Chaotic Color Image Encryption Algorithm Based on RNA Operations and Heart Shape Chunking

Mingyue Sun, Wenhua Cui, Ye Tao, and Tianwei Shi

***Abstract*—In modern society, image encryption is critical to protecting digital visual information. A chaotic image encryption scheme based on RNA operations and heart-shaped chunking is proposed for a color image. There are five phases to the program. Firstly, a new chaotic system, 2D-NICM, is designed to improve the infinite folding chaotic mapping of two-dimensional. Secondly, the segmented linear chaotic map (PWLCM) is associated with plains to generate chaotic sequences. This step leads to an improvement in the sensitivity of plain. Thirdly, the color images are layered. Then the downward and leftward circular shift diffusion operations are performed using the RNA algorithm. The selection of operators is based on the class of amino acids. Chaotic sequences ultimately control the coding rules of RNA computation. This step makes the result of the operation more unpredictable. Fourthly, this section chunks the initial cipher image after RNA operation. Finally, the chunked initial cipher images are encrypted in heart shape. The final password image is obtained after all five steps. Simulation results show that the proposed model outperforms the others. Furthermore, based on the high-entropy value, the model has a high anti-jamming ability for common attacks.**

***Index Terms*—color image encryption; RNA algorithm; cyclic shift diffusion; chaotic system**

I. Introduction

THE growing use of instant messaging technology has led to a proliferation of Internet applications for daily use. Therefore, applications such as WeChat, Facebook, Weibo and video conferencing can easily contain sensitive information images in military or medical fields. Therefore, the security of image content has become a problem that scientists and engineers must solve.

Decades of development have resulted in a variety of excellent algorithms. Chaotic mappings were the basis of chaotic cryptography, which has been split into one dimensional and higher dimensional cryptography [1]. More recently, researchers have proposed many schemes for image encryption based on color images [2-4], sequences of RNA [5], S-boxes [6], block encryption [7], and chaotic systems [8-9]. Unidimensional chaotic mappings usually contained few variables, so mappings did not guarantee security. Therefore, many scholars have combined and improved the 1D chaotic mappings. For instance, Zhu et al. [10] proposed a sine wave fusion Logistic chaotic mapping improved by 2D Logistics. Xu et al. [11] proposed an iterative chaos modulation mapping (2D-SLIM) with infinite collapse Logistic mapping based on an improved model of closed loop modulated coupling in two dimensions. Huang et al. [12] isolate the output sequence from two classical one-dimensional chaotic mappings. Logistic, Sine, and Chebyshev mappings were also introduced in this paper. Zhang et al. [13] trained ICS (Integrated Chaotic System) to act on Logistic, Sine, and Tent mapping with switching operations and non-linear combinations. A common drawback of the above chaotic mappings was that the chaotic trajectories were not wide and unevenly distributed with poor ergodicity. Unauthorized users can quickly attack and steal image information [14], so the chaos effect needs further analysis.

In recent years, a growing number of researchers have begun to focus on and study image encryption algorithms based on DNA coding algorithms [15-18]. On the other hand, only some researchers have applied RNA coding algorithms with self-complementary sequence characteristics to image encryption. For example, the color-coded hyperchaotic image encryption scheme based on zigzag T-transform broadcast and RNA coding proposed by Zhang et al. [19] was shown to be weak against differential attacks. Zhu et al. [20] introduced a scheme for image encryption based on chaotic systems and cross mutation of RNA. This scheme performed poorly in foreign entropy attacks. Compared to DNA, RNA has self-complementary sequences that facilitate modular operations [21-22]. The image encryption scheme that combined a chaotic system with a DNA algorithm has had many shortcomings. The main disadvantages were high correlation, small key space and poor anti-attack capability [23]. Given the newness of RNA coding operation, this paper proposes a color-coded chaotic image encryption algorithm based on RNA coding operation and heart shape chunking.

The goals of this paper are to propose: (1) a new chaotic

Manuscript received July 15, 2022; revised December 12, 2022. This work was supported by Joint Fund Project of the National Natural Science Foundation of China (U1908218), the Natural Science Foundation project of Liaoning Province (2021-KF-12-06), and the Department of Education of Liaoning Province (LJKFZ20220197).

Mingyue. Sun is a graduate student of School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, China. (e-mail: 1441899630@qq.com).

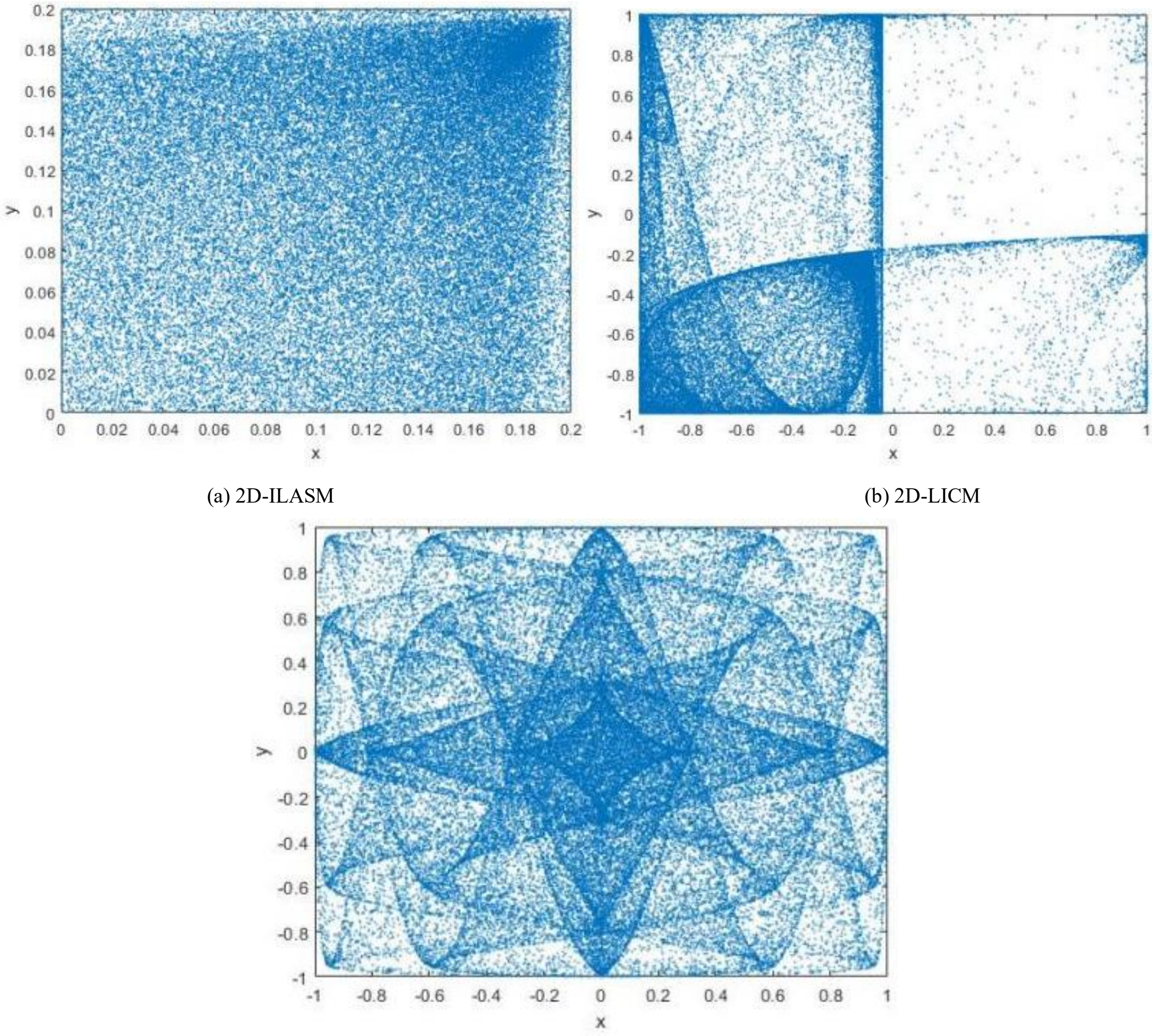
Wenhua. Cui is a Professor of School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, China. (Corresponding author to provide phone: +86-133-0422-4928; e-mail: taibeijack@126.com).

Ye. Tao is a lecturer of School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, China. (e-mail: taibeijack@163.com).

Tianwei. Shi is an associate Professor of School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, China. (e-mail: tianweiabbcc@163.com).

TABLE I
STATISTICAL RANDOMNESS TEST RESULTS

	Randomness test method	P-Value		Result
		x	y	
1	Single-bit frequency test	0.3696	0.2412	√
2	In-block frequency test	0.4575	0.4771	√
3	Run test	0.7896	0.5655	√
4	Test for longest run of ones in a block	0.3321	0.5099	√
5	Binary matrix rank test	0.2701	0.7218	√
6	Discrete Fourier (spectral) test	0.5232	0.4823	√
7	Non-overlapping template matching test	0.4564	0.2690	√
8	Overlapping template matching test	0.5440	0.8662	√
9	Maurer's "Universal Statistical" test	0.4570	0.1245	√
10	Linear complexity test	0.9656	0.5423	√
11	Sequence test	0.9895	0.2337	√
12	Approximate entropy test	0.2536	0.6567	√
13	Cumulative sums and test	0.9538	0.9940	√
14	Random travel test	0.9984	0.8770	√
15	Random travel variant test	0.6541	0.4677	√



(a) 2D-ILASM

(b) 2D-LICM

(c) 2D-NICM

Fig. 1. Phase diagrams of 2D-ILASM, 2D-LICM and 2D-NICM

system - a 2D-LICM enhanced chaotic map in two dimensions based on the one-dimensional infinite folding map (ICMIC); (2) In this paper, we propose a cyclic shift operation for RNA coding, in which RNA operations are determined by the biological composition and characteristics of the amino acids; (3) Chunking of the initial cryptographic image after RNA operations to increase the speed of operations; (4) We incorporate plain correlation in the heart shape encryption, making it impossible for an attacker to perform an attack with known plain; (5) Our experimental results and analysis of the algorithms show that our algorithm has relatively high security, fast efficiency and good applicability.

The remainder of the paper is organized as follows. Section 2 introduces related work such as 2D-NICM chaotic mapping, PWLCM chaotic mapping, RNA coding rules and operations. In Section 3, we provide a color image encryption algorithm that fuses RNA coding operations and the chaos of the cardioid chunk. Section 4 presents the experimental results, and evaluates the performance of the proposed algorithm through various experiments. Section 5 is the conclusion of this paper.

II. Preliminary work

A. 2D-NICM chaotic system

Zhang et al. [24] proposed one-dimensional infinitely folded chaotic mapping. It had a larger Lyapunov exponent than other 1D chaotic mappings. Therefore, it had stronger sensitivity to the initial value of iteration.

$$x_{i+1} = \sin(\mu / x_i) \tag{1}$$

The parameter μ ∈ (0, ∞) is given by where μ is the system parameter. ICMIC was a one parameter chaotic system with a simple topology whose state value was constrained at (0,1]. Because of the relatively small chaotic range, simple behavior and fragile chaotic interval would affect some chaos-based applications.

By concatenating two one-dimensional chaos maps, a new two-dimensional chaos map is obtained. This increases the chaotic behavior and pseudo-stochastic signal of the chaos map, as well as enlarging the key space. Moreover, [25-26] proposed the Pythagorean theorem and deformation formula. The formula yields a new chaotic system in two dimensions. The definition of chaotic 2D-NICM mapping is thus:

$$\begin{cases} x_{i+1} = \sin(a / y_i) * \cos(b / x_i) \\ y_{i+1} = \sin(a / x_i) * \cos(b / y_i) \end{cases} \tag{2}$$

From the above equation, *a*, *b* are the parameters of the chaotic mapping, *a*, *b* ∈ (0, ∞).

B. Performance evaluation of 2D-NICM chaotic systems

In this paper, we analyze the performance of chaotic 2D-NICM systems using phase diagrams, histograms of statistical sequences, and the NIST sequence randomness testing tool (SP800-22). As well as comparing it to typical chaotic one-dimensional mappings and chaotic two-dimensional mappings recently proposed in recent years.

1) Phase Diagrams

Fig. 1 shows the phase diagrams for 2D-ILASM [27], 2D-LICM [28] and 2D-NICM. Comparing these three phase diagrams, it can be seen that the range occupied by 2D-NICM is much larger than that of 2D-LICM and the uniformity of arrangement is better than that of 2D-ILASM. A good chaotic system should cover the whole phase plane uniformly. Therefore, 2D-LICM has better ergodicity and larger key space.

2) Sequence Statistics Histogram

To further study the performance of chaotic mapping, we choose 10 000 points in sequence from the chaotic sequences derived from three chaotic systems. In sequence, the statistical sequence histograms of 2D-ILASM, 2D-LICM, and 2D-NICM are shown in a, b, c, d, e, and f of Fig. 2. From a, b, c, and d of Fig. 2, it can be seen that the chaotic sequences are not uniformly distributed. 2D-ILASM has most of the data distributed on the right side and too little on the left side. 2D-LICM has most of the data concentrated on the two sides and very few in the middle. It is known that for good chaotic mapping, the histogram of chaotic sequences should be as straight as possible. As seen from e and f of Fig. 2, the 2D-NICM chaotic sequences are uniformly distributed in different intervals. As a result, it can generate more complex stochastic chaotic sequences, which is better suited for image encryption algorithms. The ideal pseudo-random lines used in cryptosystems should have good statistical properties [29].

3) NIST Sequence Randomness Test Tool (SP800-22)

The usage of the test standard of NIST SP800-22 [30,31] was introduced, and the performance of 2D-NICM chaotic mapping is analyzed. NIST SP800-22 had two test methods. First, we tested the proportion of sequences that passed statistical tests. Second, we tested whether the P-values remained consistent. Each test provided one or more p-values. And a sequence was considered random if the p-values fall into the interval (0, 1]. SP800-22 Revla recommended that the length of the bit sequence tested to be $10^3 \sim 10^7$. And here a test sequence S is used, its length n is 10^6 . Table 1 shows that the sequence under test can pass all test questions. Thus, the output sequence of the 2D-NICM can be thought of as complex and used as the key steam in image encryption. The above analysis indicates that 2D-NICM chaotic mapping is suitable for the generation of chaotic sequences with good performance. Our algorithm uses the proposed chaotic mapping to create strongly complex chaotic sequences.

C. PWLCM Chaos Mapping

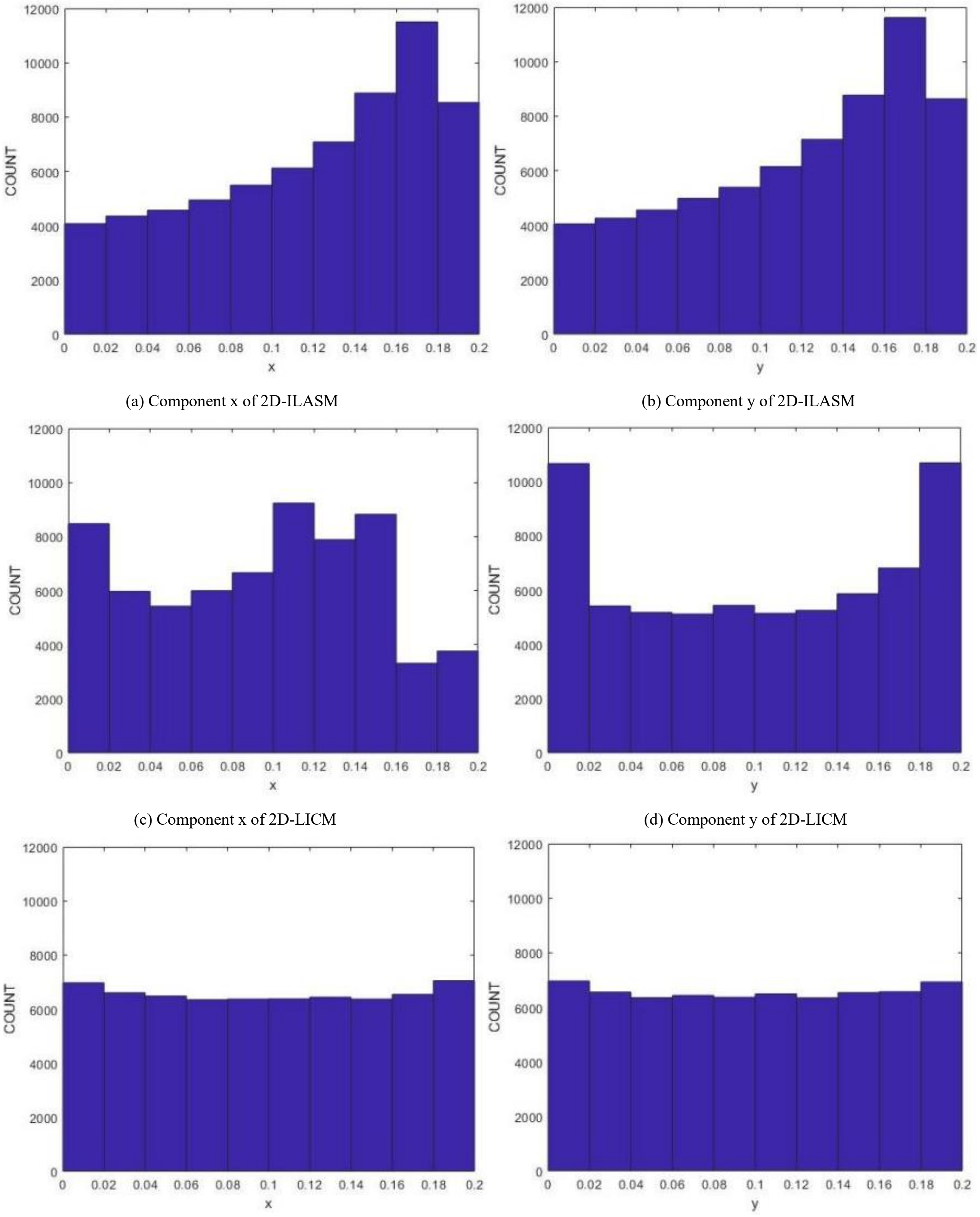
PWLCM is a chaotic mapping with simple and more expansive ergodicity [32]. Which is one of the chaotic systems most classical used in image encryption for generating good complex chaotic sequences. Therefore, it has attracted wide attention from cryptographic academia. PWLCM chaotic systems give a more comprehensive range of parameter choices. Other essential features besides simplicity and ergodicity are good dynamical behavior, simple software and hardware implementation, and uniform invariant distribution. PWLCM is defined as shown in equation (3).

TABLE 2
RNA CODING RULES OBTAINED FROM DNA TRANSCRIPTION

DNA bases	DNA bases
A	T
G	C
C	G
U	A

TABLE 3
RNA ENCODING AND DECODING RULES

Rule	1	2	3	4	5	6	7	8
00	A	A	U	U	C	C	G	G
01	C	G	C	G	A	U	A	U
10	G	C	G	C	U	A	U	A
11	U	U	A	A	G	G	C	C



(a) Component x of 2D-ILASM

(b) Component y of 2D-ILASM

(c) Component x of 2D-LICM

(d) Component y of 2D-LICM

(e) Component x of 2D-NICM

(f) Component y of 2D-NICM

Fig. 2. Serial statistical histograms of 2D-ILASM, 2D-LICM, and 2D-NICM

$$x_i = f\left(x_{i-1}, p\right)\begin{cases} \frac{x_{i-1}}{p}, 0 < x_{i-1} < p \\ \frac{x_{i-1} - p}{0.5 - p}, p \le x_{i-1} < 0.5 \\ f\left(1 - x_{i-1}, p\right), 0.5 \le x_{i-1} < 1 \end{cases} \quad (3)$$

Where p is a parameter of chaotic mapping, $0<p<0.5$, and x represents the PWLCM state variable, $0<x<1$. The initial value of the variable x_0 cannot be equal to p. The segmented linear mapping has chaotic properties when both the initial value and the parameter are within a certain numerical range.

D.RNA encoding and decoding rules

In the biogenetic process, DNA and RNA are the central substances. A DNA code is made up of four bases, namely A (adenine), C (cytosine), G (guanine) and T (thymine), which are arranged according to certain rules. An RNA sequence also consists of four bases. Only one base is different, and U (uracil) in RNA substitutes for T in DNA. Recently, DNA coding technology has been widely used in image encryption due to its excellent computational power. Chemically, the product of DNA transcription is RNA. RNA sequences can thus be obtained from DNA sequences as listed in Table 2. In RNA operations, two binary numbers are converted into a base according to 8 coding rules [33]. In light of the discussion above, this article adopts RNA coding and manipulation. A is complementary to U, and C is complementary to G. Similarly, the numbers 0 and 1 are complements in binary. Because 10 and 01, 11 and 00 are also complementary. If we encode U, A, C, and G with 11, 10, 01, and 00, there are 24 coding schemes. On the other hand, only eight of the rules in Table 3 satisfy Watson-Crick Supplementary Rule [34].

The encrypted object here is a color picture, which can be represented by three color channels: red (R), green (G) and blue (B). For example, if there is a pixel whose gray value is 167 in the red channel, its binary value is [10100111]. Following the RNA coding Rule 1 of Table 3, we can obtain the [GGCU] RNA value. If we use Rule 1 to decode the RNA value, we will obtain the correction [10100111]. On the other hand, if we use Rule 2, we will get the wrong bit value [01011011]. The above analysis allows us to understand that image pixel values can be converted to RNA sequences through RNA coding operation. The DNA sequence can be restored to pixel values by reverse RNA decoding.

In protein synthesis, the 3 neighboring bases that identify amino acids in the mRNA (messenger ribonucleic acid) chain are called genetic codons. The genetic code is a set of rules. According to this rule, codons of three nucleotides in a DNA or RNA sequence are translated into the amino acid sequence of a protein. These amino acid sequences can be used in protein synthesis. To determine the number of these nucleotides, people have carried out a large number of experiments. The study has found that RNA has four bases, combining every third base into one codon. Theoretically, 4 × 4 × 4 = 64 base combinations or 64 codons, as shown in Table 4. Despite the fact that there are 20 naturally occurring amino acids, 61 coding codons, and 3 stop codons (stop codons are the 3 nucleotides on mRNA that announce the termination of the translation process), in some animals, the genome has up to 270 tRNAs. The genetic code is the same in almost all animals.

III. Algorithm design and implementation

For the purposes of this paper, image encryption consists of 4 parts. The first step is to split the color image into 3 channels: R, G, and B. They run the same encryption algorithm. Using channel R as an example, the notion of an RNA algorithm is first used for encoding and decoding. Subsequently, the encoded initial cipher image is divided into blocks. And 256 × 256 images are divided into 4096 blocks of 4 × 4 image blocks. Afterward, the upper left heart-shaped "diffusion-confusion" encryption is performed in turn in the image blocks. Among them, the scrambling adopts the scrambling mode of plain-related. "Diffusion-scrambling" adopts the encryption mode of "forward diffusion-plain-related confusion operation-backward diffusion." Finally, three channels are merged to obtain the final encrypted color image. The encryption process is shown in Fig. 3.

A. RNA operations based on 2D-NICM for chaotic systems

Weaknesses of a single chaotic system include low key space, simple structure and high correlation. For this reason, we propose a novel color image encryption scheme with unfixed coding rules. The method first stratifies the images, and encodes RNA for R, G, and B images. They are reducing the complexity and computation of spatial computation. Then, the 2D-NICM chaotic sequence performs left and right cyclic shift operations on the encoded matrix. Reducing the risk of being vulnerable to attacks using traditional RNA operators. The RNA operations based on the chaotic system 2D-NICM are as follows:

Set parameters of 2D-NICM chaos *a* is 21, *b* is 1 and the initial value *x (1)* is 0.3, *y (1)* is 0.6. Iterate 1000 times to skip the transition state. Then $M \times N$ times are continued iterating to obtain three complex sequences *x1*, *y1*, and *z1*. In order to resist known plain attacks and increase the sum of plain pixels, the operation of formula (4) (5) is carried out.

$$\begin{cases} sum1 = sum(sum(PR)) \\ sum2 = sum(sum(PG)) \\ sum3 = sum(sum(PB)) \end{cases} \quad (4)$$

$$\begin{cases} x1 = \mathrm{mod}(floor(double(x) * sum1), 8) + 1 \\ y1 = \mathrm{mod}(floor(double(y) * sum2), 8) + 1 \\ z1 = \mathrm{mod}(floor(double(z) * sum3), 8) + 1 \end{cases} \quad (5)$$

Where *sum* is the summation operation; *floor(a)* the greatest integer less than or equal to the digit *a*; *double(s)* converts *s* into a double precision floating point number; *Pr*, *Pg*, and *Pb* represent the R, G, and B plain images, respectively.

Known as plain M rows and N columns. Change the *Pr*, *Pg*, and *Pb* arrays to 1 row $M \times N$ columns and round up, in the range 0~256. Called *ppr*, *ppg*, and *ppb*. Then change the decimal array to binary, as shown in the formula (6). *ppg* and *ppb* are the same, and the binary arrays Pg_bit and Pb_bit are obtained.

TABLE 4
GENETIC CODON

Num	Codon	Num	Codon	Num	Codon	Num	Codon
1	‘AAA’	17	‘CAA’	33	‘GAA’	49	‘UAA’
2	‘AAC’	18	‘CAC’	34	‘GAC’	50	‘UAC’
3	‘AAG’	19	‘CAG’	35	‘GAG’	51	‘UAG’
4	‘AAU’	20	‘CAU’	36	‘GAU’	52	‘UAU’
5	‘ACA’	21	‘CCA’	37	‘GCA’	53	‘UCA’
6	‘ACC’	22	‘CCC’	38	‘GCC’	54	‘UCC’
7	‘ACG’	23	‘CCG’	39	‘GCG’	55	‘UCG’
8	‘ACU’	24	‘CCU’	40	‘GCU’	56	‘UCU’
9	‘AGA’	25	‘CGA’	41	‘GGA’	57	‘UGA’
10	‘AGC’	26	‘CGC’	42	‘GGC’	58	‘UGC’
11	‘AGG’	27	‘CGG’	43	‘GGG’	59	‘UGG’
12	‘AGU’	28	‘CGU’	44	‘GGU’	60	‘UGU’
13	‘AUA’	29	‘CUA’	45	‘GUA’	61	‘UUA’
14	‘AUC’	30	‘CUC’	46	‘GUC’	62	‘UUC’
15	‘AUG’	31	‘CUG’	47	‘GUG’	63	‘UUG’
16	‘AUU’	32	‘CUU’	48	‘GUU’	64	‘UUU’

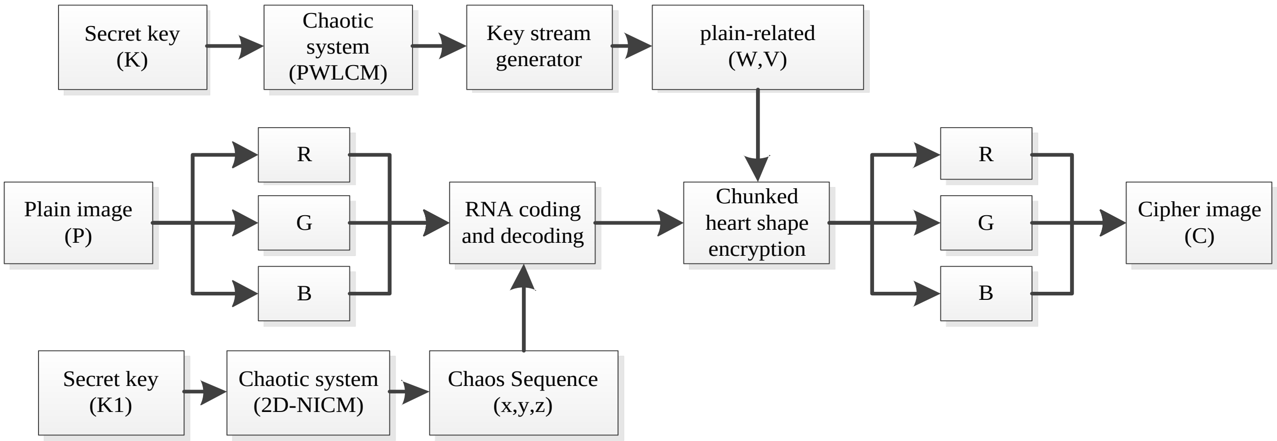


Fig. 3. Encryption flow chart

$$Pr\_bit = dec2bin(ppr) \qquad (6)$$

Where *dec2bin(t)* converts a decimal number t into a binary number represented in the form of a string. Three binary numbers are associated with plain. The generated chaos sequence together determines the code rules of RNA. That is, different images have different code rules. This process increases the difficulty of attack and effectively strengthens encryption security. The following is a textual explanation of Fig. 4.

Step 1. A pixel value is randomly taken from the three R, G, and B images. In turn, to form a 3 × 1 dimensional matrix I . And which is transformed into a matrix I_1 composed of binary numbers.

Step 2. The encoding rules are determined by the values of *Pr_bit*, *Pg_bit*, *Pb_bit* and the three chaotic sequences *x1*, *y1*, *z1* generated by the 2D-NICM chaotic system associated with plain. Take the RNA code rules in Table 3 as standard. Assuming that Rule 3 is used, the binary matrix I_1 is dynamically encoded by RNA to generate RNA matrix I_2 .

Step 3. A total of 64 combined amino acids are known, as shown in Table 4. The matrix I_2 at the end of coding is converted into an RNA genetic code matrix I_3 using Table 4 turn.

Step 4. In the case of the three chaotic sequences generated by chaotic 2D-NICM mappings with plain-related are *x1*, *y1*, and *z1*. *x1*+*y1* and *y1*+*z1* are used as the sequences required for cyclic shifting of rows and columns, respectively, as shown in (7). As an example, the cyclic shift operation inside the amino acid is performed according to the $I_3 \sim I_4$ process shown in Fig. 4. The operation equation is shown in (8).

$$\begin{aligned} left &= \mathrm{mod}(round((x1(1:20)+y1(1:20))* \\ &\qquad (sum1+sum2)),3)+1 \\ right &= \mathrm{mod}(round((y1(1:20)+z1(1:20))* \\ &\qquad (sum3+sum2)),65536)+1 \end{aligned} \qquad (7)$$

$$b = circshift(a,[left,right]) \qquad (8)$$

Where *round(a)* rounding off *a* to the nearest integer; $circshift(t,[left,right])$ performs a cyclic displacement operation on *t*.

Step 5. Taking the conversion of adenine as an example, this step converts from genetic codon matrix I_4 back to RNA encoding matrix I_5 .

Step 6. Decoding: The matrix I_5 is RNA decoded according to the corresponding rules to obtain the binary matrix I_6 . Complete the RNA encoding encryption.

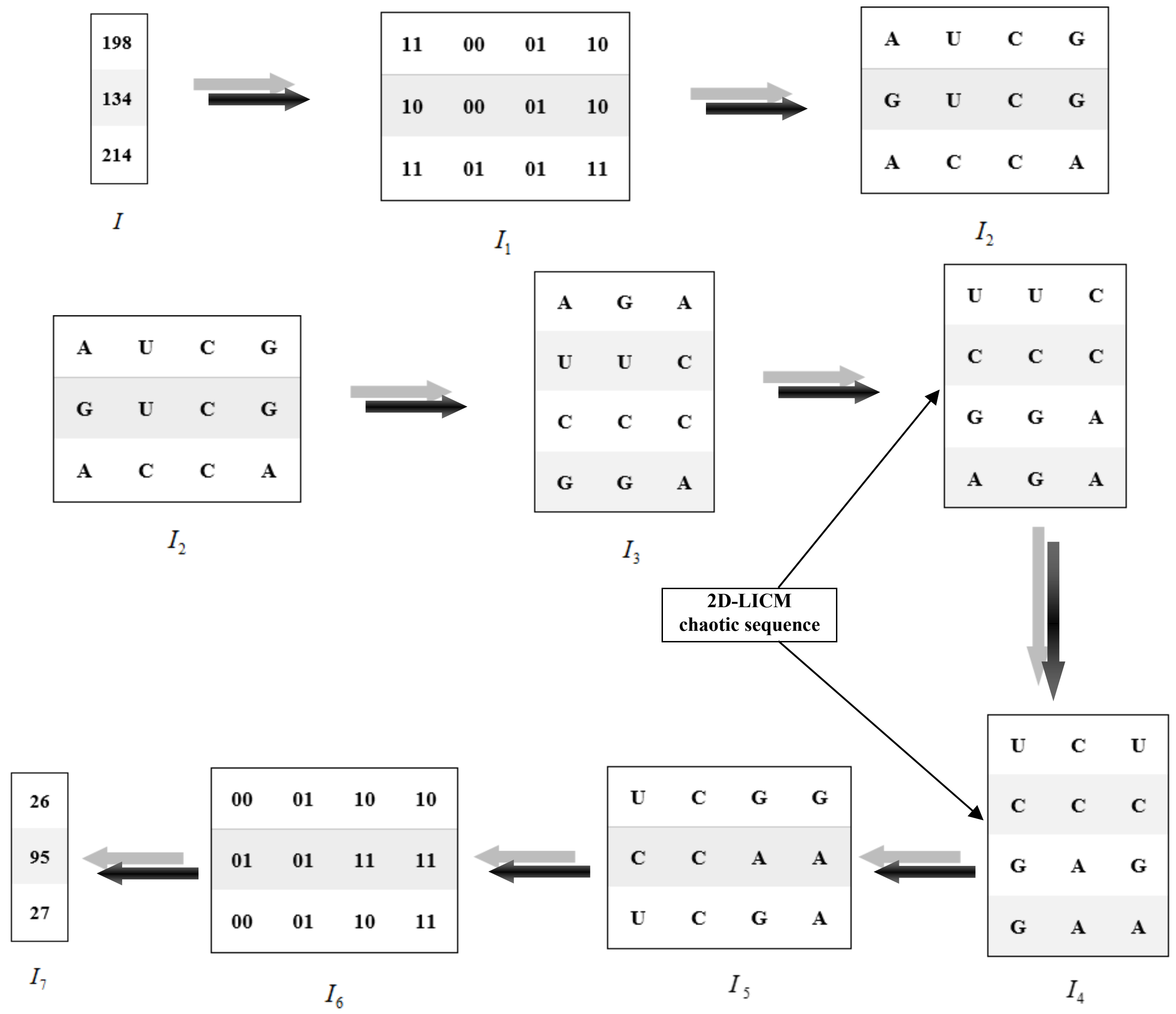


Fig. 4. Example of RNA encryption process

B. Chunked heart shape encryption based on PWLCM mapping

The goal of this section is to improve the speed and Safety of the digital image encryption algorithm. Firstly, it is a chunking operation, and subsequent encryption algorithms are executed sequentially within the chunk. Secondly, the classical PWLCM chaotic system combines the plain, and the resulting chaotic sequence is diffused and scrambled. The encryption is performed in the form of "forward diffusion-scrambling of plain-associated-backward diffusion,". In the encryption algorithm, diffusion uses heart-shaped diffusion, and scrambling uses plain correlation scrambling. In order to prevent the attacker from destroying the encrypted image using known plains. The PWLCM mapping-based chunked heart shape encryption algorithm operates as follows.

1) Chaotic cipher generator

The encryption generator uses the chaotic PWLCM mapping to generate two complex matrices. Both matrices have the same dimension as the original plain image. Referred to as W, V, and the size is $M \times N$. The steps for generating these two chaotic matrices are:

Step 1. Set the initial value w_0 and variable parameter *b* of formula (3). After iterating PWLCM $t_1 + t_2$ times, the chaotic cipher generator passes through the filter state. And then iterates $M \times N$ times to obtain the sequence with a length of $M \times N$, denoted as $\{w_i\}, i = 1, 2, \cdots, MN$.

Step 2. The initial value v_0 of formula (3) and the variable Parameter *d*. When the iteration PWLCM $t_3 + t_4$ times, the chaotic cipher generator passes through the filter state. And then iteration $M \times N$ times to obtain the same sequence length as step 1, referred to as $\{v_i\}, i = 1, 2, \cdots, MN$.

Step 3. According to the vectors w_i and v_i, $i = 1, 2, \cdots, MN$. According to the formula (9) and (10), to obtain the matrix *W* and *V*.

$$W(x, y) = floor\left[\left(\frac{t_1 + 1}{t_1 + t_3 + 2} w_{x-1 \times N+y} + \frac{t_1 + 1}{t_1 + t_3 + 2} v_{x-1*N+y}\right) \times 10^{14}\right] mod\, 256 \tag{9}$$

$$V(x, y) = floor\left[\left(\frac{t_1 + 1}{t_1 + t_3 + 2} w_{x-1 \times N+y} + \frac{t_1 + 1}{t_1 + t_3 + 2} v_{x-1*N+y}\right) \times 10^{13}\right] mod\, 256 \tag{10}$$

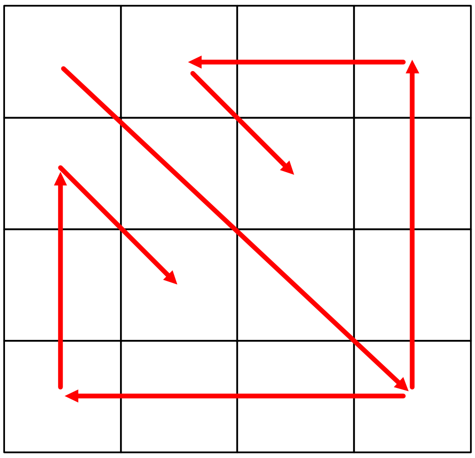


Fig. 5. Heart shape image encryption process

Where $x = 1, 2, \cdots, M$, $y = 1, 2, \ldots N$. In the encryption algorithm, the chaos matrix generated by the password generator is used for the broadcast and jamming algorithm.

2) Chunked heart shape encryption

Let the R channel image after RNA encoding and decoding be called QR. And the size is $M \times N$, divided into matrix sub-blocks with a size of 4×4, with a total of $M \times N / 4 \times 4$ sub-blocks. The "forward diffusion-scrambling of plain association-backward diffusion" is carried out in the block. Known $M = 256$, $N=256$. This chapter uses the R channel image to do experiments. The three primary color channels, G and B, are the same.

Encryption starts from the top left corner of the 4 × 4 image block each time. Take the first 4 × 4 image block as an example (all blocks follow this algorithm), and encrypting the image pixel locations and positions according to the heart shape marching method. Fig. 5 shows that encrypting from the top left corner in the diagonal direction. Reach the diagonal vertex and divide it into two channels up and left to continue encryption. And then continue to encrypt in the diagonal order. Diffusion uses the method of XOR diffusion. The method of plain association is used for scrambling. This operation is encryption without losing any pixels. The forward diffusion algorithm process is as follows:

Step 1. Diffuse the plain coordinates (1, 1) by equation (11).

$$E(1,1) = bitxor(P(1,1), W(1,1)) \tag{11}$$

Where P is the plain, E is the encrypted cipher. And the cipher is collectively referred to as E after each round of encryption.

Step 2. XOR diffusion of diagonal pixels is carried out through formula (12), taking (3,3) points on the diagonal as an example.

$$E(3,3) = bitxor(bitxor(P(3,3), W(3,3)), C(2,2)) \tag{12}$$

Step 3. Diffuse the points in the lower right corner upward and left respectively. Through formulas (13) and (14), taking points (1,3) upward and points (3,1) left as examples.

$$E(1,3) = bitxor(bitxor(P(1,3), W(1,3)), E(1,4)) \tag{13}$$

$$E(3,1) = bitxor(bitxor(P(3,1), W(3,1)), E(4,1)) \tag{14}$$

The plaintext pixel value, the point pixel value of the chaotic matrix, and the random pixel value after scattering is XOR exploited to generate the encrypted pixel value. R image repeats the diffusion process from the first step to the third step, making each pixel diffuse at least once. Backward diffusion is the reverse process of forwarding diffusion as a whole. Starting from (2, 3) (3, 2), respectively, and spreading in the opposite direction of the arrow in Fig. 4. Then the permutation of the plain association is performed. And the pixel points E (i, j), $i = 1, 2, \ldots, M/4$, $j = 1, 2, \ldots, N/4$, and E (s, t) permute their positions. The replacement steps are as follows:

Step 1. Compute the sum of all the items (excluding E (i, j)) in the row where E (i, j) is located, and count it as row_i; Compute the sum of column elements, and count it as col_i.

$$\begin{aligned} row_i &= sum(E(i,1 \text{ to } N/4)) - E(i,j) \\ col_i &= sum(E(1 \text{ to } M/4, j)) - E(i,j) \end{aligned} \tag{15}$$

Step 2. Calculate the value of the coordinate (s, t).

$$\begin{aligned} s &= row_i + V(i,j) \bmod M \\ t &= col_i + V(i,j) \bmod N \end{aligned} \tag{16}$$

Step 3. If $s = i$ or $t = j$, the position remains unchanged. Otherwise, $E(i, j)$ and $E(s, t)$ exchange positions. At the same time, according to the value of the lower three digits of E (s, t), E (i, j) is subjected to a shift operation. Shift operation according to formula (17).

$$E(i,j) = E(i,j) <<< (E(s,t) \,\&\, 0x7) \tag{17}$$

Here, $x<<<y$ means that x is cyclically shifted left by y bits. According to steps 1 to 3, the last row of matrix E is rearranged first. Next, the end column of matrix E is scrambled. Then the matrix E is shuffled sequentially depending on the sequence of scanning from left to right. Then from top to bottom, the image is obtained after complete scrambling, referred to as F. Finally, after backward diffusion, the encrypted cipher C is obtained.

There are two encryption algorithms for the image encryption devised in this chapter. And add plain elements to the chaotic sequence generation and scrambling algorithm. This method makes the encryption algorithm less vulnerable to known plain attacks.

C. Image Decryption

The decryption of images is the reverse of the encryption algorithm. And the same two small rounds of image decryption are performed. First, the second algorithm reverse operation of image encryption. Take the ciphertext as the unit to reconstruct the position and size of each pixel. The Second is the reverse operation of the first algorithm of image encryption. The inverse action of RNA encoding and decoding is performed. Merge the three primary colors to get the initial color image. Fig. 6 shows the specific steps.

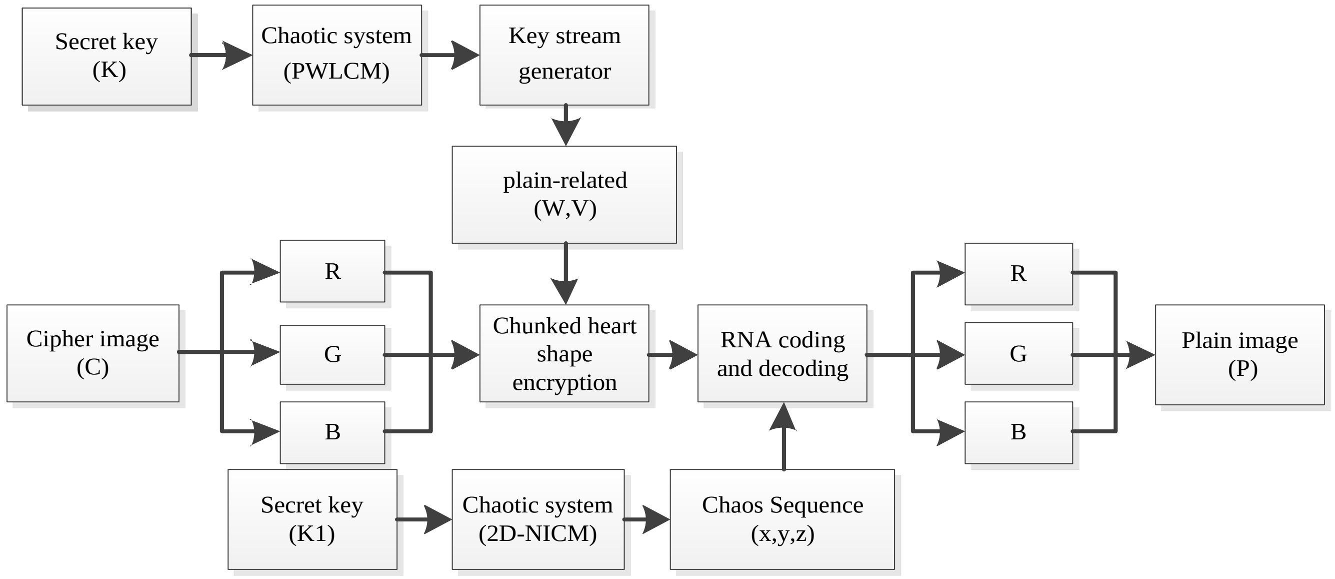


Fig. 6. Image decryption flow chart

IV. Simulation Results and Analysis

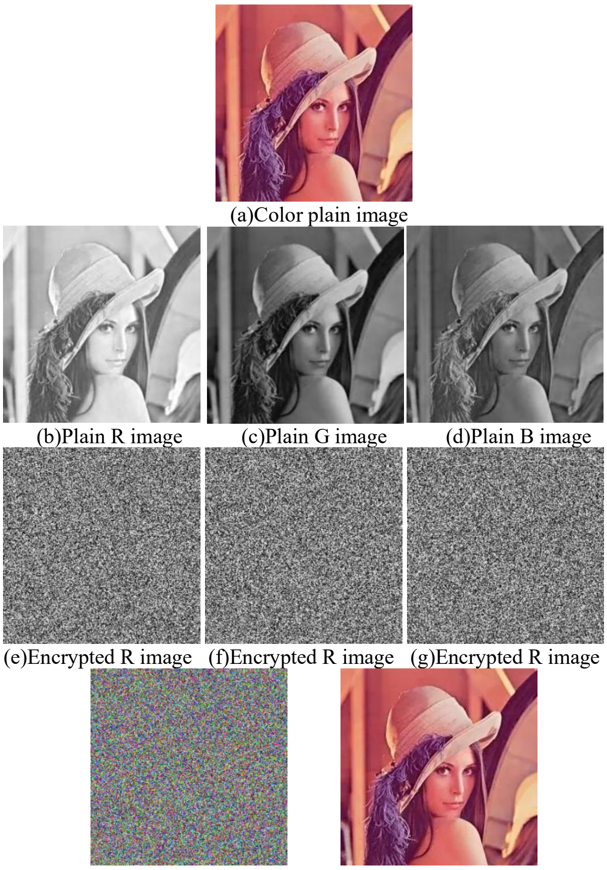
A good color image encryption algorithm can withstand many classic used attacks. Such as resistance to exhaustive attacks, resistant statistical attacks, and resistant differential attacks. Detailed figures, tables, and descriptions are given in this section to measure the proposed algorithm's performance. The statistics show the color image, and the adjacent pixel correlation for the encrypted color image. The correlation coefficients, information entropy, sensitivity and resistance to differential attacks between key space, normal color images and color coded images are given as figures and tables below. Finally, we compare the results to some similar algorithms.

A. Experimental results

In this paper, 256 × 256 color images are used for encryption and decryption simulation experiments. And the simulation environment is the MatlabR2020b software platform. The first is to use the encryption algorithm to encrypt the image. And the image of the cipher is then decrypted by the given key and decryption algorithms. Using the color image of Lena as an example, Fig. 7 shows the experimental results.

B. Key Space Analysis

A key space is a set of all lawful keys [35]. If the key space is ample, the attack time and cost will become high, making it impossible for attackers to use exhaustive attacks. As the size of the key space increases, the performance of the algorithm against exhaustive attacks increases [36]. In the image encryption algorithm in this chapter, the key of chunked cardioid encryption $K_1=\{w_0,x,v_0,y,t_1,t_2,t_3,t_4\}$. Where $w_0,v_0\in(0,1)$, the step size is 10^{-14}, $t_1\sim t_4$ is an integer in [0,255], and the step is 1. So, the key space size of key K_1 is about 1.0737×10^{65}.


(a)Color plain image

(b)Plain R image (c)Plain G image (d)Plain B image

(e)Encrypted R image (f)Encrypted R image (g)Encrypted R image

(h)Encrypting Lena image (i)Decrypting Lena image

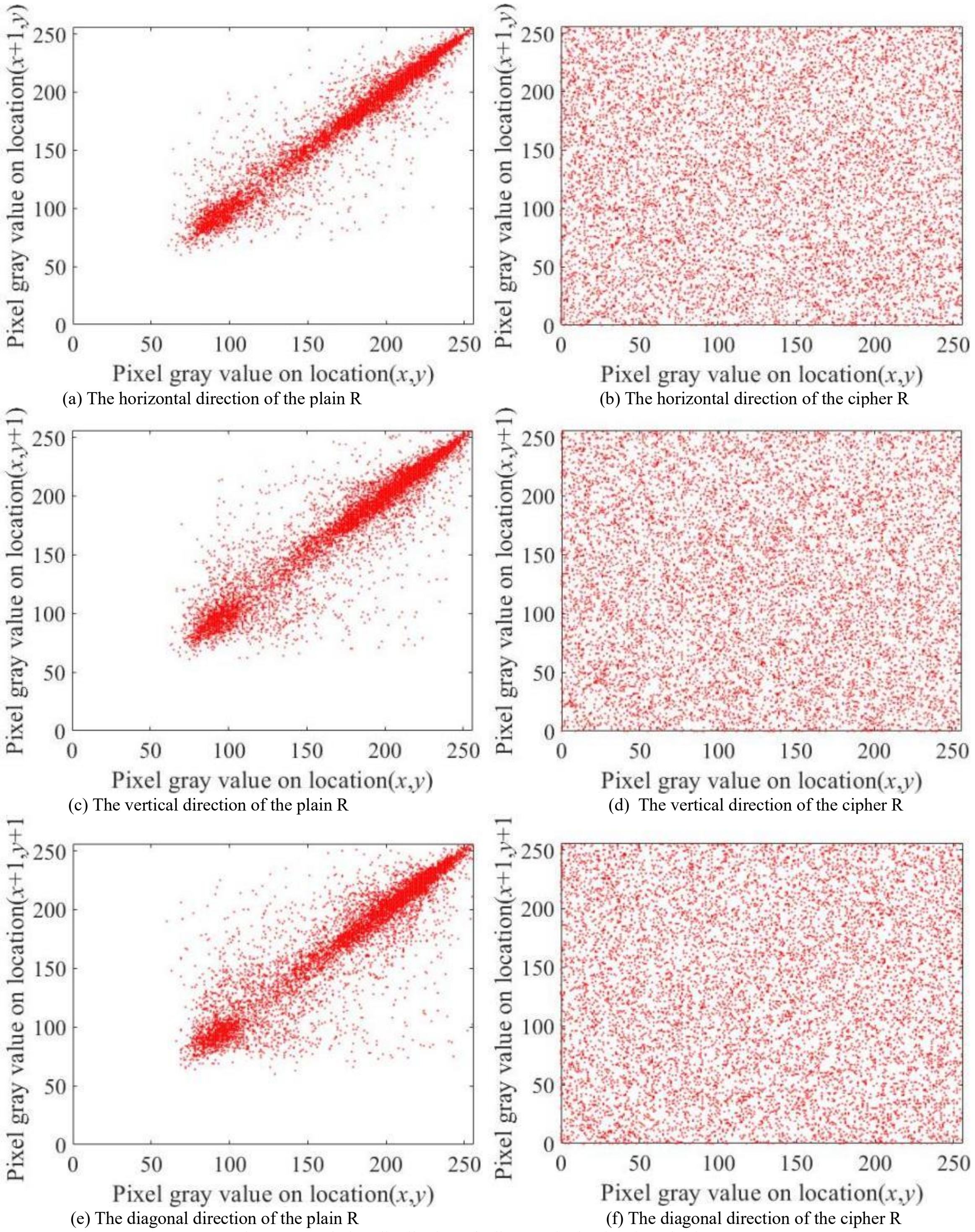
Fig. 7. Comparison of image encryption and decryption effects

TABLE 5
KEY SPACE COMPARISON

	Proposed	Ref. [2]	Ref. [3]	Ref. [4]	Ref. [19]	Ref. [20]
Key Space	10^{129}	10^{111}	10^{203}	10^{87}	10^{78}	10^{222}

TABLE 6
ADJACENT PIXEL CORRELATION COMPARISON

Images			Horizontal	Vertical	Diagonal
Lena	This article (plain)	Average value	0.9709	0.9448	0.9437
	This article(cipher)	Average value	-0.0087	-0.0063	0.0009
	Ref. [2] (cipher)	Average value	-0.0304	-0.0056	0.0058
	Ref. [3] (cipher)	Average value	0.0019	0.0035	0.0008
	Ref. [20] (cipher)	Average value	0.0040	0.0010	0.0012



(a) The horizontal direction of the plain R
(b) The horizontal direction of the cipher R
(c) The vertical direction of the plain R
(d) The vertical direction of the cipher R
(e) The diagonal direction of the plain R
(f) The diagonal direction of the cipher R

Fig. 8. Correlation distribution of adjacent pixel points in color image

The key K_2 used for RNA encoding is $\{x_0, y_0, a, b\}$. And if the system accuracy is 10^{16}, the key space K_2 of this scheme is $10^{16} \times 10^{16} \times 10^{16} \times 10^{16} = 10^{64}$. In ref. [37] it was stated that the key space should be greater than or equal to 2^{100}. At this time, the algorithm can guarantee the security of image encryption. Since $2^{10} \approx 10^3$, the key space in this paper is about 10^{129}, this algorithm is able to withstand exhaustive attacks. See Table 5 for a comparison with other literature results.

C. Statistical characteristic analysis

1) Correlation analysis

One way to measure the effectiveness of encryption is to perform correlation analysis. The lower the image correlation, the better the effect of encryption. Qualitative analysis makes an intuitive decision on the correlation strength of adjacent pixels by observing the correlation situation diagram of adjacent pixels; quantitative analysis compares the strength of correlation in quantity by calculating the correlation coefficient of adjacent pixels. If we assume that any N pairs of adjacent pixels are drawn from the image to be studied. And the values of their pixels are *(S, T)*, $i = 1, 2, \cdots, N$. The vector *S* = *{s}* and *T* = *{t}* The correlation coefficient calculation formula is as follows.

$$r_{xy} = \text{cov}(s,t) / (\sqrt{D(s)}\sqrt{D(t)}) \tag{18}$$

$$\text{cov}(s,t) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(s))(y_i - E(t)) \tag{19}$$

$$D(s) = \frac{1}{N}\sum_{i=1}^{N}(s_i - E(s))^2 \tag{20}$$

$$E(s) = \frac{1}{N}\sum_{i=1}^{N} s_i \tag{21}$$

Among them, *N* is the number of point pixels. *E(s)* and *E(t)* is the expectations of *s*, *t*, respectively. $COV(s,t)$ is the covariance, and *r* is the correlation coefficient. Using the channel R as an example, the encryption algorithm constructed in this paper is compared to the average correlation value of the encryption algorithm proposed in the literature [20], cf. Table 6. The three channel adjacent pixel correlation of Lena plain and cipher images obtained through this paper is shown in Fig. 8.

As shown in Fig. 8, on the three channels R. In all directions, pairs of adjacent pixels in a plain image are densely distributed over the line y = x. This is in contrast to adjacent pairs of pixels in a cypher image in all directions, which are uniformly distributed across the area (the smaller left corner coordinates are (0, 0), and the coordinates of the top right-hand corner are (255, 255)). To summarize, the plain image is highly correlated in all directions; the cipher image is uncorrelated in every direction.

It can be seen from Table 6 that the infinity of adjacent pixel correlation of ordinary images approaches 1, indicating that the correlation of ordinary images is strong. The infinite correlation of adjacent pixels in a cryptographic image approaches 0. At this time, the image is approximation uncorrelated (the correlation of two independent, uncorrelated chaotic sequences is theoretically 0). To summarize, the cipher image in this chapter is more approximate to the noise feature and can withstand statistical attacks more effectively.

2) Histogram analysis

The distribution of individual pixel values across the image is characterized by an image's histogram [38]. In the case of a uniform distribution of pixel value histogram, this approach is effective against statistical-based attacks. Figures 9 (a), (c), and (e) are the histograms of the original three channels of gray image distribution of Lena before encryption. (b), (d), and (f) are the distribution histograms of the three channels of the encrypted Lena image.

D. Sensitivity analysis

Two methods of analyzing the sensitivity of image cryptosystem are qualitative analysis and quantitative analysis. This section examines the sensitivity quantitatively. The two main indicators are pixel change rate (NPCR) and mean change intensity of normalization (UACI). Their theoretical values are 9 and 10, respectively. The chaotic image encryption algorithm is better able to withstand differential attacks when the experimental value is infinitely near the theoretical value.

As we all know, the function of NPCR is to compare the pixel values in the same position in two images. And record the ratio of the number of different pixels to the total. And the formula is shown in equation (22). The purpose of UACI is to compare pixels at the same location in two images. Then calculate the average of the difference between each pixel and the maximum difference. And this formula is shown in Equation (23).

$$NPCR(p_1, p_2) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} Sign \\ (p_1(i,j) - p_2(i,j)) \times 100\% \tag{22}$$

$$UACI(p_1, p_2) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} |p_1 - p_2| \\ / (255 - 0) \times 100\% \tag{23}$$

In the formula: *Sign (·)* means the following:

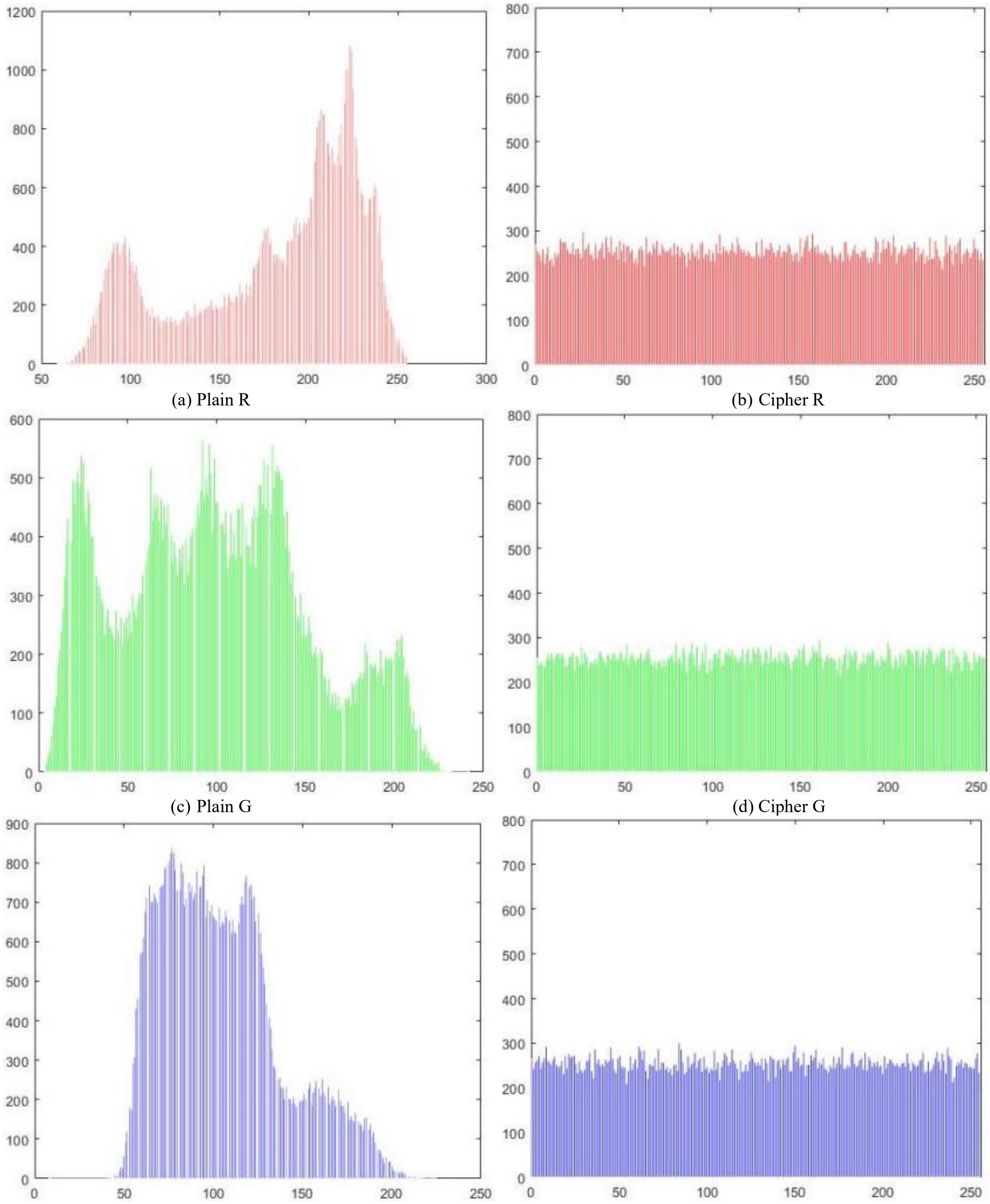
$$sign(x) = \begin{cases} 1, x > 0 \\ 0, x = 0 \\ -1, x < 0 \end{cases} \tag{24}$$

TABLE 7
KEY SENSITIVITY AND COMPARISON IN THIS PAPER

	Proposed Algorithm	Ref. [2]	Ref. [3]	Ref. [4]	Ref. [19]	Ref. [20]	Theoretical value
NPCR（%）	99.6083	99.6833	99.6145	99.6401	99.6457	99.6197	99.6094
UACI（%）	33.4637	33.4900	33.4572	33.4775	33.5835	33.3857	33.4635

TABLE 8
SENSITIVITY AND COMPARISON OF PLAIN IN THIS PAPER

	Proposed Algorithm	Ref. [2]	Ref. [3]	Ref. [4]	Ref. [19]	Ref. [20]	Theoretical value
NPCR（%）	99.6080	99.6133	99.6132	99.6101	99.6450	99.6065	99.6094
UACI（%）	33.4620	33.4233	33.4236	33.6230	33.6216	33.3930	33.4635



(a) Plain R

(b) Cipher R

(c) Plain G

(d) Cipher G

(e) Plain B

(f) Cipher B

Fig. 9. Histogram of grayscale value distribution before and after Lena color image encryption

1) Key sensitivity analysis

Minor changes are made to the keys to test the sensitivity of the key. For the selected keys K_1 and K_2, randomly change one of its bits (only one value is modified at a time, and the rest of the values remain unchanged). The key of K_1 changes 10^{-15} each time, and the key of K_2 changes one each time. Encrypting the same plain image with the key of K_1 changes 10^{-15} each time, and the key of K_2 changes one each time. Encrypt the same plain image with the key before and after the change, and calculate their NPCR and UACI averages. Compare them with other algorithms, and analyze the key sensitivity of the algorithm. Table 7 presents the results.

TABLE 9
INFORMATION ENTROPY OF THIS PAPER AND COMPARISON

	Passage	Proposed Algorithm	Ref. [2]	Ref. [3]	Ref. [4]	Ref. [19]	Ref. [20]
Lena	R	7.9987	7.9993	7.9994	7.9970	7.9971	7.9953
	G	7.9986	7.9972	7.9993	7.9968	7.9971	7.9955
	B	7.9982	7.9984	7.9993	7.9973	7.9971	7.9969
	Average value	7.9985	7.9983	7.9993	7.9970	7.9971	7.9959

As shown in Table 7, the algorithm NPCR, and UACI values in this paper are close to the theoretical values. Compared with other algorithms, the algorithm proposed in this paper is closer, which verifies that the algorithm in this paper has better sensitivity to keys.

2) Plain sensitivity analysis

Modify the plain image P slightly before the image is encrypted in order to test sensitivity to the encrypted plain. Each pixel point is chosen at random from the chosen plain image P, and its value is varied by an amount of 1. The changed value is R. The image with a slight difference from P is obtained. The difference between the two is compared, and the mean values of NPCR and UACI are counted. And, compared with other algorithms, plain text sensitivity analysis is performed on the algorithm, and the comparative analysis is shown in Table 8.

As shown in Table 8, the algorithm NPCR and UACI mean are close to the theoretical value. Compared with other algorithms, it is closer. This verifies the effectiveness of the algorithm in this paper to resist selected plain text attacks and known plain text attacks.

E. Information entropy

Information entropy is an undecidable measure of image content. For a good encrypted image, its information entropy should be infinitely close to 8 [39]. For encrypted images, entropy may be calculated using the following formula:

$$H(t) = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{25}$$

Where p_i represents the probability of occurrence of symbol t_i in the cipher image. And the range of possible values of symbol *t* is the set $\{t_1, t_2, \cdots, t_n\}$, $i = 1, 2, \cdots, n$, and $1 > p_i > 0$, $p_1 + p_2 + \cdots + p_n = 1$. The analysis of algorithm information entropy in this paper is shown in Table 9. The table shows that the algorithm in this paper is closer to the theoretical value. Therefore, the algorithm in this paper can resist foreign entropy attacks more effectively.

V. CONCLUDING REMARKS

Here we propose a novel RNA operation combined with the piecewise heart-shaped encryption algorithm. Combining plain images with chaotic sequences generated by the 2D-LICM chaos system and PWLCM chaos mapping. This step can improve the performance of plain associations. The three channels of the solid color image are then separated. After converting RNA encoding into amino acids, a 2D-LICM chaotic sequence is used for shift operation. We use the chaotic PWLCM series generated by the chaotic mapping for piecewise heart-shaped ciphers. The scrambling of plain associations provides better protection against known plain attacks. Based on the emulation results and the analysis, it can be seen that the algorithm in this paper has the advantages of a large key space, high sensitivity to both plaintext and keys, and good statistical features. As a result, the algorithm of this paper can withstand common attacks, including exhaustive attacks, statistical attacks, differential attacks, and so on.

REFERENCES

[1] Y.-X. Peng, K.-H. Sun, and S.-B. He, "Dynamics analysis of chaotic maps: From perspective on parameter estimation by meta-heuristic algorithm," Chinese Physics B, vol. 29, no. 3, pp030502, 2020.

[2] Y. Xiao, and X. Tong, "An Image Encryption Algorithm Based on Four Dimensional Hyperchaotic System," 2021 IEEE 12th International Conference on Software Engineering and Service Science (ICSESS), 2021, pp38-41.

[3] X. Zhang, and X. Yan, "Adaptive Chaotic Image Encryption Algorithm Based on RNA and Pixel Depth," Electronics, vol. 10, no. 15, pp1770, 2021.

[4] M. Es-Sabry, N. El Akkad, M. Merras, A. Saaidi, and K. Satori, "A New Color Image Encryption Algorithm Using Multiple Chaotic Maps with the Intersecting Planes Method," Scientific African, ppe01217, 2022.

[5] R. Chu, S. Zhang, and X. Gao, "A Novel 3D Image Encryption Based on the Chaotic System and RNA Crossover and Mutation," Frontiers in Physics, pp57, 2022.

[6] J. Zheng, and Q. Zeng, "An image encryption algorithm using a dynamic S-box and chaotic maps," Applied Intelligence, pp1-15, 2022.

[7] Z. Guo, and P. Sun, "Improved reverse zigzag transform and DNA diffusion chaotic image encryption method," Multimedia Tools and Applications, vol. 81, no. 8, pp11301-11323, 2022.

[8] M. Li, M. Wang, H. Fan, K. An, and G. Liu, "A novel plaintext-related chaotic image encryption scheme with no additional plaintext information, " Chaos, Solitons & Fractals, vol. 158, pp111989, 2022.

[9] M. Yan, and J. Xie, "A conservative chaotic system with coexisting chaotic-like attractors and its application in image encryption," Journal of Control and Decision, pp1-13, 2022.

[10] H. Zhu, Y. Zhao, and Y. Song, "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption," IEEE Access, vol. 7, pp14081-14098, 2019.

[11] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," Optics and Lasers in Engineering, vol. 121, pp203-214, 2019.

[12] C. Pak, and L. Huang, "A new color image encryption using combination of the 1D chaotic map," Signal Processing, vol. 138, pp129-137, 2017.

[13] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated chaotic systems for image encryption," Signal Processing, vol. 147, pp133-145, 2018.

[14] 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 and Applications, vol. 78, no. 9, pp12027-12042, 2019.

[15] X. Wang, and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," Optics and Lasers in Engineering, vol. 137, pp106393, 2021.

[16] X. Wang, and M. Zhao, "An image encryption algorithm based on hyperchaotic system and DNA coding," Optics & Laser Technology, vol. 143, pp107316, 2021.

[17] A. N. Kengnou Telem, H. B. Fotsin, and J. Kengne, "Image encryption algorithm based on dynamic DNA coding operations and 3D chaotic systems," Multimedia Tools and Applications, vol. 80, no. 12, pp19011-19041, 2021.

[18] Z. Guo, and P. Sun, "Improved reverse zigzag transform and DNA diffusion chaotic image encryption method," Multimedia Tools and Applications, vol. 81, no. 8, pp11301-11323, 2022.

[19] R. Chu, S. Zhang, and X. Gao, "A Novel 3D Image Encryption Based on the Chaotic System and RNA Crossover and Mutation," Frontiers in Physics, pp57, 2022.

[20] D. Zhang, L. Chen, and T. Li, "Hyper-chaotic color image encryption based on transformed zigzag diffusion and RNA operation," Entropy, vol. 23, no. 3, pp361, 2021.

[21] A. Ghorbani, M. Saberikamarposhti, and M. Yadollahi, "Using Ribonucleic acid (RNA) and Hénon map in new image encryption scheme," Optik, vol. 259, pp168961, 2022.

[22] M. Cui, Y. Chen, C. Zhang, X. Liang, T. Wu, S. Liu, H. Wen, and K. Qiu, "Chaotic RNA and DNA for security OFDM-WDM-PON and dynamic key agreement," Optics Express, vol. 29, no. 16, pp25552-25569, 2021.

[23] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the feistel network and dynamic DNA encoding," IEEE Photonics Journal, vol. 10, no. 4, pp1-14, 2018.

[24] C. Wu, K. Sun, and Y. Xiao, "A hyperchaotic map with multi-elliptic cavities based on modulation and coupling," The European Physical Journal Special Topics, vol. 230, no. 7, pp2011-2020, 2021.

[25] S. A. Touk, Z. Al Houchan, and M. El Bachraoui, "On q-analogues for trigonometric identities," Analysis, vol. 40, no. 2, pp105-112, 2020.

[26] C. Fleurant, and S. Bodin-Fleurant, "Trigonometry, Geometry of Plane and Space," Mathematics for Earth Science and Geography, pp67-96, 2019.

[27] X. Zhang, and X. Yan, "Adaptive Chaotic Image Encryption Algorithm Based on RNA and Pixel Depth," Electronics, vol. 10, no. 15, pp1770, 2021.

[28] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," Signal Processing, vol. 143, pp122-133, 2018.

[29] H.-X. Zhao, S.-C. Xie, J.-Z. Zhang, and T. Wu, "Efficient image encryption using two-dimensional enhanced hyperchaotic Henon map," Journal of Electronic Imaging, vol. 29, no. 2, pp023007, 2020.

[30] P. Zhou, and S. Wei, "A Novel Scrambling Method Based on Coupling Mode Switching Strategy for Digital Chaos," International Journal of Bifurcation and Chaos, vol. 32, no. 07, pp2250094, 2022.

[31] Z. Mengdi, Z. Xiaojuan, Z. Yayun, and M. Siwei, "Overview of Randomness Test on Cryptographic Algorithms." Journal of Physics: Conference Series, vol. 1861, no. 1, pp012009, 2021.

[32] P. K. Naskar, S. Bhattacharyya, and A. Chaudhuri, "An audio encryption based on distinct key blocks along with PWLCM and ECA," Nonlinear Dynamics, vol. 103, no. 2, pp2019-2042, 2021.

[33] X. Wang, and N. Guan, "A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation," Optics & Laser Technology, vol. 131, pp106366, 2020.

[34] S. Takahashi, H. Okura, P. Chilka, S. Ghosh, and N. Sugimoto, "Molecular crowding induces primer extension by RNA polymerase through base stacking beyond Watson–Crick rules," RSC advances, vol. 10, no. 55, pp33052-33058, 2020.

[35] Y. Tao, W. Cui, J. Zhao, W. Zhang, and Z. Zhang, "A Snake Encryption Algorithm for Image with Multiple Chaos Fusion," Engineering Letters, vol. 30, no. 3, pp1034-1043, 2022.

[36] Z. Wu, P. Pan, C. Sun, and B. Zhao, "Plaintext-related dynamic key chaotic image encryption algorithm," Entropy, vol. 23, no. 9, pp1159, 2021.

[37] B. Bouteghrine, C. Tanougast, and S. Sadoudi, "Novel image encryption algorithm based on new 3-d chaos map," Multimedia Tools and Applications, vol. 80, no. 17, pp25583-25605, 2021.

[38] Y. Tao, W. Cui, and Z. Zhang, "Spatiotemporal chaos in multiple dynamically coupled map lattices and its application in a novel image encryption algorithm," Journal of Information Security and Applications, vol. 55, pp102650, 2020.

[39] A. Ghorbani, M. Saberikamarposhti, and M. Yadollahi, "Using Ribonucleic acid (RNA) and Hénon map in new image encryption scheme," Optik, vol. 259, pp168961, 2022.