IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 10, 2021, accepted July 16, 2021, date of publication July 26, 2021, date of current version August 3, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3099214

Chaotic Image Encryption Algorithm Based on Zigzag Transform With Bidirectional Crossover From Random Position

HAO GAO AND XINGYUAN WANG, (Member, IEEE)
School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China

Corresponding author: Xingyuan Wang (xywang@dlmu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672124, in part by the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund under Grant MMJJ20170203, in part by the Liaoning Province Science and Technology Innovation Leading Talents Program Project under Grant XLYC1802013, in part by the Key Research and Development Projects of Liaoning Province under Grant 2019020105-JH2/103, in part by the Jinan City 20 Universities Funding Projects Introducing Innovation Team Program under Grant 2019GXRC031, and in part by the Research Fund of Guangxi Key Laboratory of Multi-Source Information Mining and Security under Grant MIMS20-M-02.

ABSTRACT This paper proposes a Zigzag transform that starts at random positions and crosses bidirectionally (ZZBCRP) to scramble the image. The number of sequence types of this new Zigzag transform is the number of pixels in the plaintext image, which is more and more complicated than other Zigzag transform methods, and Arrangement in a bidirectional crossover method can better disrupt the pixel correlation of the plaintext image. After multiple rounds of Zigzag transformation, the Logistic system is used to generate a sorted sequence to scramble the image. Then the chaotic sequence generated by the hyperchaotic Chen system is used. Perform a reversible diffusion operation on the image, and finally analyze the security of the algorithm.

INDEX TERMS Chaos, image encryption, zigzag transform, one-dimensional logistic chaotic system, hyperchaotic Chen system.

I. INTRODUCTION

In 1963, when Lorenz was simulating meteorological changes, the results were very different due to the slight errors in the input meteorological data. After further research by Lorenz, he published a paper in the "Journal of Atmospheric Sciences" in the same year and proposed the Lorenz system [1], a brand new discipline. Since the birth of chaos theory, more and more scholars are devoted to the research of chaos theory, and it also provides new research methods for other disciplines. Shannon's two papers published in 1948 and 1949 pioneered modern cryptography [2], [3], and pointed out two ways of information encryption, confusion and diffusion. Chaotic systems are sensitive to initial values, long-term unpredictable, and pseudo-random. They are suitable for information hiding in the encryption field. In 1989, Matthews used the chaotic system for encryption for the first time [4], linking chaos theory with cryptography. Pioneered chaotic cryptography. In 1997, Fridrich published a paper [5] using two steps of scrambling and diffusion to encrypt images. Since then, more people have invested in the field of chaotic image encryption [6]–[11]. New encryption ideas and encryption methods have continued to emerge [12]–[17]. Combining two-dimensional compressed sensing and embedding technology, Chai *et al.* [18] proposed an efficient and visually significant two-color image encryption algorithm. A color image encryption system based on improved genetic algorithm and matrix semi-tensor product (STP) is also proposed [19]. Peng *et al.* proposed a discrete memristor model based on the difference theory, and proved the three fingerprint characteristics of the model according to the definition of generalized memristor [20], and based on the improved two-dimensional closed-loop modulation coupling model, proposed a new two-dimensional sinusoidal improved Logistic iterative chaotic mapping (ICMIC) modulation mapping (2D-SLIM) [21]. Chen *et al.* [22] in order to further improve the security under limited accuracy, proposed an improved cryptosystem based on a new two-dimensional

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

chaotic map based on sine map, Chebyshev map and linear function (2D-SCL).

The common practice of Zigzag transformation is to start from one corner of the matrix, scan all elements perpendicular to the diagonal, and then to the diagonal end, generate a one-dimensional vector containing all the elements, and re-create the one-dimensional vector according to certain predetermined rules. Arrange into the original matrix size [23]–[26]. Yang *et al.* [27] proposed that Zigzag traversal of the matrix can be carried out from the four corners, so that Zigzag is expanded from one traversal method to four traversal methods. The traditional Zigzag transform has its natural defects. On the one hand, the initial scan position is only starting from the four corners, only four one-dimensional vectors can be generated. On the other hand, the continuous scanning of the Z word still has a great correlation between the elements [28]–[36]. Aiming at the problems of Zigzag transformation commonly used in image scrambling, such as simple transformation, few transformation methods, and high pixel correlation after transformation, this paper proposes a Zigzag transformation that starts at random positions and crosses bidirectionally. The above problems are solved through experiments and analysis.

II. INTRODUCTION TO RELATED THEORIES

A. ZIGZAG TRANSFORMATION WITH TWO-WAY CROSSING AT RANDOM POSITION

Zigzag transform is an algorithm that rearranges a two-dimensional matrix to weaken the correlation between its matrix elements, so it is often used to scramble the image in image encryption. Aiming at the shortcomings of traditional Zigzag, this chapter proposes a Zigzag transform that starts bidirectional crossover at random positions. The Zigzag transform is expanded from four to $m \times n$. $m \times n$ represents the size of the matrix. The algorithm is described as follows:

Let P be the $n \times n$ size matrix to be transformed.

Step 1 (Generate Initial Coordinates): Generate two random numbers $1 \leq i, j \leq n$, where (i, j) is the starting coordinate position of the transformation.

Step 2 (Scan): Starting from position (i, j), perform Z-scanning to the upper right corner and the lower left corner respectively to generate two vectors $\vec{v}_1$ and $\vec{v}_2$.

Step 3 (Cross Merge): Cross merge the vectors $\vec{v}_1$ and $\vec{v}_2$ to generate a vector $\vec{v}$.

Step 4 (Arrangement): The vector $\vec{v}$ is rearranged into a matrix of size $n \times n$ according to the rule of column first, and the end is complete.

The drawing compares the two Zigzag transforms, and the results are shown in Fig. 1 and Fig. 2.

Two Zigzag transforms are used to compare the results of one round, two rounds, and three rounds of scrambling on the Boat graph. The results are shown in Fig. 3.

Next, calculate the correlation coefficients of the adjacent pixels of the image in Fig 3, and use Eq. (11) to calculate the three of the Boat plaintext image, the Zigzag one, two, and three rounds of the ciphertext image, and the new Zigzag one, two, and three rounds of the ciphertext image. Correlation coefficients of adjacent pixels in two directions, the results are shown in Table 1.

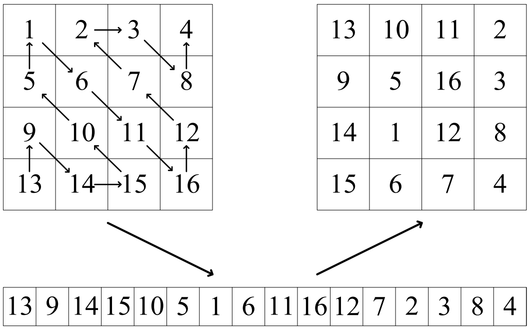


FIGURE 1. **Zigzag transformation process.**

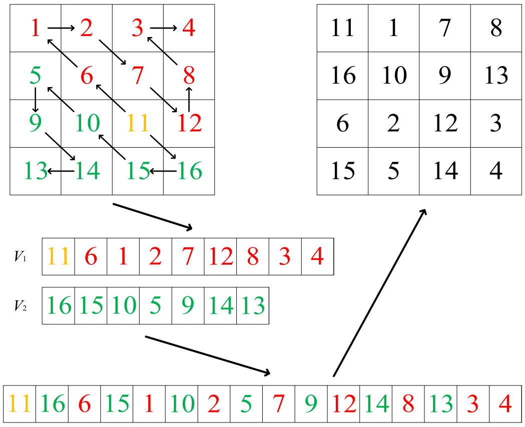


FIGURE 2. **Random position starts with a two-way crossover Zigzag transformation process.**

TABLE 1. **Correlation coefficient of adjacent pixels.**

Test images	Adjacent pixel correlation coefficient		
	H	V	D
Boat plaintext image	0.9383	0.9713	0.9223
One round transformation of Zigzag	−0.0407	0.9223	−0.0397
One round of transformation of the new Zigzag	−0.0972	−0.1364	−0.0291
Two rounds transformation of Zigzag	−0.0137	−0.0397	0.0051
Two rounds of transformation of the new Zigzag	−0.0082	0.0117	−0.0146
Three rounds transformation of Zigzag	0.0034	0.0052	−0.0008
Three rounds of transformation of the new Zigzag	−0.0019	0.0005	0.0005

It can be seen from Table 1 that the Zigzag transform proposed in this paper starts bidirectionally at random positions and the adjacent pixel correlation coefficient is lower than that of the Zigzag transform, indicating that the Zigzag transform proposed in this paper can effectively reduce the correlation of image pixels.

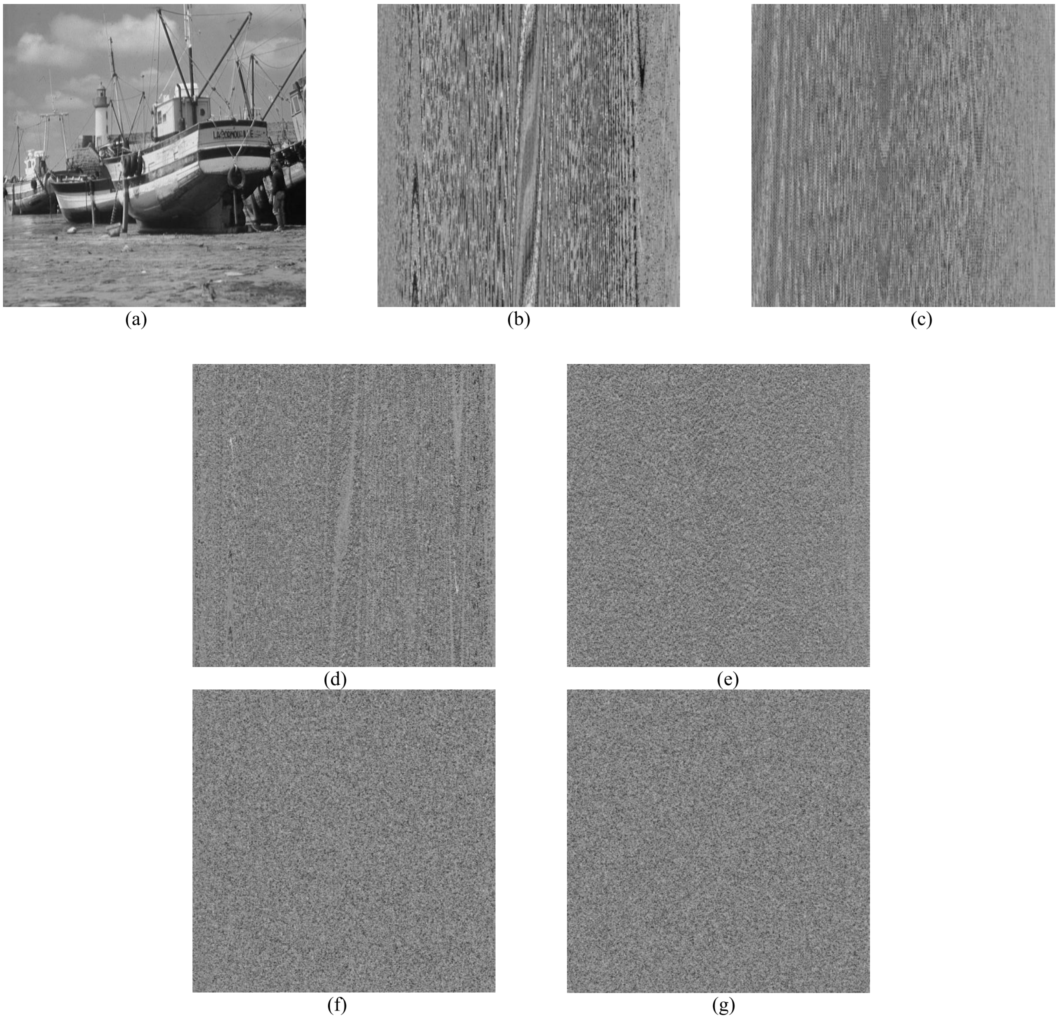


FIGURE 3. The two Zigzag transformations perform a round scramble comparison of the Boat diagrams (a) Boat plaintext image (b) One round transformation of Zigzag (c) One round of transformation of the new Zigzag (d) Two rounds transformation of Zigzag (e) Two rounds of transformation of the new Zigzag (f) Three rounds transformation of Zigzag (g) Three rounds of transformation of the new Zigzag.

The following is a summary of the advantages and disadvantages of the Zigzag transform that starts at random positions and crosses bidirectionally.

Advantage 1: Ordinary ZigZag transformation has four transformation results. The transformation result of Zigzag transformation, which starts to cross bidirectionally at a random position, is as many as the number of image pixels.

Advantage 2: It can be seen from Fig. 3 and Table 1 that the scrambling effect of the Zigzag transform that starts from a random position and crosses bidirectionally is significantly better than that of the ordinary ZigZag transform. The disadvantage is that the Zigzag transform that crosses bidirectionally at a random position needs to input the coordinates of the starting point, while the ordinary ZigZag transform does not.

B. ONE-DIMENSIONAL LOGISTIC CHAOTIC SYSTEM

One-dimensional Logistic chaotic system [37] is a system that leads from period-doubling bifurcation to chaos. Because of its simple expression, good performance, low time complexity, and the generated chaotic sequence fully meets the characteristics of non-periodic, initial value sensitive, and long-term unpredictability, it is often used for image encryption. Its mathematical expression is expressed as follows:

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

Among them, the parameter $n(n = 0, 1, 2, 3 \ldots\ldots)$ is the number of iterative steps, $x_n \in (0, 1)$ is the system state when the number of iterative steps is n, and $\mu \in (0, 4]$ is the chaotic parameter. When $\mu \in (3.5699456, 4]$, the system is in a chaotic state, in order to have a better chaotic performance of the system, $\mu \in (3.9, 4]$ is selected in this chapter.

C. HYPERCHAOTIC CHEN SYSTEM

Chen system [38] is a three-dimensional chaotic system similar to Lorenz system discovered by Professor Guanrong Chen. Although Chen system is similar to Lorenz system, the two are not equivalent, and the former has more complex dynamic characteristics than the latter. Chen system The kinetic equation of is expressed as follows.

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz, \end{cases} \tag{2}$$

The system is in a state of chaos when the parameters $a = 35$, $b = 3$, and $c = 28$.

The hyperchaotic Chen system [39] is a four-dimensional hyperchaotic system extended by Li on the Chen system. Compared with the Chen system, the hyperchaotic Chen system has more feedback control parameters and more complex chaotic behavior. The dynamic equation of the hyperchaotic Chen system is expressed as follows.

$$\begin{cases} \dot{x} = a(y - x) + w \\ \dot{y} = dx + cy - xz \\ \dot{z} = xy - bz \\ \dot{w} = yz + rw, \end{cases} \tag{3}$$

Among them, when the parameters $a = 35, b = 3, c = 12, d = 7, 0 < r \leq 0.085$, the system is in a chaotic state, when the parameters $a = 35$, $b = 3$, $c = 12$, $d = 7$, $0.085 < r \leq 0.798$, the system is in a hyper-chaotic state, this chapter will take $0.085 < r \leq 0.798$ in order to obtain better chaotic characteristics.

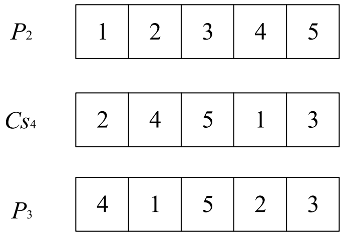
III. ALGORITHM DESCRIPTION

A. KEY GENERATION AND ACQUISITION OF CHAOTIC SEQUENCES

Let the size of the plaintext image P be $M \times N$. First, the plaintext image is used as the input of the Hash-256 algorithm, and then a 256-bit key stream is generated, denoted as Key, and then the key stream Key is divided into a group of 32 bits and divided into 8 groups. The key stream is denoted as $Key = \{k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8\}$, and the key stream is mapped to the initial value of the system through calculations. The mapping rules are as follows.

$$\begin{cases} Zi = \lfloor \mathrm{mod}(k_1, 512) + 1 \rfloor \\ Zj = \lfloor \mathrm{mod}(k_2, 512) + 1 \rfloor \\ \mu = 0.1 \times (k_3/2^{32}) + 3.9 \\ x_0 = k_4/2^{32} \\ Cr = (0.798 - 0.085) \times (k_5/2^{32}) + 0.085 \\ Cx_0 = (k_6/2^{32}) \times 20 \\ Cy_0 = (k_7/2^{32}) \times 20 \\ Cz_0 = (k_8/2^{32}) \times 20 \\ Cw_0 = ((k_1 \oplus k_8)/2^{32}) \times 20, \end{cases} \tag{4}$$

where, Zi, Zj are the starting position of the two-way Zigzag transformation, μ, x_0 are the initial value of the one-dimensional Logistic mapping, and $Cx_0, Cy_0, Cz_0, Cw_0, Cr$ are the initial value of the Chen chaotic system. The initial value μ, x_0 is brought into the one-dimensional Logistic mapping to obtain a chaotic sequence of length $M \times N$. Denote it as s_1. Bring the initial value $Cx_0, Cy_0, Cz_0, Cw_0, Cr$ into the Chen chaotic system to obtain four chaotic sequences of length Cs_1, Cs_2, Cs_3, Cs_4, denoted as Cs_1, Cs_2, Cs_3, Cs_4, and then map the five chaotic sequences. In this chapter, s_1 is mapped to the ordered sequence after sorting s_1. The subscript sequence in the original sequence, Cs_4 is mapped to the subscript sequence of the ordered sequence elements in the original sequence after Cs_4 is sorted, and Cs_1, Cs_2, Cs_3, Cs_4 s is mapped to the random number [0, 255], the mapping formula is as follows.



P_2	1	2	3	4	5
Cs_4	2	4	5	1	3
P_3	4	1	5	2	3

FIGURE 4. Sort for example.

$$\begin{cases} [\sim, s_1] = \mathrm{sort}(s_1) \\ Cs_1 = \mathrm{mod}(\left\lfloor Cs_1 \times 10^{10} \right\rfloor, 256) \\ Cs_2 = \mathrm{mod}(\left\lfloor Cs_2 \times 10^{10} \right\rfloor, 256) \\ Cs_3 = \mathrm{mod}(\left\lfloor Cs_3 \times 10^{10} \right\rfloor, 256) \\ [\sim, Cs_4] = \mathrm{sort}(Cs_4), \end{cases} \tag{5}$$

The sort function is a built-in function of the simulation software, which is used to sort vector elements and return two vectors, a collection of ascending vectors and index vectors.

B. SCRAMBLE

The scrambling is divided into two steps. The first step is to perform three rounds of Zigzag transformation at random positions to start bidirectional crossover, and the second step is to perform Sort.

First, take the initial value coordinate (Zi, Zj) as the starting point to perform three rounds of Zigzag transformation at random positions to start bidirectional crossing of the image P to obtain P_1.

Then, use the s_1 sequence to sort P_1 to get the intermediate result P_2, the formula is as follows.

$$P_2 = \mathrm{Sort}(P_1, s_1), \tag{6}$$

Finally, use the Cs_4 sequence to sort P_2 to get the intermediate result P_3, the formula is as follows.

$$P_3 = \mathrm{Sort}(P_2, Cs_4), \tag{7}$$

The scrambling is over.

Sort sorting is different from the sort function in Section 2.1. It means that the vector to be sorted is sorted by a given index, and an example of Sort sorting is drawn. The result is shown in Fig. 4.

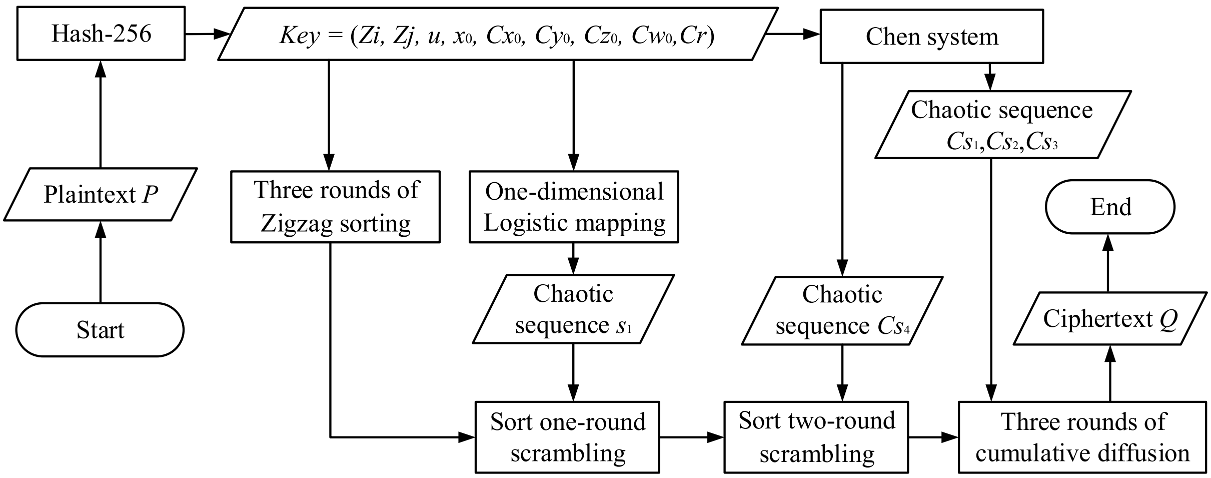

Hash-256
Key = (Zi, Zj, u, x0, Cx0, Cy0, Cz0, Cw0, Cr)
Chen system
Chaotic sequence Cs1,Cs2,Cs3
Plaintext P
Three rounds of Zigzag sorting
One-dimensional Logistic mapping
End
Start
Chaotic sequence s1
Chaotic sequence Cs4
Ciphertext Q
Sort one-round scrambling
Sort two-round scrambling
Three rounds of cumulative diffusion

FIGURE 5. Image encryption algorithm flow chart.

C. DIFFUSION

In order to get a better encryption effect, this algorithm will perform three rounds of diffusion. Each round of diffusion uses accumulation operation. Each element will be accumulated with the previous element. Because the first element has no predecessor element, special processing is done here. Round diffusion uses Cs_1 and P_3 to accumulate to get the intermediate result P_4, the formula is as follows.

$$P_4 = \begin{cases} P_3(i) + \mathrm{C}s_1(i), & i = 1 \\ P_3(i) + Cs_1(i) + P_4(i-1), & i > 1, \end{cases} \tag{8}$$

Then according to Eq. (8), two rounds of diffusion are carried out to get the ciphertext $Q = \mathrm{mod}(P_6, 256)$. The encryption end.

The following draws the flow chart of the chaotic image encryption algorithm based on the Zigzag transform that starts at a random position and crosses bidirectionally. The result is shown in Fig. 5.

The decryption process is opposite to the encryption process. First, the received secret key is used to find the chaotic sequence, and then the inverse process of diffusion and the inverse process of scrambling is performed on the ciphertext, and finally three rounds of inverse random positions are performed to start the biphasic cross-Zigzag transformation. Decryption is complete.

IV. SIMULATION

The following is an encryption and decryption experiment for the images in the chaotic image encryption data set. In this chapter, gray images (Tanks, Plane, Boat, Bridge, Goldhill) and color images (Baboon) are selected for simulation experiment. The results are shown in Fig 6.

V. ANALYSIS AND TESTING OF EXPERIMENTAL RESULTS

A. KEY SPACE AND SENSITIVITY ANALYSIS

Analyzing the key space is to calculate the size of the key. Generally speaking, if the key space is larger than 2^{100}, it is enough to resist brute force attacks; the sensitivity analysis of the key means that when the key is slightly changed, it cannot be decrypted correctly. Plain text, and the decryption result is chaotic. This requirement for image encryption security coincides with the initial sensitivity of the chaotic system [40].

This algorithm uses Hash-256 to generate a 256-bit key stream. Different plaintext images can generate different key streams. It meets the encryption algorithm requirements of "one time one key" and can effectively resist selected ciphertext attacks. The key space size is 2^{256} ($2^{256} > 2^{100}$), it can be seen that this encryption algorithm can completely resist brute force attacks.

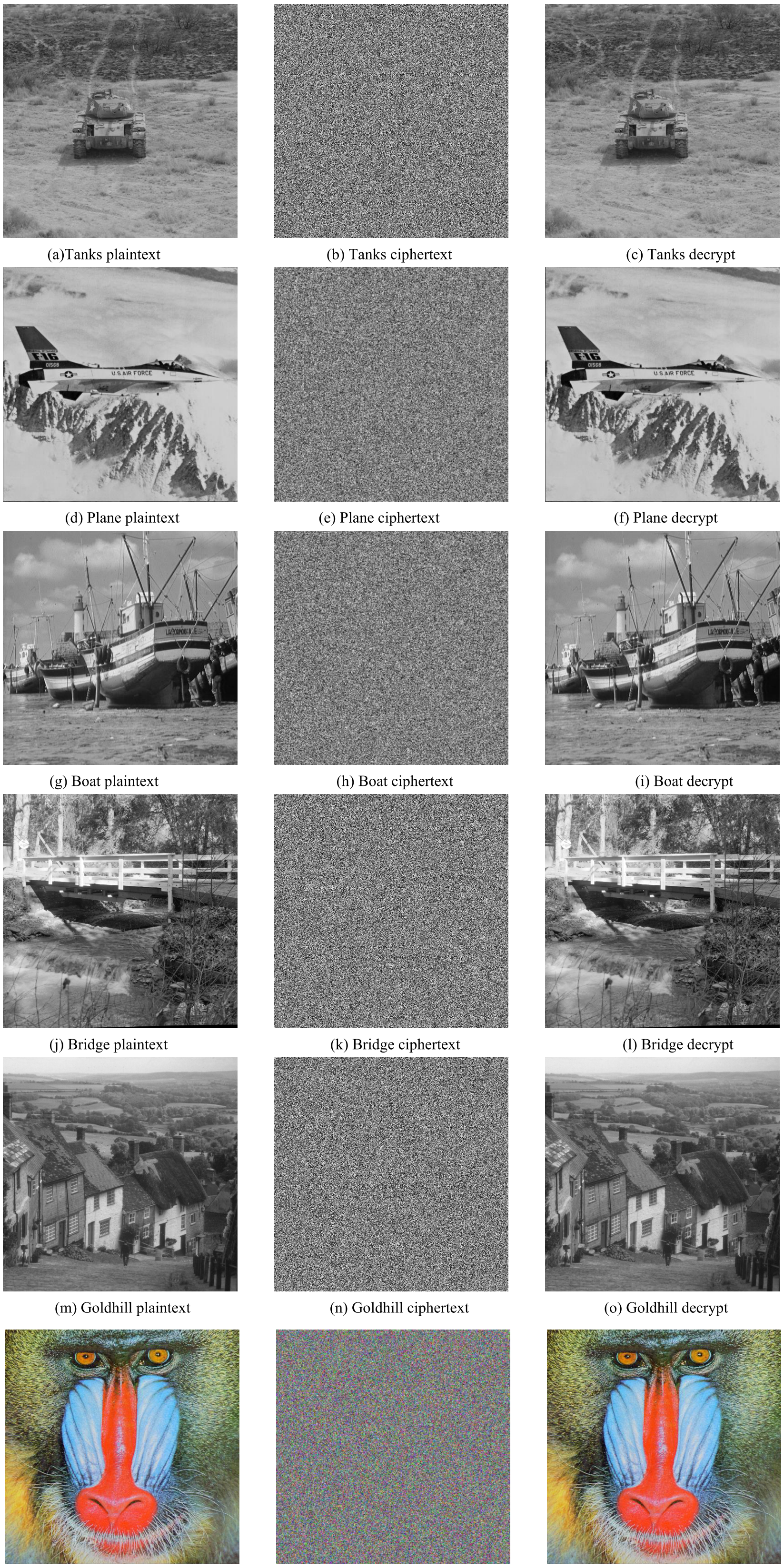
Make subtle changes to the key stream and conduct a sensitivity test. The correct key Key_1 of the Tanks graph algorithm and the wrong key Key_2, Then use the correct secret key Key_1 and the wrong secret key Key_2 after changing the last bit to decrypt, and the result is shown in Fig 7.

Experiments show that this algorithm meets the requirements of secret key sensitivity.

B. TIME COMPLEXITY ANALYSIS

Time complexity is an important indicator to measure the efficiency of an algorithm. It can be seen from the algorithm description in this article that the time complexity of this article mainly depends on the three parts of generating secret keys and obtaining chaotic sequences, scrambling and diffusion. The time complexity of the three parts are $O(4 \times M \times N)$, $O(8 \times M \times N)$ and, $O(3 \times M \times N)$ after removing the coefficients, the total time complexity is expressed as $O(MN)$.

In the simulation experiment, the algorithm running time of the encryption process is calculated, and compared with other publicly published algorithms. The time unit is second. The running environment of this algorithm is i5 8400 processor, 8G memory, Win10 operating system, respectively for different sizes the pictures are tested, and the results are shown in Table 2.



(a)Tanks plaintext (b) Tanks ciphertext (c) Tanks decrypt

(d) Plane plaintext (e) Plane ciphertext (f) Plane decrypt

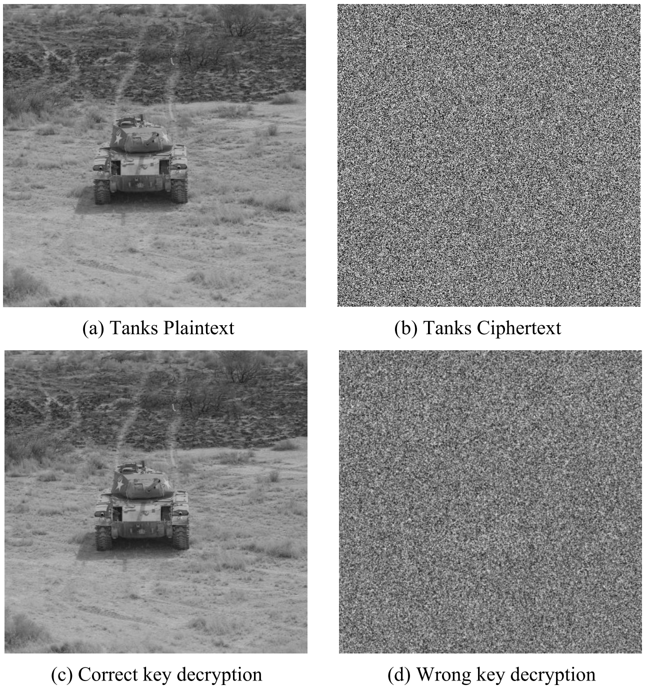
(g) Boat plaintext (h) Boat ciphertext (i) Boat decrypt

(j) Bridge plaintext (k) Bridge ciphertext (l) Bridge decrypt

(m) Goldhill plaintext (n) Goldhill ciphertext (o) Goldhill decrypt

(p) Baboon plaintext (q) Baboon ciphertext (r) Baboon decrypt

FIGURE 6. Simulation experiment of algorithm encryption and decryption.


(a) Tanks Plaintext

(b) Tanks Ciphertext

(c) Correct key decryption

(d) Wrong key decryption

FIGURE 7. Sensitivity analysis of the secret key of tanks graph.

TABLE 2. Comparison of algorithm running time (unit: seconds).

Algorithms	128×128	256×256	512×512	1024×1024
Diacon[41]	0.0579	0.2224	0.9731	3.8377
PXMW[42]	0.0902	0.3440	1.3357	5.3223
CCB[43]	0.2757	0.9810	3.8539	15.4565
HZ[44]	0.1531	0.6347	2.4913	9.9185
XLLH[45]	0.0247	0.1164	0.4924	20.144
ZBC[46]	0.0933	0.3843	1.4824	5.8175
LLZ[47]	0.0323	0.1440	0.5510	2.0864
LSC-IES[48]	0.0244	0.0949	0.4010	1.9857
ZZBCRP	0.0151	0.0492	0.2329	0.8753

C. ANALYSIS OF THE ABILITY TO RESIST DIFFERENTIAL ATTACKS

Differential attack means that the attacker has obtained the plaintext image and the black box encryption algorithm. By making subtle pixel value changes to the plaintext, the two plaintext images are passed through the encryption algorithm to obtain two ciphertext images, and then the ciphertext image is obtained. Analyze to get information about the key, or find the defects of the encryption algorithm. In order to counter the differential attack, when the image encryption algorithm requires slight changes in the plaintext image, the difference between the obtained ciphertext image should be as close to the theoretical value as possible. The general method is to associate the civilized image with the key, and different plaintext The image corresponds to different keys. Even if the plaintext image has a small change, the corresponding key will change greatly; or iterative operation is performed on the pixel value to expand the small change of the plaintext pixel value, and for other pixel values Impact. In order to judge whether the encryption algorithm can resist differential attacks, it is necessary to test the ratio of the number of pixel changes (NPCR) and the average change intensity of pixel values (UACI). The intensity of pixel value change, the theoretical value of NPCR is 99.609375%, and the theoretical value of UACI is 33.4635%. The evaluation formulas of NPCR and UACI are given below:

TABLE 3. NPCR and UACI analysis.

Test images and related literature	NPCR(%)	UACI(%)
Tanks	99.61	33.49
Plane	99.61	33.42
Boat	99.61	33.43
Ref. [34]	99.62	33.59
Ref. [50]	99.63	33.45
Ref. [51]	99.62	33.46

$$\mathrm{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%, \tag{9}$$

$$\mathrm{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| \frac{p_1(i,j) - p_2(i,j)}{255} \right| \times 100\%, \tag{10}$$

Among them, $M \times N$ represents the size of the image, $D(i,j)$ represents whether the pixel value at the coordinate (i,j) position has changed, $D(i,j) = 1$ represents a change, $D(i,j) = 0$ represents no change, $p_1(i,j)$ represents the pixel value of the ciphertext after the original plaintext is encrypted, $p_2(i,j)$ represents the ciphertext after changing the plaintext encryption The pixel value of [49].

In order to prove whether this algorithm can resist differential attacks, the absolute value of the first pixel of the plaintext image is changed to 1, and the values of NPCR and UACI are calculated according to Eq. (9) and Eq. (10), and then combined with other algorithms Comparison, the results are shown in Table 3.

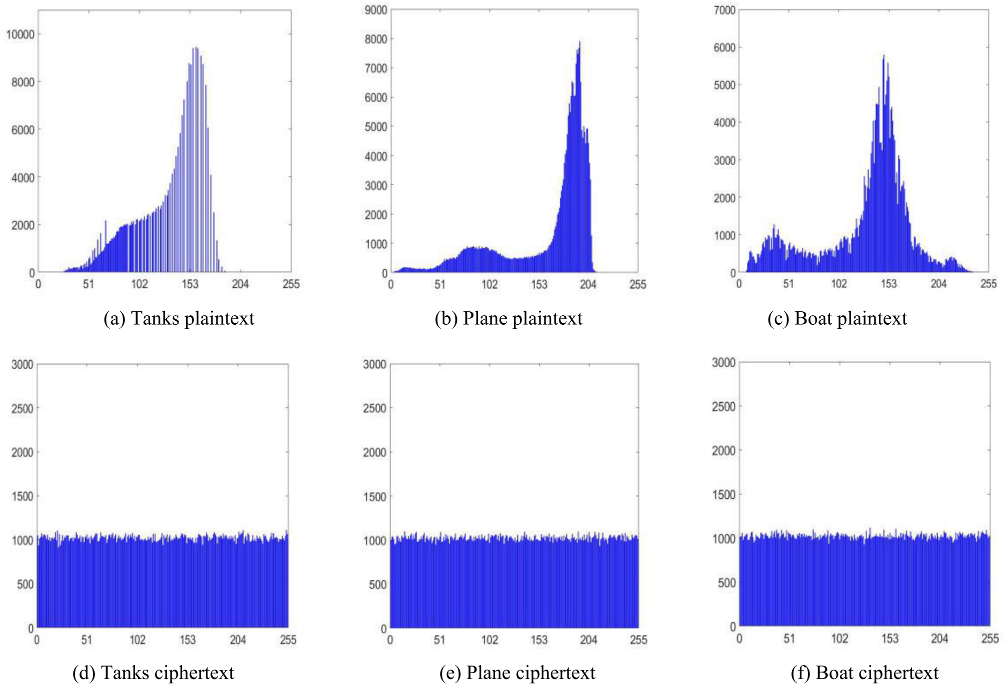
Experimental data shows that this algorithm has the ability to resist differential attacks.

D. HISTOGRAM ANALYSIS

There are 256 types of pixel values in a grayscale image. In a plaintext image, because the image expresses a certain meaning, the number of pixel values is often uneven, which makes it easy for an attacker to obtain plaintext information by analyzing the number of pixel values. The purpose of the encryption algorithm is to distribute the number of pixel values as evenly as possible, and the purpose of hiding the information of the pixel value has been achieved. Generally, the pixel value is diffused to achieve an even distribution of the number of pixel values.

Select Tanks chart, Plane chart, Boat chart to analyze the histogram. First, draw the histogram of the plaintext image and compare it with the histogram of the ciphertext image. The result is shown in Fig 8.

It can be seen from Figure 8 that the pixel histogram of the plaintext image, the number of pixel values is unevenly



(a) Tanks plaintext (b) Plane plaintext (c) Boat plaintext

(d) Tanks ciphertext (e) Plane ciphertext (f) Boat ciphertext

FIGURE 8. Compare plain histograms with cipher histograms.

distributed, and there is obvious image information. The ciphertext image obtained by the encryption algorithm has a uniform number of pixel values, which hides the image information well. Which can effectively resist the attack method of statistical analysis.

E. ADJACENT PIXEL CORRELATION

An image is a way to represent information, which determines that the pixels of an image must be related to each other and cannot be messy, so that the image can express a certain meaning. The encryption algorithm is to break this correlation, so as to achieve the purpose of hiding image information. In this article, qualitative and quantitative methods are used to measure the correlation of adjacent pixels. One is to use the values of two adjacent pixels as coordinates in the plane space to trace the points and visually observe the correlation of adjacent pixels. One method is to find the average correlation coefficient of adjacent pixels through a mathematical formula, and carry out quantitative analysis and comparison. The mathematical formula for solving the correlation coefficient is expressed as follows.

$$\begin{aligned} r_{xy} &= \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \\ cov(x,y) &= E\left[(x-E(x))(y-E(y))\right], \\ D(x) &= \frac{1}{n}\sum_{i=1}^{n}(x_i-E(x))^2, \\ E(x) &= \frac{1}{n}\sum_{i=1}^{n}x_i, \end{aligned} \tag{11}$$

TABLE 4. Correlation coefficient of adjacent pixels.

Test images	Plaintext			Ciphertext		
	H	V	D	H	V	D
Tanks	0.9657	0.9308	0.9172	−0.0015	−0.0014	−0.0014
Plane	0.9714	0.9641	0.9425	0.0024	−0.0027	−0.0027
Boat	0.9383	0.9713	0.9223	0.0002	−0.0026	−0.0012
Ref. [31]	− −	− −	− −	0.0142	0.0197	−0.0136
Ref. [34]	− −	− −	− −	−0.0237	−0.0178	−0.0284
Ref. [35]	− −	− −	− −	0.1487	0.1364	0.0338

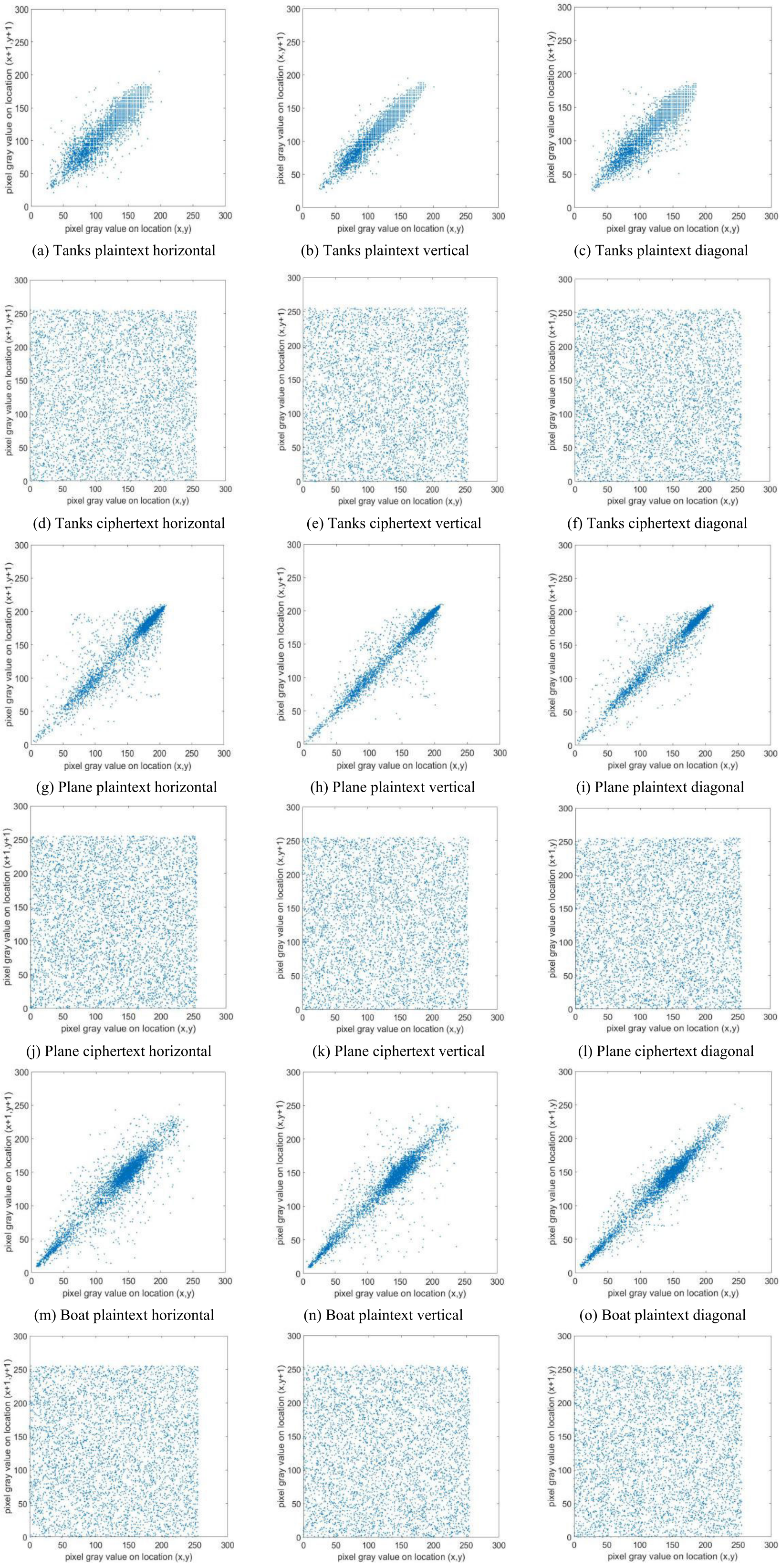
As the correlation coefficient r of adjacent pixels decreases, the correlation of pixels also decreases, and the encryption effect of the algorithm is better [52].

Select Tanks map, Plane map, Boat map to analyze the correlation of adjacent pixels, and draw the correlation scatter plots of adjacent pixels in the three directions of the plaintext image and the ciphertext image. The results are shown in Fig 9.

It can be seen from the above experimental results that the pixel values of the encrypted image are evenly distributed.

Next, calculate the correlation coefficients of adjacent pixels in the Tanks map, Plane map, and Boat map. Use Eq. (11) to calculate the correlation coefficients of adjacent pixels in the three directions of the plaintext image and the ciphertext image. The results are shown in Table 4.

It can be seen from the table that, compared with the adjacent pixel correlation coefficient of the plaintext image, the adjacent pixel correlation coefficient of the ciphertext image is significantly reduced, making it difficult for the attacker to obtain value from the analysis of the relationship between the pixels of the ciphertext image. The information



(a) Tanks plaintext horizontal (b) Tanks plaintext vertical (c) Tanks plaintext diagonal

(d) Tanks ciphertext horizontal (e) Tanks ciphertext vertical (f) Tanks ciphertext diagonal

(g) Plane plaintext horizontal (h) Plane plaintext vertical (i) Plane plaintext diagonal

(j) Plane ciphertext horizontal (k) Plane ciphertext vertical (l) Plane ciphertext diagonal

(m) Boat plaintext horizontal (n) Boat plaintext vertical (o) Boat plaintext diagonal

(p) Boat ciphertext horizontal (q) Boat ciphertext vertical (r) Boat ciphertext diagonal

FIGURE 9. Plain image and cipher image adjacent pixel correlation.

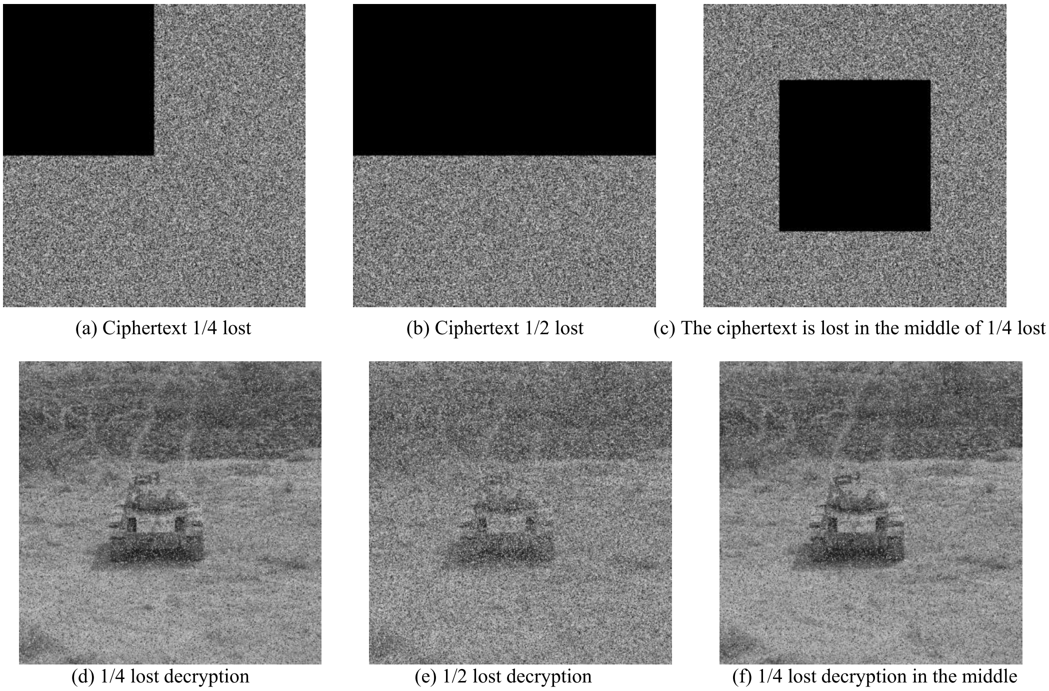

(a) Ciphertext 1/4 lost
(b) Ciphertext 1/2 lost
(c) The ciphertext is lost in the middle of 1/4 lost
(d) 1/4 lost decryption
(e) 1/2 lost decryption
(f) 1/4 lost decryption in the middle

FIGURE 10. Cropping attacks.

can effectively resist ciphertext-only attacks, and the effect is better when compared with data from other documents.

F. χ^2 TEST

The χ^2 test can be said to be a quantification of the histogram, which is used to indicate whether the histogram is evenly distributed. The average number of different pixel values in an image is different from the number of each pixel value. Its mathematical expression is as follows.

$$\chi^2 = \sum_{i=0}^{255} \frac{(v_i - v)^2}{v},$$
$$v = \frac{1}{256} \times \sum_{i=0}^{255} v_i, \tag{12}$$

Among them, v_i represents the number of pixels with a pixel value of i, v represents the average number of pixels for each pixel value, the smaller the value of χ^2, the more even the distribution of the number of pixels of each pixel value, the better the encryption effect of the algorithm, and the more secure the algorithm [53].

Quantify the histogram, analyze whether the pixel value distribution is uniform, use Eq. (12) to calculate the χ^2 value of the plaintext image and the ciphertext image of the Tanks map, the Plane map, and the Boat map, and compare it with other documents. The results are shown in Table 5.

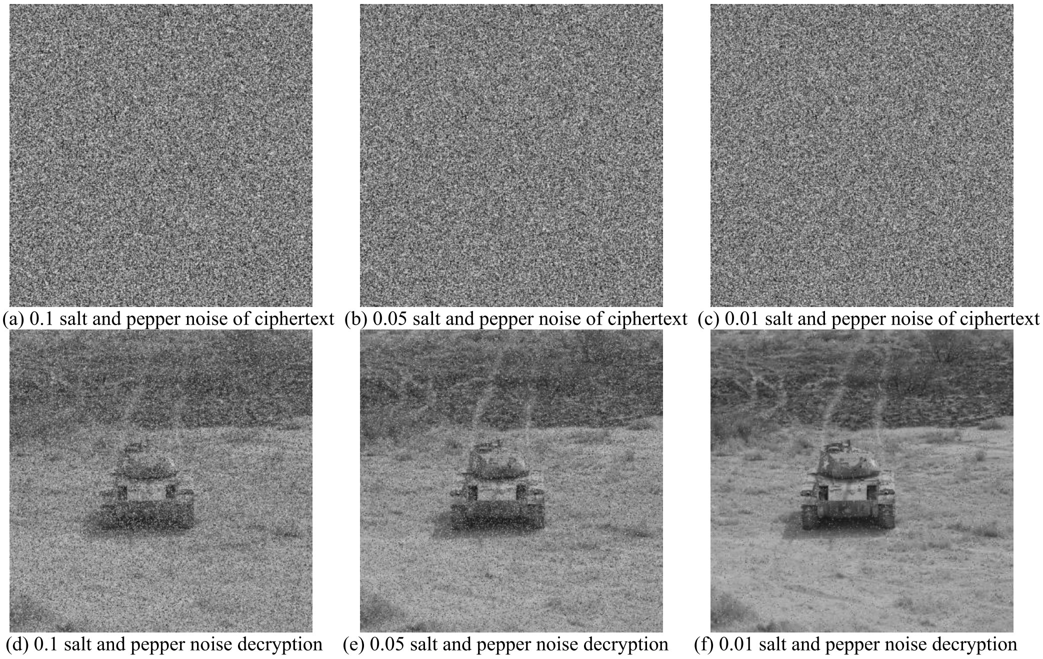
It can be seen from the table that the χ^2 value of the ciphertext is significantly reduced compared with the χ^2 value of the plaintext. The average χ^2 value of the three ciphertext images is better than the theoretical value, and the effect is better compared with the data of other documents.

TABLE 5. χ^2 test.

Test images	Plaintext	Pass or No pass	Ciphertext	Pass or No pass
Tanks	957950	No pass	285.9805	Pass
Plane	715670	No pass	246.1309	Pass
Boat	383970	No pass	239.9453	Pass
Ref. [54]	100670	No pass	242.0234	Pass
Ref. [51]	39651	No pass	260.4141	Pass
Ref. [55]	75187	No pass	272.2969	Pass

G. INFORMATION ENTROPY AND LOCAL INFORMATION ENTROPY

In information theory, information entropy is defined as the average amount of information in a message. The more random the source, the greater the average amount of information expressed. Therefore, information entropy can be used to characterize the degree of randomness of information. In image encryption, it can be used Information entropy quantitatively calculates the degree of randomness of the pixel value distribution. The more random the pixel value distribution, the greater the information entropy. Like the χ^2 test, it is also a supplement to the quantitative analysis of histogram analysis. The maximum value of information entropy in a grayscale image It is 8. In actual measurement, the closer the information entropy is to 8, the better the encryption effect of the algorithm. When the information entropy is equal to 8, the histogram is uniformly distributed, and the χ^2 value is equal to 0. The formula of gray image


(a) 0.1 salt and pepper noise of ciphertext (b) 0.05 salt and pepper noise of ciphertext (c) 0.01 salt and pepper noise of ciphertext

(d) 0.1 salt and pepper noise decryption (e) 0.05 salt and pepper noise decryption (f) 0.01 salt and pepper noise decryption

FIGURE 11. Salt and pepper noise.

TABLE 6. Information entropy.

Test images	Plaintext	Ciphertext
Tanks	6.1898	7.9992
Plane	6.7059	7.9993
Boat	7.1914	7.9993
Ref. [34]	7.6320	7.9990
Ref. [57]	7.4436	7.9960
Ref. [54]	7.1587	7.9973

TABLE 7. Local information entropy.

Test images and comparative	Plaintext	Ciphertext
Tanks	6.1346	7.9027
Plane	6.6259	7.9029
Boat	7.0946	7.9021
Ref. [51]	3.4024	7.9061

information entropy can be expressed as:

$$H(s) = \sum_{i=0}^{255} p(s_i) \log_2 \frac{1}{p(s_i)}, \tag{13}$$

Among them, the parameter s_i represents the number of pixels with a value of i, and $p(s_i)$ represents the proportion of pixels with a pixel value of i in the image.

The information entropy of the entire image does not fully reflect the random distribution of local pixel values in an image. Therefore, Wu *et al.* [56] proposed local information entropy. The formula for local information entropy can be expressed as.

$$\overline{H_{k,T_B}}(S) = \sum_{i=1}^{k} \frac{H(S_i)}{k}, \tag{14}$$

TABLE 8. NPCR and UACI analysis.

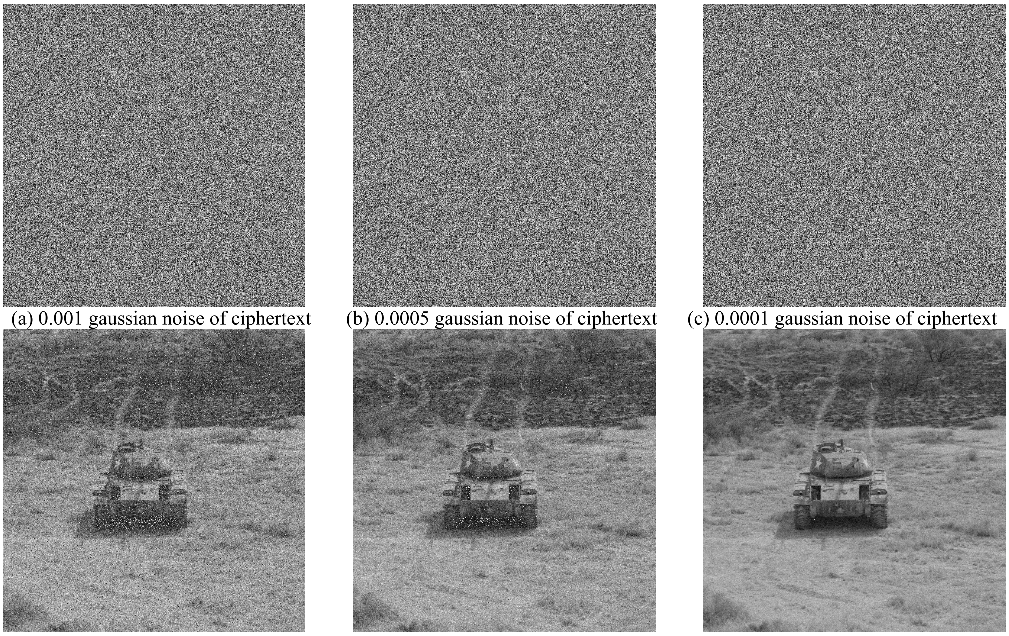
Attack type	Attack intensity	NPCR(%)	UACI(%)
Cropping attacks	1/4	25.20	06.83
	1/2	50.37	13.69
	1/4 middle	25.18	06.87
Salt and pepper noise	0.1	34.26	09.27
	0.05	18.53	05.06
	0.01	03.92	01.07
Gaussian noise	0.001	98.89	11.47
	0.0005	98.39	07.95
	0.0001	96.49	03.59

In Eq. (14), S_i represents the i-th selected pixel group of the image, T_B represents the number of pixels in S_i, k represents the number of selected pixel groups, and $H(S_i)$ represents the information entropy of S_i.

Calculate the information entropy, check whether the pixel value histogram is evenly distributed, use Eq. (13) to calculate and analyze the information entropy of the plaintext image and the ciphertext image of the Tanks, Plane, and Boat diagrams. The results are shown in Table 6.

According to the definition of local information entropy, when, and, the local information entropy is between, it means that the local information entropy meets the target requirement. Use Eq. (14) to compare the plaintext image and ciphertext of Tanks, Plane, and Boat. The local information entropy of the image is calculated and analyzed, and the results are shown in Table 7.

From the data in Table 6 and Table 7, it can be seen that the information entropy in Table 6 is close to the theoretical value of 8, and the local information entropy in Table 7 is in the theoretical interval, indicating that the encryption algorithm meets the security requirements of randomness.


(a) 0.001 gaussian noise of ciphertext (b) 0.0005 gaussian noise of ciphertext (c) 0.0001 gaussian noise of ciphertext

(d) 0.001 gaussian noise decryption (e) 0.0005 gaussian noise decryption (f) 0.0001 gaussian noise decryption

FIGURE 12. Gaussian noise.

TABLE 9. NIST random numbers test.

Test	Plaintext P-value	Ciphertext P-value
The Frequency (Monobit) Test	0	0.186566
Frequency Test within a Block	0	0.162606
The Runs Test	0	0.911413
Tests for the Longest-Run-of-Ones in a Block	0	0.311542
The Binary Matrix Rank Test	0	0.122325
The Discrete Fourier Transform (Spectral) Test	0	0.911413
The Non-overlapping Template Matching Test	0	0.991468
The Overlapping Template Matching Test	0	0.689019
Maurer's "Universal Statistical" Test	0	0.311542
The Linear Complexity Test	0.299251	0.350485
The Serial Test	0	0.637119
The Approximate Entropy Test	0	0.834308
1The Cumulative Sums (Cusums) Test	0	0.991468
The Random Excursions Test	0	0.213309
The Random Excursions Variant Test	0	0.213309

H. ROBUSTNESS ANALYSIS

Robustness is also called robustness. In cryptography, the ciphertext may be damaged due to environmental interference or man-made destruction. A robust cryptographic system should resist this attack to a certain extent. Clipping and noise are generally used in image encryption. To test the system, the system should still be able to decrypt the approximate plaintext under a certain cutting and noise attack intensity, saying that the cryptographic system is robust.

In order to perform robustness tests, the Tanks map is tested using cropping attack, salt and pepper noise, and Gaussian noise. The cropping attack uses quarter cropping, half cropping, and quarter intermediate cropping. The coefficients of salt and pepper noise are selected as 0.1, 0.05, 0.01 for testing, Gaussian noise coefficients were selected as 0.001, 0.0005, 0.0001 for testing, the results are shown in Fig. 10, Fig. 11, and Fig. 12.

For the above three different types of attacks, calculate the NPCR and UACI of the plaintext image and the decrypted image after the attack, analyze the pixel change ratio and the change intensity of the pixel value of the decrypted image after attacking the ciphertext image, and then illustrate the robustness of the algorithm The strength of sex, the values of NPCR and UACI are calculated according to Eq. (9) and Eq. (10), and the results are shown in Table 8.

The experimental image results and Table 8 show that under a certain intensity of cropping attacks, salt and pepper noise and Gaussian noise attacks, it is still possible to decrypt clear and identifiable images.

I. NIST

The NIST random number statistical test [58] is a method commonly used in cryptography to detect the randomness of a binary sequence. The test method consists of 15 sub-test methods. Many of the tests in the test use the standard normal distribution and chi-square as the reference distribution. If the tested sequence is actually non-random, the calculated test statistic will fall in the extreme region of the reference distribution. During testing, statistical hypothesis testing is a process of generating conclusions with two possible outcomes, either accept or reject. Calculate a test statistical value P-value for the tested sequence. Compare this test statistic with the critical value α. If the test statistic exceeds the critical value, the null hypothesis of randomness is rejected. Otherwise, accept the null hypothesis of randomness. In practice, statistical hypothesis testing is effective because the reference distribution and critical value depend on and are generated under the randomness of the hypothesis. In this paper, the test critical value α is set to 0.01, and the Tanks chart is tested. The test results are shown in Table 9.

VI. CONCLUSION

The Zigzag transform that starts at random positions and crosses bidirectionally is proposed in this paper to scramble the image. It can be seen from the experimental data that compared with other Zigzag transforms, the Zigzag transform scrambling that starts at random positions and crosses bidirectionally is better because it has more transform types. The two-way crossover sorting method is more obvious than the traditional Zigzag transform to reduce the intensity of pixel correlation. After multiple rounds of Zigzag transformation with two-way cross at random positions, the pixel matrix is sorted by the sorting array. In the diffusion stage, multiple rounds of coupling diffusion are used to achieve the purpose of changing the pixel value. Finally, through the analysis of algorithm security, it can be concluded that the chaotic image encryption algorithm of Zigzag transform that starts to cross bidirectionally at random position has good security and time efficiency, and it fully meets the requirements of image encryption. The image encryption algorithm proposed in this paper can only be applied to the encryption of bitmap images. The focus of future work is to expand the scope of application of the algorithm in this paper, so that it can be applied to the encryption of bitmap images, as well as the encryption of other information carriers such as sound and text.

REFERENCES

[1] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.
[2] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.
[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[4] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.
[5] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.
[6] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.
[7] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 38, pp. 5973–5978, Sep. 2008.
[8] S. M. Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal Process.*, vol. 92, no. 5, pp. 1202–1215, May 2012.
[9] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. M. Lopez-Gutiérrez, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Process.*, vol. 109, pp. 119–131, Apr. 2015.
[10] O. Mirzaei, M. Yaghoobi, and H. Irani, "A new image encryption method: Parallel sub-image encryption with hyper chaos," *Nonlinear Dyn.*, vol. 67, no. 1, pp. 557–566, 2012.
[11] Z. Liu, S. Li, W. Liu, W. Liu, and S. Liu, "Image hiding scheme by use of rotating squared sub-image in the gyrator transform domains," *Opt. Laser Technol.*, vol. 45, pp. 198–203, Feb. 2013.
[12] A. A. Badawi, L. Hoang, C. F. Mun, K. Laine, and K. M. M. Aung, "PrivFT: Private and fast text classification with homomorphic encryption," *IEEE Access*, vol. 8, pp. 226544–226556, 2020.
[13] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy," *Signal Process.*, vol. 176, Nov. 2020, Art. no. 107684.
[14] X. Chai, H. Wu, Z. Gan, Y. Zhang, and Y. Chen, "Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107525.
[15] Z. Gan, X. Chai, J. Zhang, Y. Zhang, and Y. Chen, "An effective image compression–encryption scheme based on compressive sensing (CS) and game of life (GOL)," *Neural Comput. Appl.*, vol. 32, no. 17, pp. 14113–14141, Sep. 2020.
[16] X. Chai, X. Zheng, Z. Gan, and Y. Chen, "Exploiting plaintext-related mechanism for secure color image encryption," *Neural Comput. Appl.*, vol. 32, no. 12, pp. 8065–8088, Jun. 2020.
[17] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Opt. Lasers Eng.*, vol. 121, pp. 203–214, Oct. 2019.
[18] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, "An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing," *Inf. Sci.*, vol. 556, pp. 305–340, May 2021.
[19] X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, "Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption," *Signal Process.*, vol. 183, Jun. 2021, Art. no. 108041.
[20] Y. Peng, K. Sun, and S. He, "A discrete memristor model and its application in Hénon map," *Chaos, Solitons Fractals*, vol. 137, Aug. 2020, Art. no. 109873.
[21] Y. Peng, S. He, and K. Sun, "A higher dimensional chaotic map with discrete memristor," *AEU Int. J. Electron. Commun.*, vol. 129, Feb. 2021, Art. no. 153539.
[22] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Process.*, vol. 168, Mar. 2020, Art. no. 107340.
[23] J. Wenli, Z. Minrui, and J. Yuping, "Research on digital image scrambling algorithm based on Zigzag transform," *Comput. Appl. Softw.*, vol. 26, no. 3, pp. 71–73, 2009.
[24] L. Zhentai, X. Xuegang, and C. Wufan, "Digital image encryption based on Zigzag coding," *Comput. Eng. Des.*, vol. 30, no. 9, pp. 2145–2146, 2009.
[25] M. Padmaa and D. Y. Venkataramani, "ZIG-ZAG PVD—A nontraditional approach," *Int. J. Comput. Appl.*, vol. 5, no. 6, pp. 5–10, Aug. 2010.
[26] X. Xu and J. Feng, "Research and implementation of image encryption algorithm based on Zigzag transformation and inner product polarization vector," in *Proc. IEEE Int. Conf. Granular Comput.*, Aug. 2010, pp. 556–561.
[27] Y. Yuqin, J. Tianfa, and L. Gen, "Digital image scrambling method based on extended Zig-Zag transform," *Inf. Netw. Secur.*, vol. 11, no. 10, pp. 57–58, 2011.
[28] D. Husheng, L. Ping, and M. Xiaohu, "Image encryption algorithm based on CNN hyperchaotic system and extended Zigzag," *Comput. Appl. Softw.*, vol. 30, no. 5, pp. 132–136, 2013.
[29] L. Gen, J. Tianfa, and J. Wei, "A color image scrambling algorithm based on Zigzag transform," *Comput. Eng. Sci.*, vol. 35, no. 5, pp. 106–111, 2013.
[30] S. Mallik, "Image hiding using Zigzag and spiral traversal algorithms," *Amer. J. Adv. Comput.*, vol. 1, no. 1, pp. 15–18, Jul. 2014.

[31] Y. Li, X. Li, X. Jin, G. Zhao, S. Ge, Y. Tian, X. Zhang, K. Zhang, and Z. Wang, ''An image encryption algorithm based on Zigzag transformation and 3-dimension chaotic logistic map,'' in *Proc. Int. Conf. Appl. Techn. Inf. Secur.* Berlin, Germany: Springer, 2015, pp. 3–13.

[32] W. Xingyuan, Z. Junjian, and C. Guanghui, ''An image encryption algorithm based on Zigzag transform and LL compound chaotic system,'' *Opt. Laser Technol.*, vol. 119, Nov. 2019, Art. no. 105581.

[33] X. Wang and H. Sun, ''A chaotic image encryption algorithm based on Zigzag-like transform and DNA-like coding,'' *Multimedia Tools Appl.*, vol. 78, no. 24, pp. 34981–34997, Dec. 2019.

[34] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, ''An image encryption scheme based on block scrambling, modified Zigzag transformation and key generation using enhanced logistic—Tent map,'' *Entropy*, vol. 21, no. 7, p. 656, Jul. 2019.

[35] X.-Y. Ji, S. Bai, Y. Guo, and H. Guo, ''A new security solution to JPEG using hyper-chaotic system and modified Zigzag scan coding,'' *Commun. Nonlinear Sci. Numer. Simul.*, vol. 22, no. 1, pp. 321–333, May 2015.

[36] S. Farrag, W. Alexan, and H. H. Hussein, ''Triple-layer image security using a Zigzag embedding pattern,'' in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Apr. 2019, pp. 1–8.

[37] R. M. May, ''Simple mathematical models with very complicated dynamics,'' *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[38] G. Chen and T. Ueta, ''Yet another chaotic attractor,'' *Int. J. Bifurcation Chaos*, vol. 9, no. 7, pp. 1465–1466, 1999.

[39] Y. Li, W. K. S. Tang, and G. Chen, ''Generating hyperchaos via state feedback control,'' *Int. J. Bifurcation Chaos*, vol. 15, no. 10, pp. 3367–3375, 2005.

[40] G. Alvarez and S. Li, ''Some basic cryptographic requirements for chaos-based cryptosystems,'' *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[41] A.-V. Diaconu, ''Circular inter–intra pixels bit-level permutation and chaos-based image encryption,'' *Inf. Sci.*, vols. 355–356, pp. 314–327, Aug. 2016.

[42] P. Ping, F. Xu, Y. Mao, and Z. Wang, ''Designing permutation-substitution image encryption networks with Henon map,'' *Neurocomputing*, vol. 283, pp. 53–63, Mar. 2018.

[43] X. Chai, Y. Chen, and L. Broyde, ''A novel chaos-based image encryption algorithm using dna sequence operations,'' *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[44] Z. Hua and Y. Zhou, ''Design of image cipher using block-based scrambling and image filtering,'' *Inf. Sci.*, vol. 396, pp. 97–113, Aug. 2017.

[45] 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.

[46] Y. Zhou, L. Bao, and C. P. Chen, ''A new 1D chaotic system for image encryption,'' *Signal Process.*, vol. 97, no. 11, pp. 172–182, 2014.

[47] X. Liao, S. Lai, and Q. Zhou, ''A novel image encryption algorithm based on self-adaptive wave transmission,'' *Signal Process.*, vol. 90, no. 9, pp. 2714–2722, Sep. 2010.

[48] Z. Hua, Y. Zhou, and H. Huang, ''Cosine-transform-based chaotic system for image encryption,'' *Inf. Sci.*, vol. 480, no. 1, pp. 403–419, Apr. 2019.

[49] V. Patidar, N. K. Pareek, and K. K. Sud, ''A new substitution–diffusion based image cipher using chaotic standard and logistic maps,'' *Commun. Nonlinear Sci. Numer. Simul.*, vol. 14, no. 7, pp. 3056–3075, Jul. 2009.

[50] H.-S. Ye, N.-R. Zhou, and L.-H. Gong, ''Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion,'' *Signal Process.*, vol. 175, Oct. 2020, Art. no. 107652.

[51] C. Zhu, Z. Gan, Y. Lu, and X. Chai, ''An image encryption algorithm based on 3-D DNA level permutation and substitution scheme,'' *Multimedia Tools Appl.*, vol. 79, pp. 7227–7258, Dec. 2019.

[52] G. Chen, Y. Mao, and C. K. Chui, ''A symmetric image encryption scheme based on 3D chaotic cat maps,'' *Chaos, Solitons Fractals*, vol. 21, pp. 749–761, Jul. 2004.

[53] R. E. Boriga, A. C. Dăscălescu, and A. V. Diaconu, ''A new fast image encryption scheme based on 2D chaotic maps,'' *IAENG Int. J. Comput. Sci.*, vol. 41, no. 4, pp. 249–258, 2014.

[54] F. Yang, J. Mou, C. Ma, and Y. Cao, ''Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application,'' *Opt. Lasers Eng.*, vol. 129, Jun. 2020, Art. no. 106031.

[55] Q. Xu, K. Sun, S. He, and C. Zhu, ''An effective image encryption algorithm based on compressive sensing and 2D-SLIM,'' *Opt. Lasers Eng.*, vol. 134, Nov. 2020, Art. no. 106178.

[56] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, ''Local Shannon entropy measure with statistical tests for image randomness,'' *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.

[57] N.-R. Zhou, L.-X. Huang, L.-H. Gong, and Q.-W. Zeng, ''Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map,'' *Quantum Inf. Process.*, vol. 19, no. 9, pp. 1–21, Sep. 2020.

[58] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. McLean, VA, USA: Booz-Allen and Hamilton, 2001.

HAO GAO received the bachelor's degree from Linyi University, China. He is currently pursuing the master's degree in software engineering with Dalian Maritime University, China. His research interests include image processing and chaos cryptography.

XINGYUAN WANG (Member, IEEE) received the B.S. degree in applied physics and the M.S. degree in optics from Tianjin University, Tianjin, China, in 1987 and 1992, respectively, and the Ph.D. degree in computer software and theory from Northeastern University, Shenyang, China, in 1999. From 1999 to 2001, he was a Postdoctoral Fellow in automation and a Postdoctoral Researcher with Northeastern University. He is currently a Second-Level Professor with the School of Information Science and Technology, Dalian Maritime University, Dalian, China. He has published more than 560 SCI articles, with a total citation 13 000 and an H-index 58 (Web of ScienceTM), and six papers and 23 papers are respectively selected as the hot papers and highly cited papers of the ESI. He has also published three books and over 400 scientific articles in refereed journals and proceedings. He has applied for 26 invention patents, and has authorized 18 invention patents (15 in international and three in China). His research interests include chaos, fractal, and complex network theory and application research. His other research interests include nonlinear dynamics and control, image processing, chaos cryptography, systems biology, and complex networks. He was in the top 2% of scientists 2020 in the world—China (Top 200 for Science Impact 2019), was a highly cited researcher worldwide, for the year 2020 and 2018. He won one First Prize of the Natural Science of Liaoning Province (the only complete person), and one Second Prize of the Natural Science of Ministry of Education (the first complete person).