $X_V = \{X_{V1}, X_{V2}, X_{V3}, \ldots, X_{V8n}\}$.

Step 4: Use two sets of chaotic sequences X_H and X_V to scramble the rows and columns of $P_{GrayBin}$ to obtain P_{En1Bin}, and the corresponding decimal image is represented as P_{En1Dec}.

$$P_{En1Bin} = \begin{pmatrix} p_{h1,v1} & p_{h1,v2} & \cdots & p_{h1,v8n} \\ p_{h2,v1} & p_{h2,v2} & \cdots & p_{h2,v8n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{hm,v1} & p_{im,v2} & \cdots & p_{hm,v8n} \end{pmatrix}$$

$$P_{En1Dec} = \begin{pmatrix} p_{H1,V1} & p_{H1,V2} & \cdots & p_{H1,Vn} \\ p_{H2,V1} & p_{H2,V2} & \cdots & p_{H2,Vn} \\ \cdots & \cdots & \cdots & \cdots \\ p_{Hm,V1} & p_{Hm,V2} & \cdots & p_{Hm,Vn} \end{pmatrix}$$

where $P_{Hi,Vj} = \text{bin2dec}(P_{hi,j\times8-7}P_{hi,j\times8-6}P_{hi,j\times8-5}P_{hi,j\times8-4}P_{hi,j\times8-3}P_{hi,j\times8-2}P_{hi,j\times8-1}P_{hi,j\times8})$.

Step 5: Convert P_{En1Bin} from two-dimensional to one-dimensional sequence $P_{En1Bin1D}$, $P_{En1Bin1D} = \{p1, p2, p3, \ldots\ldots, pmn, \}$.

Step 6: Use equation 2 to generate two-dimensional chaotic sequences X_1 and X_2, $X_1 = \{X_{1,1}, X_{1,2}, X_{1,3}, \ldots\ldots, X_{1,mn}\}$, $X_2 = \{X_{2,1}, X_{2,2}, X_{2,3}, \ldots\ldots, X_{2,mn}\}$.

Step 7: Process X_1 and X_2 using equation 3:

$$X_i = floor(\text{mod}(X_i \times 10^{14}), 256) \quad (3)$$

where i = 1, 2.

Step 8: Convert X_1 and X_2 after step 7 into binary representation. Get the binary sequence: B_1 and B_2.

Step 9: Bitwise XOR the P_{En1Bin} and B_1 to obtain E_1 = bitxor (P_{En1Bin}, B_1).

Step 10: Bitwise XOR the E_1 and B_2 to get E_2 = bitxor (E_1, B_2).

Step 11: Convert binary E2 into decimal and convert it into two-dimensional E. E is the encrypted image.Step 2: generating two sets of chaotic sequences using two-dimensional Lorenz, and performing serial XOR with the result of step one;

$$\mathbf{E} = \begin{pmatrix} E_{i1,j1} & E_{i1,j2} & \cdots & E_{i1,jn} \\ E_{i2,j1} & E_{i2,j2} & \cdots & E_{i2,jn} \\ \cdots & \cdots & \cdots & \cdots \\ E_{im,j1} & E_{im,j2} & \cdots & E_{im,jn} \end{pmatrix}$$

Taking the Lena (256 × 256) image as an example, the key scheme 1 is used as the encryption key. The encryption step diagram is shown in Figure 2.

The steps to decrypt an image using this encryption and decryption algorithm are as follows:

Step 1: Obtain the ciphertext image E, and convert E into a one-dimensional sequence Edec1D.

Step 2: Convert E_{dec1D} into binary one-dimensional sequence E_{bin1D}.

Step 3: Use equation 2 to generate two-dimensional chaotic sequences X_1 and X_2, $X_1 = \{X_{1,1}, X_{1,2}, X_{1,3}, \ldots\ldots, X_{1,mn}\}$, $X_2 = \{X_{2,1}, X_{2,2}, X_{2,3}, \ldots\ldots, X_{2,mn}\}$.

Step 4: Process X_1 and X_2 using equation 3.

Step 5: Convert X_1 and X_2 after step 4 into binary representation. Get the binary sequence: B1 and B2.

Step 6: Bitwise XOR the E_{bin1D} and B_2 to obtain C_1 = bitxor (E_{bin1D}, B_1).

Step 7: Bitwise XOR the C_1 and B_1 to get C_2 = bitxor (C_1, B_2).

Step 8: Convert one-dimensional sequence C_2 to two-dimensional sequence $C_{22D_\circ}$

Step 9: Use Logistic to generate two sets of chaotic sequences X_H and X_V, $X_H = \{X_{H1}, X_{H2}, X_{H3}, \ldots, X_{Hm}\}$, $X_V = \{X_{V1}, X_{V2}, X_{V3}, \ldots, X_{V8n}\}$.

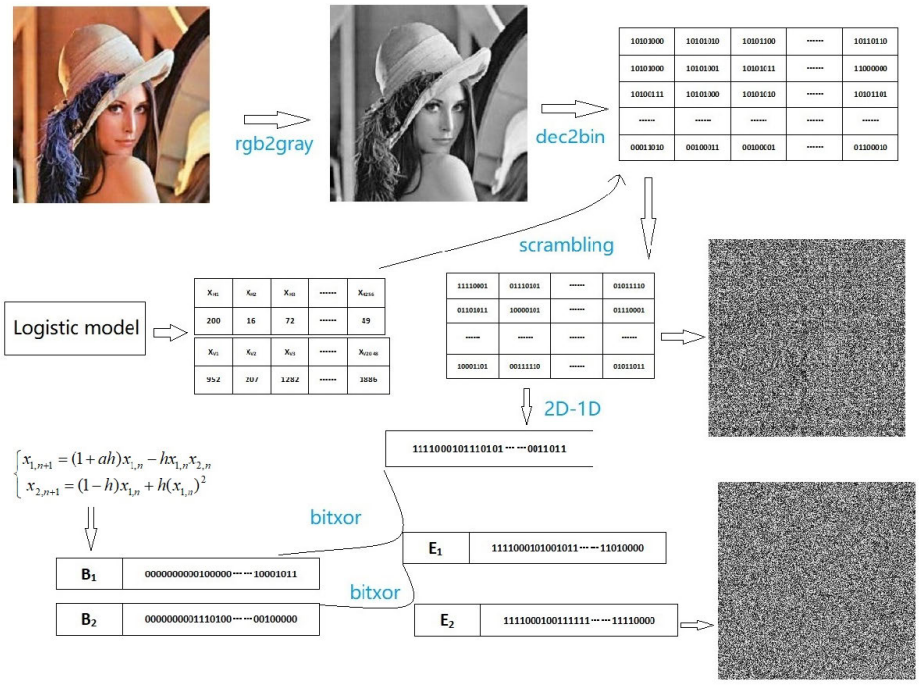

FIGURE 2. Encryption step diagram (Lena 256 × 256, Keys: scheme 1).

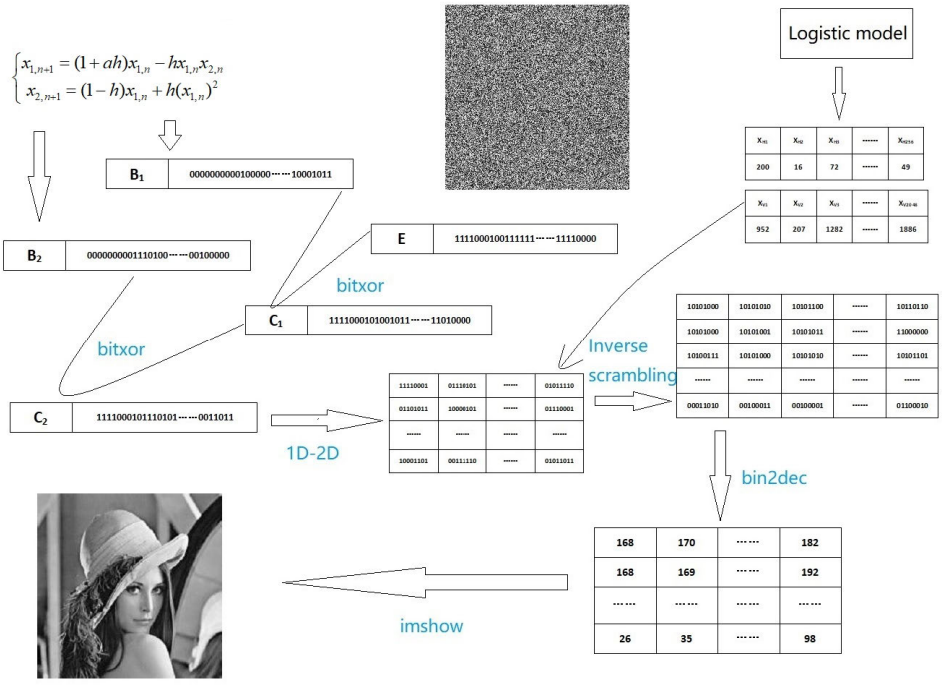

FIGURE 3. Decryption step diagram (Lena 256 × 256, Keys: scheme 1).

Step 10: Use X_H and X_V to reversely scramble the rows and columns of C_{22D} to obtain C_{2c2D}.

Step 11: Convert the binary pixel value C_{2c2D} into a decimal pixel value C, where C is the decrypted image.

Taking Lena (256 × 256) image as an example, the key scheme 1 is used as the decryption key. The decryption steps are shown in Figure 3.

IV. EXPERIMENTAL ANALYSIS

In order to prove the applicability of the image encryption and decryption algorithms proposed in this article, this chapter will use the encryption algorithm proposed in this article to encrypt and decrypt several classic images, including Lena (128 × 128, 256 × 256, 512 × 512), Barbara (256 × 256), airplane (512 × 512), boat (512 × 512), baboon (512 × 512),

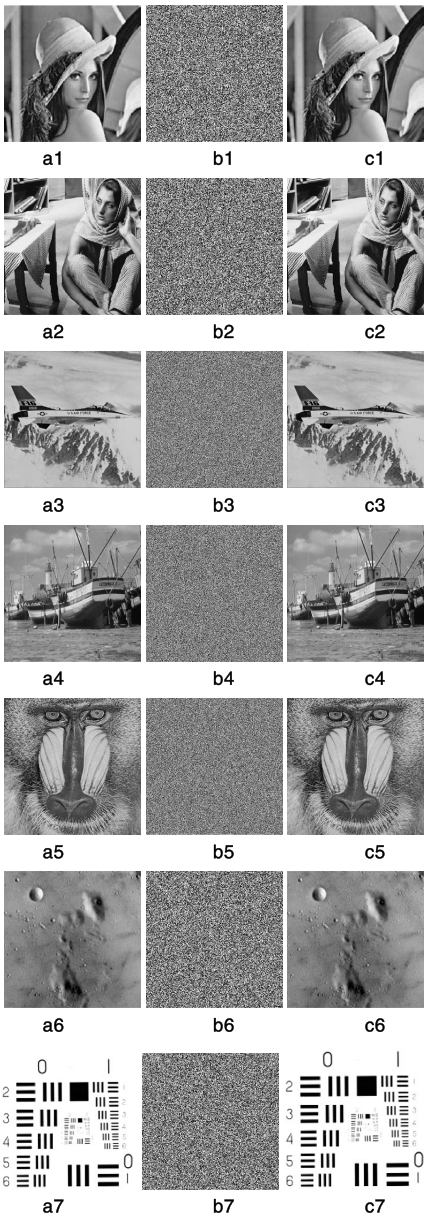

FIGURE 4. Encrypt and decrypt images(Keys: scheme 1). (a) is the original image, (b) is the encrypted image, and (c) is the decrypted image.

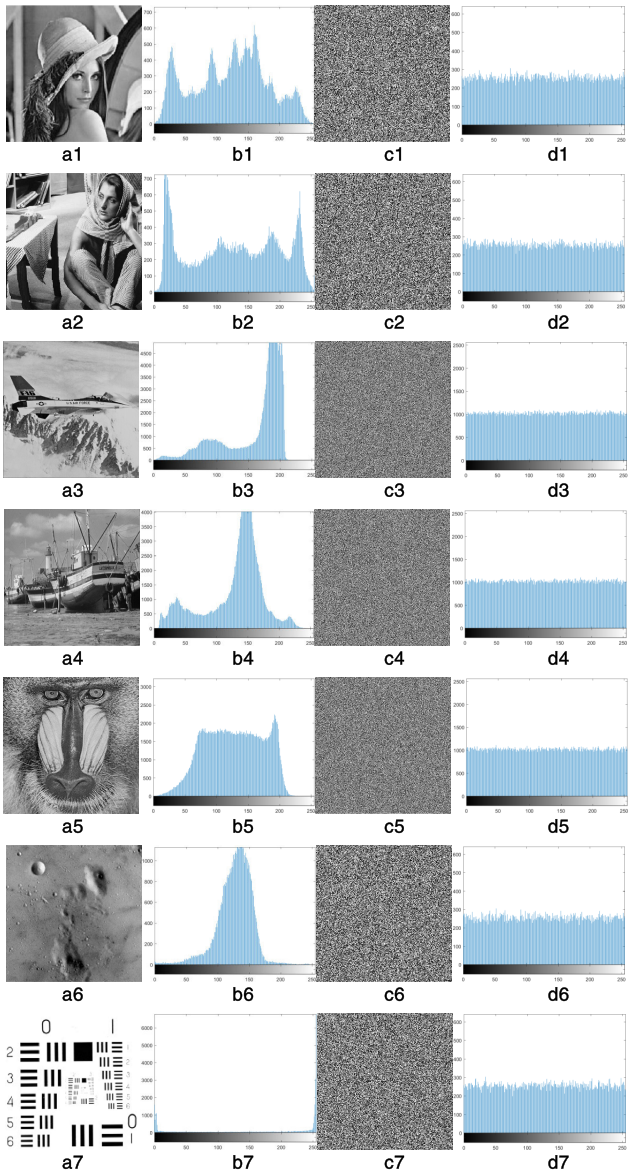

FIGURE 5. Comparison of gray histogram between original image and ciphertext image (Keys: scheme 1). (a) is the original image, (b) is the gray histogram of the original image, (c) is the encrypted image, and (d) is the gray histogram of the encrypted image.

moon surface (256 × 256), and resolution chart (256 × 256). Use key scheme one as the encryption key and the decryption key. The encryption and decryption effect diagram is shown in Figure 4.

V. SECURITY ANALYSIS

In image encryption, a good encryption algorithm needs the following characteristics: after encryption, the gray histogram of ciphertext image is more average; Good entropy of information; Low correlation of ciphertext; Can resist differential attack; High sensitivity to secret keys; The secret key space is large enough; Anti-noise attack and so on. This chapter will test the image encryption algorithm in this paper.

A. STATISTICAL ANALYSIS

1) ANALYSIS OF THE HISTOGRAM

The gray level histogram reflects the relationship between each gray level in the digital image and its frequency of occurrence. It can describe the overview of the image. Figure 5 is a comparison of the gray level histograms of plain text and cipher text of several classic images.

2) ENTROPY PROCESS OF INFORMATION

Entropy can describe the chaos of data in statistics. It can be used to calculate the entropy of ciphertext images to measure the pros and cons of image encryption algorithms. For the source of symbol S, the process of entropy is represented by

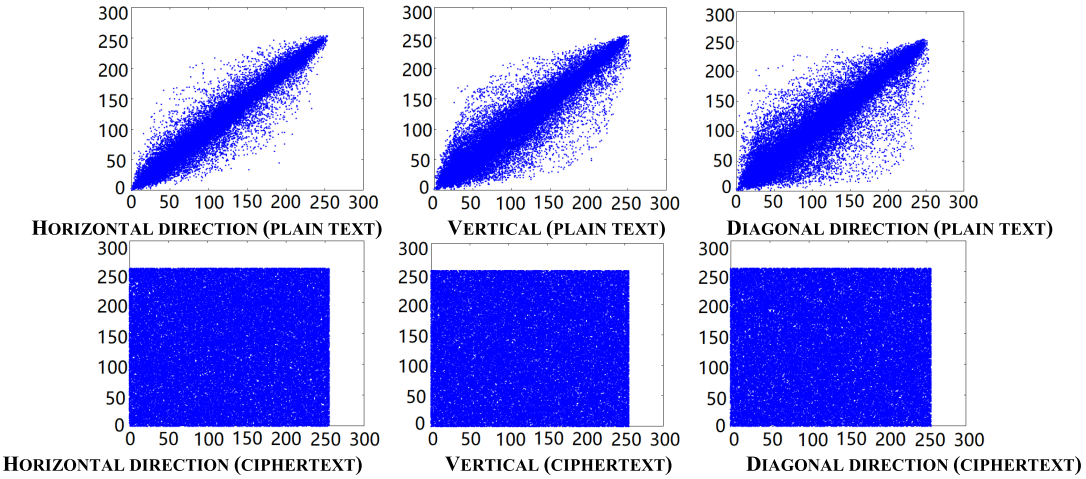

FIGURE 6. Correlation of plain text and cipher text in horizontal, vertical and diagonal components of Lena image (Keys: scheme 1).

TABLE 2. Comparison of information entropy between plaintext and ciphertext images (keys: scheme 1).

image	entropy	
	Plaintext image	Ciphertext image
Lena (128×128)	7.7872	7.9809
Lena (256×256)	7.7488	7.9894
Lena (512×512)	7.7545	7.9916
Barbara (256×256)	7.8046	7.9893
Airplabe (512×512)	6.7059	7.9916
Boat (512×512)	7.1901	7.9916
Baboon (512×512)	7.4273	7.9914
Moon surface (256×256)	6.6876	7.9886
Resolution chart (256×256)	3.0738	7.9895

H [39], and the equation is as follows:

$$H(S) = -\sum_{i=0}^{N-1} p(s_i)\log_2 p(s_i) \tag{4}$$

where $p(s_i)$ is the probability of sign s_i. For images with the same probability, when $N = 256 = 2^8$ and 8bit represents the gray scale, the theoretical value of entropy H(S) is 8. Information entropy shows the distribution of gray values. Table 2 is a test of the information entropy of the plaintext image and the ciphertext image of the image encryption scheme proposed in this paper. Table 3 is a comparison of several algorithms.

3) EXAMINATION OF CORRELATION

The correlation between adjacent pixels of the original image is high. The encryption effect can be detected by calculating and comparing the correlation between the original video image and the encrypted video image [40]. The correlation between two adjacent pixels can be calculated by equation (5).

$$\rho_{AB} = \frac{Conv(A,B)}{\sqrt{D(A)}\sqrt{D(B)}} \tag{5}$$

where: A and B are pixel values of two adjacent positions.

$$Conv(A,B) = \frac{1}{N}\sum_{i=1}^{N}[A_i - E(A)][B_i - E(B)]$$

$$D(A) = \frac{1}{N}\sum_{i=1}^{N}[A_i - E(A)]^2$$

$$E(A) = \frac{1}{N}\sum_{1}^{N}A_i$$

Taking Lena (256 × 256) image as an experimental object, the correlation between the plaintext image and the ciphertext image using the encryption algorithm in the horizontal, vertical and diagonal directions was tested. Table 4 compares the correlation between Lena (256 × 256) encryption using the proposed encryption algorithm and other encryption algorithms. Table 5 shows the plaintext and ciphertext correlation test of several classic images. Figure 6 shows the correlation between the horizontal, vertical, and diagonal directions of the Lena image before and after encryption.

B. STATISTICAL ANALYSIS

High-security encryption algorithms should be highly sensitive to keys, and small changes in the key or the original image will produce completely different encrypted images [42].

1) DIFFERENTIAL ATTACK

In order to better understand the influence of the change of a single pixel in a cryptographic image on a cryptographic image, measurement methods such as NPCR (pixel number change rate) and UACI (uniform average change intensity)

TABLE 3. Comparison of information entropy of different encryption algorithms.

Image	entropy								
	proposed	[6]	[7]	[36]	[37]	[41]	[45]	Logistic	Lorenz
Lena (256×256)	7.9894	7.9887	7.9994	-	7.9974	7.9969	7.9976	7.9823	7.9894
Airplabe (512×512)	7.9916	-	7.9996	7.9020	-	7.9994	-	7.9678	7.9916
Moon surface (256×256)	7.9886	-	7.9982	7.9023	-	7.9972	-	7.9829	7.9891
Resolution chart (256×256)	7.9895	-	7.9980	7.9023	-	7.9972	-	5.0149	7.9897

TABLE 4. Correlation comparison of different encryption algorithms.

		Plain image	Cipher image							
			proposed	[6]	[7]	[36]	[37]	[41]	[45]	Logistic	Lorenz
Lena (256×256)	H	0.9381	0.0044	0.0216	0.0005	-	-0.0230	0.0077	-0.0027	0.0186	-0.0022
	V	0.9810	0.0015	0.2065	0.0017	-	0.0019	0.0168	-0.0111	0.0169	-0.0039
	D	0.9770	0.0019	0.0463	0.0025	-	-0.0034	0.0104	0.0014	0.0024	0.0061

are used [7]:

$$NPRC = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{6}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|I_1(i,j) - I_2(i,j)|}{255}\right] \times 100\% \tag{7}$$

where,

$$D(i,j) = \begin{cases} 1, & if\ (I_1(i,j) \neq I_2(i,j)) \\ 0, & otherwrise \end{cases} \tag{8}$$

I_1 and I_2 represent the encrypted ciphertext image of the original image and the original image that arbitrarily changes the pixel value of a pixel point through encryption algorithm. W and H represent the width and height of the image respectively. Generally speaking, the NPCR value of chaotic image encryption algorithm needs to be greater than 90% and UACI value greater than 33% to ensure the security of the algorithm. Table 6 shows UACI and NPRC for encryption algorithm validation.

2) KEY SENSITIVITY TEST

A highly secure encryption algorithm should be highly sensitive to the key. When the decryption key is slightly different from the encryption key, the encryption and decryption algorithm cannot correctly decrypt the image, and it cannot obtain any original image in the wrong decrypted image. Relevant effective information.

In order to test the key sensitivity of the image encryption algorithm, the encryption key is set to key scheme 1, the decryption key is set to key scheme 2, and the key of scheme 2 is shown in Table 7. That is, only the value of the key h in the keys of the two-dimensional chaotic system is changed, and the size is changed to 0.000000001, and the remaining keys are not changed. Figure 7 shows the results of three images encryption and error encryption using this test scheme, and the correlation between the incorrectly encrypted image and the original image is calculated. Table 8 shows the correlation.

TABLE 5. Correlation between plaintext and ciphertext images in the horizontal, vertical and diagonal directions (keys: scheme 1).

Image		Plain image	Cipher image
Lena (128×128)	H	0.7988	-7.4202e-4
	V	0.9287	0.0019
	D	0.9059	-0.0343
Lena (256×256)	H	0.9381	0.0044
	V	0.9810	0.0015
	D	0.9770	0.0019
Lena (512×512)	H	0.9829	-7.4202e-4
	V	0.9949	0.0019
	D	0.9942	-0.0.43
Barbara (256×256)	H	0.8121	-6.8985e-4
	V	0.8708	0.0023
	D	0.9191	-0.0283
Airplabe (512×512)	H	0.9670	0.0011
	V	0.9639	0.0032
	D	0.9557	0.0169
Boat (512×512)	H	0.9443	0.0025
	V	0.9428	7.9976e-4
	D	0.9810	0.0326
Baboon (512×512)	H	0.9328	8.5747e-4
	V	0.9221	5.7689e-5
	D	0.9322	-0.0069
Moon surface (256×256)	H	0.9500	-0.0063
	V	0.9336	-0.0019
	D	0.9217	-0.0682
Resolution chart (256×256)	H	0.9670	-0.0087
	V	0.8894	0.0024
	D	0.8817	0.0711

C. THE ANALYSIS OF OUR KEY SPACE

A high-security encryption algorithm should have a large enough key space to resist exhaustive attacks. A high-security encryption algorithm should have a key space greater than 2^{100} [43]. The two sets of chaotic sequences used for bit-level row and column scrambling in this algorithm are generated by the Logistic model, and the key includes two sets of x_0 and r_0. In addition, the two-dimensional chaotic model has four initial values $x_{1,0}$, $x_{2,0}$, a, h. Therefore, the key in the image encryption algorithm proposed in this paper consists of 8 values. Therefore, the size of the key space of the algorithm is 10^{112}, far exceeding 2^{100}. Table 9 shows that the key

TABLE 6. Comparison of the Number of Pixels Change Rate (NPCR) and Unifified Average Changing Intensity (UACI) of the lena (256 × 256), barbara (256 × 256), and resolution chart (256 × 256) images with size 256 × 256 using our proposed algorithm and other algorithms.

Cipher algorithm	NPRC	UACI
lena 256×256	99.66%	33.42%
barbara 256×256	99.67%	33.43%
resolution chart (256×256	99.63%	33.42%
[7]	99.60%	33.43%
[36]	99.60%	33.46%
[37]	99.62%	33.51%
[41]	99.59%	30.63%
[45]	-	-
Logistic	99.61%	33.40%
Lorenz	99.58%	33.42%

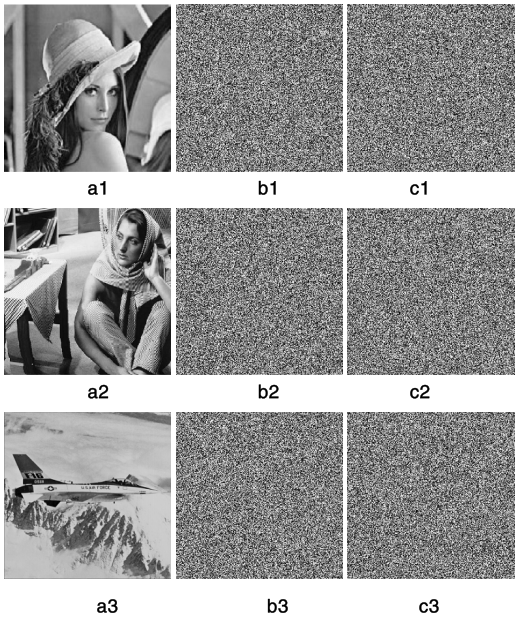

FIGURE 7. Key sensitivity test (Encryption key: scheme 1, decryption key: scheme 2). (a) is the original image, (b) is the encrypted image, and (c) is the wrongly decrypted image.

TABLE 7. Key scheme 2.

Logistic mapping key				2D Lorenz mapping key			
μ	x_0	μ	x_0	$x_{1,0}$	$x_{2,0}$	a	h
3.9985	0.02	3.9995	0.3	0.11	0.12	0.95	0.9999999999

TABLE 8. Correlation between the original image and the incorrectly decrypted image.

image	lena	barbara	Moon surface
The correlation	-0.0062	0.0029	0.0044

space of our proposed algorithm is larger than the key space in [6], [36], [37]. Therefore, the key space of our algorithm is large enough to resist exhaustive attacks.

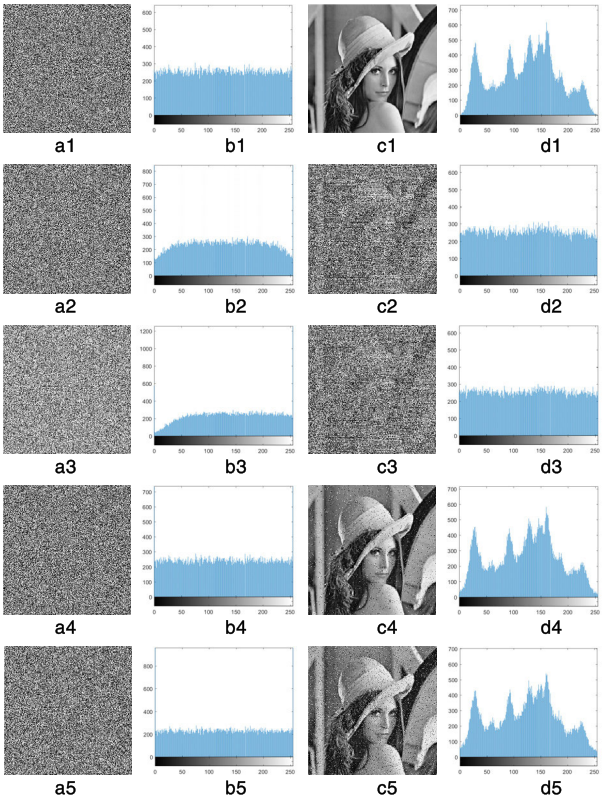

FIGURE 8. (a1) is the original ciphertext image, (a2) ∼(a5) is the ciphertext image under different noise attacks, (b) is the grayscale histogram of ciphertext, (c1) is the decryption image of ciphertext image without noise attacks, (c2) ∼(c5) is the decryption image of ciphertext image under different noise attacks. (d) is the gray histogram of the decrypted image.

D. NOISE ATTACKS

This section will detect two classical noise algorithms for image encryption and decryption proposed in this paper. Gaussian noise and pepper and salt noise are used to attack the encrypted ciphertext images respectively. These noises are: Gaussian noise with variance of 0.01 and 0.1, and pepper and salt noise with density of 0.05 and 0.1, respectively. Their mean square error (MSE) and peak signal to noise ratio (PSRN) were measured by equation 9 and equation 10.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - Y_{ij})^2 \tag{9}$$

$$PSRN = 10 \times \log_{10}(\frac{I^2}{MSE}) \tag{10}$$

where X represents the image after decryption of the ciphertext after being attacked by noise, and Y represents the image after decryption of the ciphertext without being attacked by noise. M and N represent the number of pixels in the rows and columns of the image, respectively. I represents the pixel value with the highest probability of occurrence in the image. Table 10 shows the comparison of the mean square error

TABLE 9. Encryption algorithm secret key space comparison.

algorithm	Proposed	[6]	[7]	[36]	[37]	[41]	[45]	Logistic	Lorenz
Key Space	10^{112}	10^{84}	10^{140}	$2^{256} \approx 1.16\times10^{77}$	$2^{210} \approx 1.65\times10^{63}$	10^{140}	$2^{320} \approx 2.136\times10^{96}$	10^{50}	10^{62}

TABLE 10. Noise attack contrast.

noise		Proposed	[7]	[44]	Logistic	Lorenz
Gaussian noise with variance = 0.01 and mean = 0	MSE	105.0683	2321.4	4410.1	103.5671	82.8773
	PSRN	23.8677	14.5	11.7	23.302	24.8980
Gaussian noise with variance = 0.1 and mean = 0	MSE	106.0403	5201.2	5631.4	87.6134	92.1036
	PSRN	23.8277	11.0	10.6	24.6567	24.4396
Salt and pepper noise With density 0.05	MSE	12.2870	437.9	869.9	12.4648	5.5721
	PSRN	33.1880	21.7	18.7	33.1255	36.6222
Salt and pepper noise With density 0.1	MSE	24.2675	893.1	1829.6	24.4329	11.4071
	PSRN	30.2321	18.6	15.5	30.2077	33.5106

TABLE 11. Contrast analysis of plaintext and ciphertext (Keys: scheme 1).

image	contrast	
	Plain image	Cipher image
Lena (256×256)	0.3563	10.6320
Barbara (256×256)	0.9617	10.6184
Baboon (512×512)	0.6249	10.6279

and peak signal-to-noise ratio of this algorithm with other encryption algorithms. Figure 8 shows the decryption effect of the Lena graph after being subjected to different types of noise attacks.

Figure 8 shows the decryption effect of Lena diagram under different types of noise attacks.

E. CONTRAST ANALYSIS

The gray level co-occurrence matrix is generated from the gray level image, and the gray level co-occurrence matrix is detected by equation 11 to observe the contrast of the encrypted image.

$$C = \sum_{i,j} |i-j|^2 p(i,j) \tag{11}$$

where P(i,j) represents the number of grayscale worth in the grayscale co-occurrence matrix.

Table 11 is a comparative analysis of the encryption of several classic images using the encryption algorithm proposed in this paper. Table 12 is a comparative analysis of Lena image encryption using the encryption algorithm proposed in this article and other encryption algorithms.

F. GRAY VALUE DEGREE ANALYSIS

Gray image can be analyzed by comparing the pixel difference between a pixel point in the image and its four surrounding pixels. Gray-scale analysis of the image is carried out by calculating equation 12, equation 13 and equation 14 [7].

$$G(x,y) = \frac{\sum \left| I(x,y) - I(\ddot{x}, \ddot{y}) \right|^2}{4},$$

$$(\ddot{x}, \ddot{y}) = \begin{cases} (x-1, y) \\ (x+1, y) \\ (x, y-1) \\ (x, y+1) \end{cases} \tag{12}$$

$$\bar{I}(x,y) = \frac{\sum_{x=2}^{M-1} \sum_{y=2}^{N-1} G(x,y)}{(M-2)\times(N-2)} \tag{13}$$

$$GVD = \frac{\ddot{I}(x,y) - \bar{I}(x,y)}{\ddot{I}(x,y) + \bar{I}(x,y)} \tag{14}$$

where, $\ddot{I}$ represents the average of four adjacent pixel points, and $\bar{I}$ represents the average of the encrypted image. Table 13 shows the gray-level values detected by the encryption algorithm proposed in this paper for several classic images, and table 14 shows the image gray-level values of different encryption algorithms.

G. COMPUTATIONAL COMLIEXITY ANALYSIS

Use MATLAB software to analyze the computational complexity of the algorithm, select three pixel lena plots (128 × 128, 256 × 256, 512 × 512), and use a computer (Intel (R) Core (TM) i5-5200U processor 2.2 GHz) was used to test the algorithm encryption time using MATLAB R2016a. The test results are shown in Table 15.

H. TEST FOR RSSISTANCE TO SHEAR ATTACKS

In order to achieve effective protection of digital image information, anti-shearing attacks can test the effect of image data transmission on channels with poor quality. In order to resist malicious cutting or graffiti attacks, experimental detection proves that the encryption scheme is anti-shearing. Offensive ability. Figure 9 shows the detection of anti-shear attack.

I. TEST FOR RSSISTANCE TO SHEAR ATTACKS

The reset value of the ciphertext image encrypted by the encryption algorithm with higher security should be evenly distributed. Local Shannon entropy (LSE) can be used to test the degree of uniform distribution of median values in

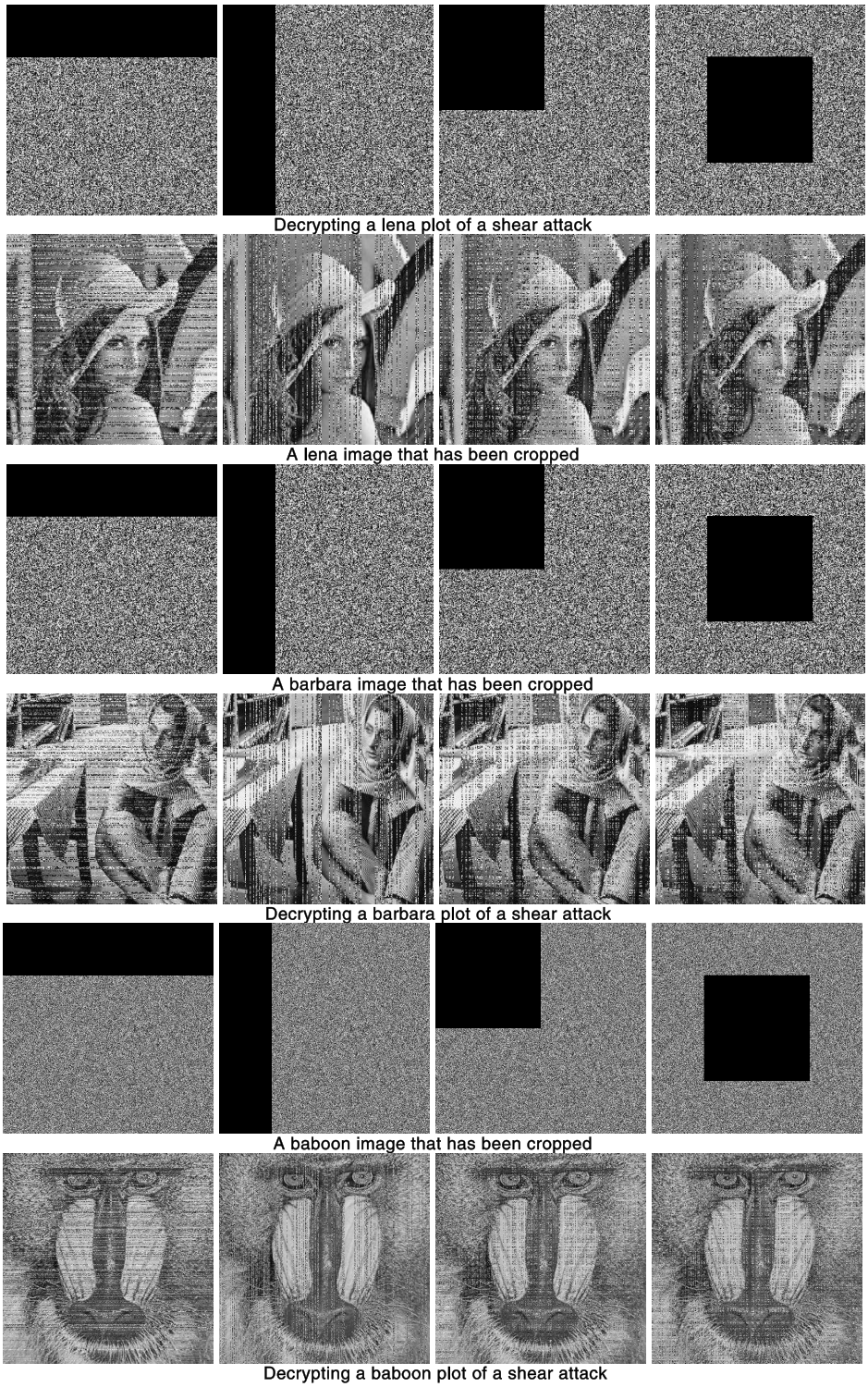

FIGURE 9. Shear attack detection.

ciphertext images. For a ciphertext image I, randomly select k pixels of non-overlapping pixel blocks with a number of T_B, and the local entropy calculation formula is:

$$\overline{H_{k,T_B}}(I) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{15}$$

where, the calculation method of $H(S_i)$ is formula (4). Table 16 shows the test results of local Shannon entropy.

VI. APPLIICATION IN YHE FIELD OF COLOR ENCRYPTION

The image encryption scheme designed in this paper can be used to encrypt grayscale images, as well as color

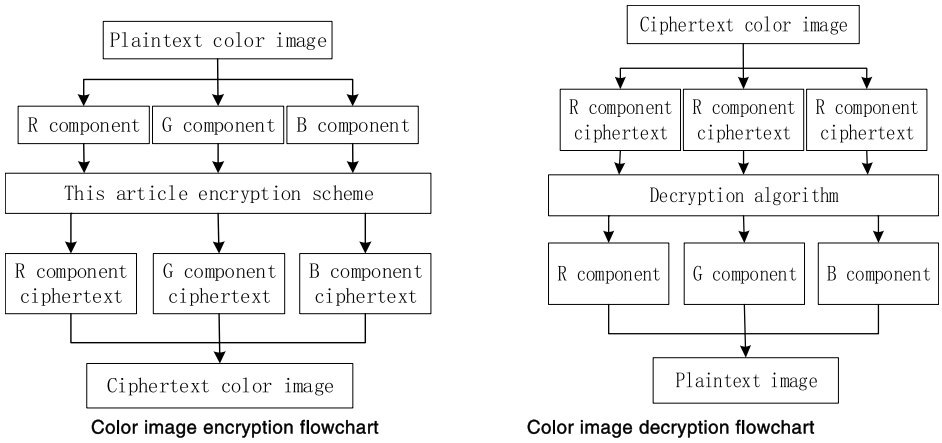

FIGURE 10. Color image encryption and encryption flowchart.

FIGURE 11. Effect of color image encryption and decryption.

images. The color image encryption step is: separating the R component, G component and B component of the color image, encrypting the three components separately using the proposed scheme for gray image encryption, and finally combining the ciphertext image into a color ciphertext image. The decryption algorithm is the inverse process of the encryption algorithm. The encryption and decryption process is shown in Figure 10.

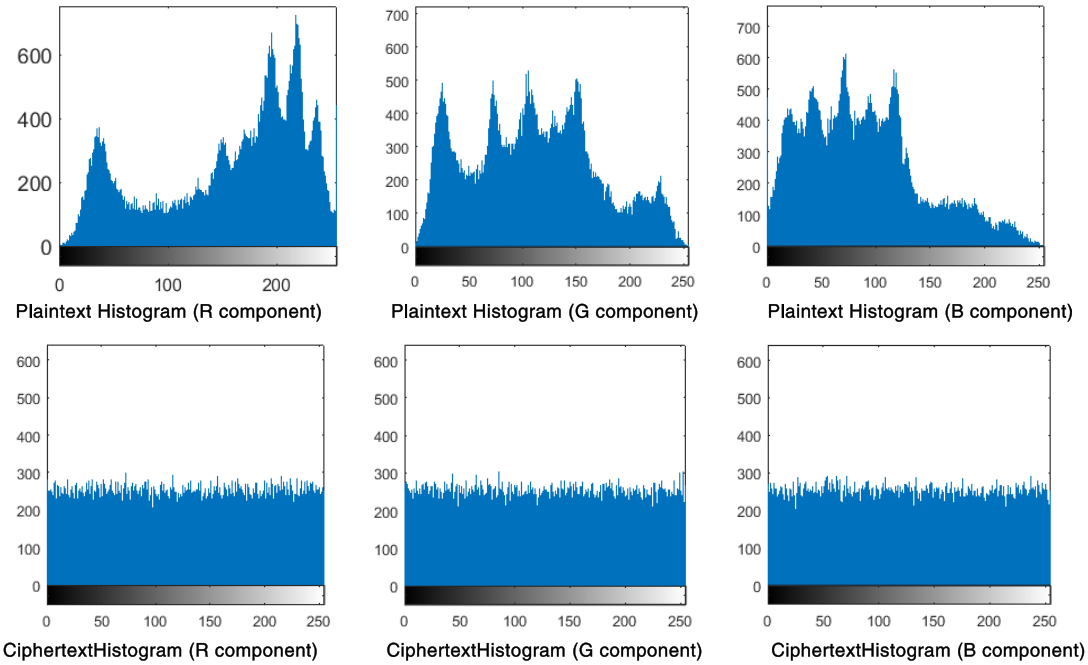

FIGURE 12. Histograms of R, G, and B components of color plaintext and ciphertext images.

TABLE 12. Contrast analysis of the plain (Lena (256 × 256)) and cipher image using the proposed algorithm (Keys: scheme 1) and someone else's algorithm.

image	contrast						
	Plain image	Cipher image					
		Our algorithm	[7]	[36]	[41]	Logistic	Lorenz
Lena	0.3563	10.6320	10.6201	10.5034	10.4767	10.2665	10.5675

TABLE 13. Gray value degree for different test images.

image	GVD value
Lena	0.9684
Barbara	0.9791
Moon surface	0.9631
airplane	0.9478
baboon	0.9843
boat	0.9612

TABLE 14. GVD analysis of the proposed algorithm with other algorithms.

image	GVD					
	Our Algorithm	[7]	[45]	[46]	Logistic	Lorenz
Lena	0.9684	0.9653	0.9540	0.9624	0.9615	0.9614

TABLE 15. Computational complexity analysis (ms).

	Bit-Scramble	Diffusion	Total	[6]
Lena(128×128)	32.982	11.261	44.243	-
Lena(256×256)	68.884	44.119	113.003	186.933
Lena(512×512)	294.693	165.782	460.475	1110.333

Select several color images to verify the encryption and decryption effect. The encryption and decryption effect is shown in Figure 11. Select lena (256 × 256) to test the grayscale histograms of the R, G, and B components of the plaintext and ciphertext images, as shown in Figure 12.

TABLE 16. Local shannon entropy test.

image	LSE
Lena	7.902812
Barbara	7.904017
Moon surface	7.902392
airplane	7.901678
baboon	7.901945
boat	7.902412

VII. CONCLUSION

In this paper, an image encryption algorithm is proposed. The classical chaotic model is used in the encryption algorithm to generate two sets of chaotic sequences to encrypt the image. The two-dimensional Lorenz chaotic model is used to generate chaotic sequences to encrypt and encrypt the image. Through the security analysis in Chapter 5, it can be concluded that the image encryption algorithm proposed in this paper is sensitive to the secret key and has a large secret key space. It can resist exhaustive attacks to a high degree and can resist noise interference. The algorithm has strong

security and robustness and is suitable for image encryption with high security level.

REFERENCES

[1] P. Zhan and X. Xie, "Implementation of DES and AES algorithms and their efficiency in image encryption," *Netw. Secur. Technol. Appl.*, vol. 9, pp. 41–42, 2018.
[2] N. Islam, Z. Shahid, and W. Puech, "Denoising and error correction in noisy AES-encrypted images using statistical measures," *Signal Process., Image Commun.*, vol. 41, pp. 15–27, Feb. 2016.
[3] A. Chatterjee, J. Dhanotia, V. Bhatia, S. Rana, and S. Prakash, "Optical image encryption using fringe projection profilometry, Fourier fringe analysis, and RSA algorithm," in *Proc. 14th IEEE India Council Int. Conf. (INDICON)*, Roorkee, India, Dec. 2017, pp. 1–5.
[4] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 144, pp. 444–452, Mar. 2018.
[5] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Process.*, vol. 148, pp. 124–144, Jul. 2018.
[6] S. S. Askar, A. A. Karawia, and A. Alshamrani, "Image encryption algorithm based on chaotic economic model," *Math. Problems Eng.*, vol. 2015, Dec. 2015, Art. No. 341729.
[7] S. Askar, A. Karawia, A. Al-Khedhairi, and F. Al-Ammar, "An algorithm of image encryption using logistic and two-dimensional chaotic economic maps," *Entropy*, vol. 21, no. 1, p. 44, Jan. 2019.
[8] R. Matthews, "On the derivation of a chaotic encryption algorithm," *Cryptologia*, vol. 13, pp. 29–42, Jan. 1989.
[9] C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 12027–12042, May 2019.
[10] E. Xu, L. Shao, G. Cao, Y. Ren, and T. Qu, "A new method of information encryption," in *Proc. Int. Colloq. Comput., Commun., Control, Manage.*, Sanya, China, vol. 4, Aug. 2009, pp. 583–586.
[11] F. Zhao, C. Li, C. Liu, J. Zhang, and Q. Hu, "Analysis of the effects of scrambling and diffusion of logistic chaotic map on image encryption," in *Proc. Int. Conf. Digit. Image Process.*, 2019.
[12] H. Pan, Y. Lei, and C. Jian, "Research on digital image encryption algorithm based on double logistic chaotic map," *EURASIP J. Image Video Process.*, vol. 2018, no. 1, p. 142, 2018.
[13] S. Rajagopalan, S. Sharma, S. Arumugham, H. Upadhyay, J. Rayappan, and R. Amirtharajan, "YRBS coding with logistic map—A novel Sanskrit aphorism and chaos for image encryption," *Multimedia Tools Appl.*, vol. 78, no. 8, pp. 10513–10541, 2019.
[14] S. Suri and R. Vijay, "A synchronous intertwining logistic map-DNA approach for color image encryption," *J. Ambient Intell. Hum. Comput.*, vol. 10, no. 6, pp. 2277–2290, Jun. 2019.
[15] A. M. Hemdan, O. S. Faragallah, O. Elshakankiry, and A. Elmhalaway, "A fast hybrid image cryptosystem based on random generator and modified logistic map," *Multimedia Tools Appl.*, vol. 78, no. 12, pp. 16177–16193, Jun. 2019.
[16] S. Stalin, P. Maheshwary, P. Shukla, M. Maheshwari, B. Gour, and A. Khare, "Fast and secure medical image encryption based on non linear 4D logistic map and DNA sequences (NL4DLM_DNA)," *J. Med. Syst.*, vol. 43, no. 8, p. 267, 2019.
[17] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools Appl.*, vol. 78, no. 15, pp. 22023–22043, Aug. 2019.
[18] J. Chen, X. Zhang, and H. Zhang, "Image block encryption algorithm based on Lorenz map and logistic map," *J. Guilin Univ. Electron. Technol.*, vol. 39, no. 01, pp. 76–81, 2019.
[19] C. Hun, C. Ruan, and Z. Niu, "Image encryption algorithm based on improved logistic mapping," *Comput. Syst. Appl.*, vol. 28, no. 6, pp. 125–129, 2019.
[20] T Gopalakrishnan, S Ramakrishnan, "Image encryption using hyper-chaotic map for permutation and diffusion by multiple hyper-chaotic maps," *Wireless Pers. Commun.*, vol. 109, no. 1, pp. 437–454, 2019.
[21] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Comput. Appl.*, vol. 31, no. 7, pp. 2395–2405, Jul. 2019.
[22] U. Arshad, S. I. Batool, and M. Amin, "A novel image encryption scheme based on Walsh compressed quantum spinning chaotic lorenz system," *Int. J. Theor. Phys.*, vol. 58, no. 10, pp. 3565–3588, Oct. 2019.
[23] W. Lv, R. Bai, and X. Sun, "Image encryption algorithm based on hyper-chaotic lorenz map and compressed sensing theory," in *Proc. Chin. Control Conf. (CCC)*, Jul. 2019, pp. 371–376.
[24] J. Hua and X. Qu, "Image encryption system using DNA coding and Lorenz chaotic system," *J. Ningde Teachers College, Natural Sci. Ed.*, vol. 31, no. 1, pp. 16–23, 2019.38.
[25] T. Gopalakrishnan and S. Ramakrishnan, "Chaotic image encryption with hash keying as key generator," *IETE J. Res.*, vol. 63, no. 2, pp. 172–187, Mar. 2017.
[26] C. Gao, X. Huang, X. Tang, and B. X. Du, "Chaotic scrambling—Diffusion image encryption algorithm," *J. Natural Sci. Heilongjiang Univ.*, vol. 36, no. 03, pp. 363–370, 2019.
[27] Y. P. K. Nkandeu and A. Tiedeu, "An image encryption algorithm based on substitution technique and chaos mixing," *Multimedia Tools Appl.*, vol. 78, no. 8, pp. 10013–10034, Apr. 2019.
[28] Y. Cao and C. Fu, "An image encryption scheme based on high dimension chaos system," in *Proc. Int. Conf. Intell. Comput. Technol. Automat.*, Changsha, China, vol. 2, Oct. 2008, pp. 104–108.
[29] Y. Zhang, "The image encryption algorithm based on chaos and DNA computing," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 21589–21615, Aug. 2018.
[30] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018.
[31] 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, Sep. 2018.
[32] T. Sivakumar and R. Venkatesan, "Image encryption based on pixel shuffflfling and random key stream," *Int. J. Comput. Inf. Technol.*, vol. 3, pp. 1468–1476, Nov. 2014.
[33] J. Zhang, D. Fang, and H. Ren, "Image encryption algorithm based on DNA encoding and chaotic maps," *Math. Problems Eng.*, vol. 2014, Dec. 2014, Art. no. 917147.
[34] W. Wang, H. Tan, Y. Pang, Z. Li, P. Ran, and J. Wu, "A novel encryption algorithm based on DWT and multichaos mapping," *J. Sens.*, vol. 2016, Mar. 2016, Art. no. 2646205.
[35] J. Zou and T. Weng, "A new image encryption instant communication method based on matrix transformation," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing* (Smart Innovation, Systems and Technologies), vol. 63, J. S. Pan, P. W. Tsai, and H. C. Huang, Eds. Berlin, Germany: Springer, 2017, pp. 321–329.
[36] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.
[37] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.
[38] J. Ran, Y. M. Liu, C. F. Wang, and Z. W. Wang, "Complexity analysis of two-dimensional discrete Lorenz chaotic system," *J. Zunyi Normal Univ.*, vol. 20, no. 4, pp. 81–82, and 99, 2008.
[39] M. Sobhy and A. Shehata, "Methods of attacking chaotic encryption and countermeasures," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Salt Lake City, UT, USA, vol. 2, May 2001, pp. 1001–1004.
[40] K. Shahna and A. Mohamed, "An image encryption technique using logistic map and Z-order curve," in *Proc. Int. Conf. Emerg. Trends Innov. Eng. Technol. Res. (ICETIETR)*, Ernakulam, India, 2018, pp. 1–6.
[41] S. S. Askar, A. A. Karawia, and F. Alammar, "Cryptographic algorithm based on pixel shuffflfling and dynamical chaotic economic map," *IET Image Process.*, vol. 12, pp. 158–167, 2018.
[42] N. Pareek, V. Patidar, and K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, Sep. 2006.
[43] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.*, vol. 285, no. 1, pp. 29–37, Jan. 2012.
[44] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimedia Tools Appl*, vol. 75, no. 17, pp. 10631–10648, Sep. 2016.
[45] G. Hanchinamani and L. Kulakarni, "Image encryption based on 2-D Zaslavskii chaotic map and pseudo Hadmard transform," *Int. J. Hybrid Inf. Technol.*, vol. 7, no. 4, pp. 185–200, 2014.
[46] R. Rhouma, E. Solak, and S. Belghith, "Cryptanalysis of a new substitution–diffusion based image cipher," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, pp. 1887–1892, Jul. 2010.

TAO LI was born in Xiangcheng, Henan, China, in 1996. He received the bachelor's degree in engineering from Henan Urban Construction College in 2018. He is currently pursuing the master's degree in engineering (majoring in electronic and information engineering) with Heilongjiang University. His research direction is information security and video image.

During his undergraduate study from 2011 to 2014, he received provincial awards, invented and authorized a patent for utility model, and participated in University-Level Scientific Research Projects.

BAOXIANG DU received the bachelor's degree in electronic information science and technology from Northeast Normal University in 2002, the master's degree in communication and information systems from Harbin Engineering University in 2009, and the Ph.D. degree in microelectronics and solid state electronics from Heilongjiang University, in 2014. He is currently an Associate Professor with the School of Electronic Engineering, Heilongjiang University. His research interests include information security and secure communications, and analysis and prediction for nonlinear systems.

XIAOWEN LIANG was born in Chengde, Hebei. She received the bachelor's degree in engineering from the Henan Urban Construction College, in 2018. She is currently pursuing the master's degree in machine learning and residue detection with the School of Electronic Engineering, Heilongjiang University.