Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System

QIAN LIU AND LINGFENG LIU
School of Software, Nanchang University, Nanchang 330029, China
Corresponding author: Lingfeng Liu (vatanoilcy@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 61862042.

ABSTRACT This paper combines DNA computing with double-chaos systems and proposes an algorithm for color image encryption at the bit level. First, we use Arnold algorithm to scramble the three components of the color image, and the number of iterations was determined by the average of the three components, which improved the scrambling effect of Arnold algorithm. Secondly, after a lot of experiments, we propose a double-chaos system composed of Lorenz chaotic mapping with variable parameters and fourth-order Rossler hyperchaotic mapping to generate three sets of chaotic sequences for diffusion operation. The double-chaos system compensates the pseudo-randomness of the two types of chaotic mappings, making chaotic sequences more difficult to predict. Then, we transform the chaotic component images and chaotic sequences into DNA sequences in accordance with eight DNA coding rules, and the coding rules are determined by plaintext information or generated chaotic sequences. We also perform addition, subtraction, and XOR operations on them. DNA computation can realize color image bit-level diffusion and reduce the computational cost. The plaintext information is embedded in the encryption process to achieve “One-Time Pad”. Simulation experiments and detailed analysis are conducted with the proposed encryption scheme to prove that the algorithm has good security performance and can effectively resist all types of attacks, indicating that the proposed algorithm is competitive.

INDEX TERMS Color image encryption, bit level, DNA computing, double-chaos system.

I. INTRODUCTION
The rapid development of the Internet has ushered in a new era of global economy, culture, military, education, and other fields. In the new era, people can easily realize the transmission of image information. However, digital images may involve private or confidential information, which may cause incalculable consequences when leaked. The most common approach to protect the security of image information is image encryption.

Digital image encryption is the main method of image information security protection. Traditional encryption technologies, such as data encryption standard, advanced encryption standard, public key cryptography algorithm, and international data encryption algorithm, convert plaintext data into a binary stream for processing during encryption. These encryption schemes can safely and efficiently process text data. However, when they are applied to digital image encryption, their inherent characteristics of massive information, uneven energy distribution, strong correlation between adjacent pixels, and high data redundancy lead to low efficiency and security [1], [2].

The chaos system is complex, deterministic, and nonlinear. It has excellent characteristics, such as high sensitivity to initial values and parameters, autocorrelation of rapid decay, long-term unpredictability, and pseudo-randomness, which determine its natural relation with cryptography [1], [2]. Shannon, the founder of information theory, pointed out that the design of the encryption algorithm must satisfy the two basic principles of confusion and diffusion [3]. In 1998, J. Fridrich proposed an image encryption scheme based on a chaotic system. He applied the iterative value generated by the chaotic system to the scrambling of image pixels, thus marking the beginning of the study of chaotic image encryption [4]. Since then, many researchers of image encryption algorithms have developed algorithms with high security and practical application value.

Researchers have discovered problems in the application of chaotic systems to cryptography. For example, low-dimensional chaotic systems, such as logistic, tent, and
sine maps, the encryption and decryption speeds are high, but defects, including small key space and poor security, exist [5]–[7]. High-dimensional [8] and hyper chaotic systems can solve these problems [9]–[13]. However, due to the complex structure and high computational complexity of chaotic systems, the encryption and decryption efficiency is low. With the development of cryptanalysis, cryptographers have developed several encryption algorithms based on chaotic mapping [14]–[16]. Evidently, the adoption of new encryption technology to improve the encryption system mechanism is necessary. Current researchers are actively exploring the use of the interdisciplinary design of new image encryption schemes, such as S-box [17], quantum code [18], optical encryption [19], [20], DNA computing [1, 12s, 13, 20-36], and RNA code [37].

The principle of DNA computing involves using the DNA sequence as the information carrier and realizes image encryption via modern biotechnology. In information processing, the DNA molecule has the advantages of large information storage capacity, strong parallel computing capacity, and ultralow energy consumption. Many chaotic image encryption schemes based on DNA computation have been proposed [1], [12], [13], [20]–[36]. Several researchers designed image encryption schemes based on DNA sequence computation and 2D chaotic mapping [21], [22], [25], [27], [29], [36]. Dou et al. [21] proposed a robust encryption algorithm based on DNA and chaotic logistic mapping. The security of the encryption algorithm depends on the initial conditions of the 1D and 2D logistic chaotic maps, which include the sum of the front and rear pixels of the ordinary image. However, the scheme is unsecure because an attacker can determine the sum of the first half part and latter half part pixels. Wu et al. [22] proposed an image encryption scheme based on a new 2D chaotic mapping Henon sine map (2D-HSM) and DNA methods. The 2D-HSM was generated by combining Henon mapping with the sine map to extend the key scope. Awad and Miri [36] presented a novel chaos-based algorithm for image encryption via 2D piecewise linear chaotic mapping (PWLCM). However, the randomness of the sequences generated by the Henon mapping or PWLCM they used was not high enough, which might have affected the performance of the encryption scheme. Liu et al. [27] proposed a color image encryption algorithm based on DNA encoding combined with logistic chaotic mapping for color image characteristics. Liu et al. [29] combined DNA operation and PWLCM and proposed a novel confusion and diffusion method for image encryption. However, the scheme proposed by [27], [29] cannot resist known plaintext attacks. Many image encryption schemes based on DNA sequence computation and high-dimensional chaotic or hyperchaotic systems can overcome the defects of these low-dimensional chaotic systems. In addition, the schemes proposed by [13], [24] cannot combat ciphertext and plaintext attacks. Spatiotemporal chaotic systems combined with DNA encoding were developed in [1], [26], [28], [34], [35] to overcome this problem in chaos digitalization. For instance, Wu et al. [1] proposed a color image encryption scheme based on DNA sequence operations, one-time keys, and spatiotemporal chaos. The key streams are generated by the nonlinear chaotic algorithm map-based couple map lattices (CML), where the hash function SHA-256 is used to update the system parameters and initial conditions in combination with the plain image and secret keys. Experimental and analysis results showed that this scheme can resist various typical attacks and has good encryption efficiency. Hu et al. [26] proposed an image encryption scheme based on logistic-sine system (LSS)-based CML and DNA deletion and insertion pseudo operations. Wang et al. [28] developed an encryption algorithm for color images by using the extended Hamming distance and logistic map-based CML and DNA sequence operations to resist the selected plaintext attack. Zhen et al. [34] presented a new image encryption algorithm that uses information entropy, DNA coding, and logistic map-based CML. Zhang et al. [35] provided a new image encryption scheme based on DNA sequence operations and mixed linear-nonlinear CML (MLNCML). The experiment results proved that MLNCML has larger range of parameters and fewer periodic windows than CML.

Chaotic image encryption schemes based on DNA computation have been expanded in recent years. Huo et al. [20] proposed an optical image encryption scheme based on DNA theory and double random phase coding (DRPE) technology. Key images and random phase masks were generated via PWLCM to determine DNA coding rules. This scheme aims to realize the XOR operation of DNA by using the optical XOR gate to realize super-high-speed DNA encryption. Different types of plaintext use different initial values of PWLCM, which are generated by message digest algorithm 5. Plaintext passes through two rounds of DNA encryption then forms ciphertext through DRPE. The researcher verified the security and effectiveness of this method by attacking the encrypted image. Maddodi et al. [23] proposed a new pseudorandom sequence generator that combines a neural network with chaos and a chaotic encryption algorithm based on DNA rules for the secure transmission and storage of images. This scheme uses a new control encryption algorithm of the heterogeneous chaotic neural network generator and optimizes the performance of the generated chaotic sequences by dynamically updating the control parameters and number of iterations of the chaotic map. The experimental results showed that the chaos generator has high randomness and confirmed that the security and effectiveness of the genetic encryption method based on chaos. Mahmud et al. [37] used the concepts of RNA sequence and genetic algorithm (GA) and proposed a new symmetric image encryption method, namely, RNA-GA. The scheme first uses the logistic mapping function to generate a specified number of initial cipher images. Second, the codon truth table is utilized to convert the initial codon image into the corresponding 1D binary sequence and codon array. Third, the encryption key and encryption RNA tables are used to update the codon array to form the initial population of GA. Lastly, GA optimizes the population via
selection, crossover, and mutation operations. Experimental results show that this method has high resistance to known attacks.

In summary, due to the good effect of the image encryption scheme based on DNA computing, as well as the disadvantages of some schemes, for example, Ref. [22] can only encrypt grayscale images; the computational complexity of Ref. [35] is too high; there are also some encryption schemes mentioned earlier that use low-dimensional chaotic systems that are not secure enough. This paper presents a new color image encryption scheme based on DNA computing. The chaos encryption algorithm proposed in this paper for color images is also based on DNA computing, it combines a double-chaos system composed of Lorenz and Rossler chaotic mapping. The random sequences generated by the improved Lorenz chaotic system and fourth-order Rossler chaotic system greatly improve the randomness of chaotic sequences, and the double-chaos system compensates for the randomness of random sequences. Hence, the chaotic sequences become more difficult to predict. The eight DNA coding rules and three DNA operation rules used in the encryption scheme realize the color image bit-level diffusion operation, improve the security performance of the encryption scheme, enhance its anti-attack capability, and reduce the computation complexity compared with ordinary bit-level encryption algorithm. During encryption, we associate the key with the plaintext information to realize a “one-time pad.” The encryption scheme requires only one round of scrambling and diffusion encryption to achieve the desired encryption effect. The simulation results show that the proposed encryption algorithms have good security and practicality.

The remainder of this paper is organized as follows: Section 2 introduce the double-chaos system and the randomness of the generated chaotic sequence is tested. Section 3 briefly introduces the process of DNA computation and diffusion operation. Section 4 introduces the process of scrambling operation. Section 5 introduces the encryption and decryption process of the algorithm in detail. Section 6 carries out simulation experiments on the proposed encryption scheme, and a detailed analysis is performed on histogram, key space, key sensitivity, correlation, information entropy, resistance to differential attacks, robustness, and algorithm complexity to prove the good performance of our image encryption algorithm. Section 7 concludes the paper.

II. DOUBLE-CHAOS SYSTEM

For this encryption algorithm, we propose a double-chaos system. In this system, we use two types of typical 3D chaotic mapping, namely, Lorenz and Rossler chaotic mapping, which are widely used in image encryption systems. The improved Lorenz and Rossler chaotic mappings are utilized to form a double-chaos system that improves the randomness of generated chaotic sequences. Consequently, the chaotic sequences used for encryption become more difficult to predict.

A. IMPROVED LORENZ MAPPING

Lorenz chaotic mapping is a typical 3D chaotic system discovered by meteorologist E.N. Lorenz in his study of convection phenomena. Compared with low-dimensional chaotic mapping, Lorenz chaotic mapping has a more complex structure, the sequence is more random, and the key space is greatly increased. Lorenz chaotic mapping is defined as follows:

$$\begin{align*}
\dot{x} &= a(y - x) \\
\dot{y} &= cx - xz - y \\
\dot{z} &= xy - bz
\end{align*}$$

where \(x, y,\) and \(z\) are state variables and \(a, b,\) and \(c\) are system parameters. When \(a = 10, \ b = 8/3,\) and \(c = 28,\) the Lorenz chaotic system is in a chaotic state. Three chaotic sequences \((x, y,\) and \(z)\) can be generated using the Runge-Kutta method. Fig. 1 shows the attractor of classical Lorenz chaotic mapping and the phase diagram of each plane.

Although Lorenz chaotic systems are widely used and have produced good results in many algorithms, many decryption schemes for classical Lorenz chaotic maps should be studied due to the development of cryptography. To improve the security of the encryption system and the randomness of the sequence generated by the chaotic system, we use a Lorenz chaotic system with variable parameters in this chapter. The
improved Lorenz chaotic system is defined as follows:

\[
\begin{align*}
\dot{x} &= ax + pyz \\
\dot{y} &= (z - y)(b - c(cos(dt))) \\
\dot{z} &= -pxy - (e(cos(dt)) + f)y + (g - hz(cos(dt)))
\end{align*}
\] (2)

In this formula, we set \(a = 8/3, b = 25, c = 10, d = 5.3, e = 17.5, f = 10.5, g = 13.3,\) and \(h = 14,\) and \(t\) is the interval of this differential equation. When \(\cos(5.3t) \geq 0,\) take \(p = 1;\) otherwise, \(p = -1.\) Thus, the values of \(p\) and \(\cos(5.3t)\) vary with \(t.\)

The attractor and phase diagram of each plane of the improved Lorenz chaotic sequence are shown in Fig. 2. Comparative results indicate that the motion trajectory of the Lorenz chaotic system with a cosine function is complex, and the randomness of the generated \(x, y,\) and \(z\) is improved.

**B. ROSSLER HYPERCHAOTIC MAPPING**

A physical chemist in Germany developed an asymmetric attractor structure; by repeatedly performing experiments while studying attractors, he discovered a simple Rossler system that can generate chaos. Rossler chaotic mapping is defined as follows:

\[
\begin{align*}
\dot{x} &= -y - z \\
\dot{y} &= x + ay \\
\dot{z} &= b + xz - cz
\end{align*}
\] (3)

where \(a, b,\) and \(c\) are system parameters. We set \(a = 0.2, b = 0.4,\) and \(c = 5.7,\) similar to those in the previous section. We then obtain the attractor of classical Rossler chaotic mapping and the phase diagram of each plane (Fig. 3).

Fig. 3 shows that the \(x, y,\) and \(z\) sequence distributions generated by classical Rossler chaotic mapping have certain periodicity. Thus, we still use the improved Rossler chaotic system in this encryption algorithm to improve the performance of the chaotic system. The function definition of the improved fourth-order Rossler hyperchaotic system is shown in Formula (4).

\[
\begin{align*}
\dot{x} &= a(y - x) \\
\dot{y} &= -xz + dx + cyw \\
\dot{z} &= xy - bz \\
\dot{w} &= x + k
\end{align*}
\] (4)

where \(x, y, z,\) and \(w\) are state variables and \(a, b, c, d,\) and \(k\) are system parameters. We set \(a = 36, b = 3, c = 28, d = -16,\) and \(k = 0.5.\) Comparison shows that the trajectory of the improved fourth-order Rossler chaotic system is complex and disordered. Thus, the randomness of the three generated groups of chaotic sequences \((x, y,\) and \(z)\) is improved.

**C. GENERATION OF RANDOM SEQUENCES**

We introduce the generation of chaotic sequences for diffusion operations. We use the variable parameters of Lorenz chaotic mapping to produce three chaotic sequences \((x_1, x_2,\) and \(x_3),\)
and x_3) and fourth-order Rossler chaotic mapping to produce four chaotic sequences (y_1, y_2, y_3, and y_4). We combine the decimal places of chaotic sequences generated by the two chaotic maps. Then, after several experiments, we obtain three chaotic sequences, namely, z_1, z_2, and z_3, with good chaotic performance. After converting the chaotic sequences into DNA sequences, they are used to diffuse the red (R), green (G), and blue (B) components that have been scrambled. z_1, z_2, and z_3 are evaluated with Formula (5).

\[
\begin{align*}
 z_1 &= \text{mod}(x_1y_2 \times 10^3, 1) \\
 z_2 &= \text{mod}(\text{mod}(x_2y_2 \times 10^3, 1) + \text{mod}(x_3y_3 \times 10^3, 1), 1) \\
 z_2 &= \text{floor}(\text{mod}(z_2, 1) \times 256) \\
 z_3 &= \text{mod}(x_3 \times 10^3, 1) + \text{mod}(Y_3 \times 10^4, 1) \times 10^{-1} + \text{mod}(x_3 \times 10^5, 1) \times 10^{-2} + \text{mod}(Y_4 \times 10^6, 1) \times 10^{-3} \\
 z_3 &= \text{floor}(\text{mod}(z_3, 1) \times 256)
\end{align*}
\]

We select three calculation methods to obtain the z_1, z_2, and z_3 sequences. These methods effectively compensate for the randomness of chaotic sequences and make them difficult to predict.

**D. CHAOTIC SEQUENCE RANDOMNESS TEST**

We conduct frequent random tests on the generated chaotic sequences to ensure the randomness of the sequences and their safety performance. The test results of the random sequences are provided below.

1) **SEQUENCE DISTRIBUTION TEST**

A uniform distribution of the random sequences indicates that the sequences have good randomness and safety performance. However, if the distribution of random sequences is uneven and the occurrence frequency of different values is significantly different, then the randomness of the sequences is weak, the security performance is poor, and the sequences are vulnerable to statistical attacks.

Figs. 5(a)-5(c) show the distribution of random sequences \{z_1\}, \{z_2\}, and \{z_3\} generated by the proposed double-chaos system. Comparison with Figs. 2(e)-2(g) and Figs. 4(e)-4(g) shows that the distribution is more uniform. Therefore, the double-chaos system has more robust randomness and better security than the improved Lorenz and Rossler mappings.

2) **APPROXIMATE ENTROPY (APEN) ANALYSIS OF CHAOTIC SEQUENCES**

ApEn is a nonlinear dynamical parameter used to quantify the regularity and unpredictability of time series fluctuations. This parameter uses a non-negative number to represent the complexity of a time series, thus reflecting the possibility of new information occurring in the time series. A large ApEn series indicates a complex time.

By calculating the ApEn values of the chaotic sequences generated by different value methods, we select three groups of chaotic sequences that have passed the ApEn test and performed well in the National Institute of Science and Technology (NIST) test. All sequences exhibit good chaotic performance (Formula 5).

3) **NIST RANDOMNESS TEST**

Randomness testing of a sequence determines whether the test sequence is truly random or the difference between the test sequence and true randomness. Hypothesis testing is the basis of randomness testing techniques. The most common sequence randomness test is the NIST test. With regard to the chaotic sequence used for encryption, we select 2,000,000 bits for the NIST test. One set of results is used as an example, and the results are shown in Table 1.

In the NIST random test, \(p < 0.01\) means that the random sequence fails the test item, and the sequence is not random. Table 1 shows that the \(p\) values of the 15 test items are
TABLE 1. NIST test result of \( z_3 \).

| Test Index             | P-value  | Result |
|------------------------|----------|--------|
| Frequency              | 0.727840 | success|
| block-frequency        | 0.492885 | success|
| Cumulative Sums        | 0.467379 | success|
| Runs                   | 0.539295 | success|
| Longest Run of Ones    | 0.503831 | success|
| Rank                   | 0.719200 | success|
| FFT                    | 0.358795 | success|
| Non Periodic Template  | 0.234494 | success|
| Overlapping Template (m=9) template≈0000000001 | 0.157774 | success|
| Universal              | 0.607603 | success|
| Approximate Entropy    | 0.838764 | success|
| Random Excursions (x=−2) | 0.792377 | success|
| Random Excursions Variant (x=−9) | 0.949623 | success|
| Linear Complexity      | 0.640112 | success|
| Serial(m=16)           | 0.276930 | success|

greater than the significance level (0.01). The p values of nine items (frequency, runs, longest run of ones, rank, universal, approximate entropy, random excursions, random excursions, and linear complexity) are more than 0.5. These results show that the key stream sequence generated by the double-chaos system is random, and the security of the algorithm is guaranteed. Similarly, the p value of all test items of \( z_1 \) and \( z_2 \) is greater than 0.01, and the p value of eight items exceeds 0.5. The results of several test items, such as non-periodic template, random excursions, and random excursions, have multiple p values. Thus, we randomly select only a p value with the same values of x and “template” for comparison. The p values of certain cases are more ideal than those of others.

III. DNA COMPUTING

We briefly introduce DNA computing methods (mainly DNA coding and DNA operation) and image encryption schemes based on DNA computing.

A. DNA ENCRYPTION ALGORITHM

DNA is a crucial genetic material in the process of human evolution. DNA is made up of bases, phosphoric acid, and penta-deoxyribose. The four bases of DNA are adenine (A), guanine (G), thymine (T), and cytosine (C). According to the principle of base complementary pairing in biology, A is paired with T and C with G. The DNA operation has been applied to many cross-disciplines, such as chaotic image encryption, due to the advantages of the DNA sequence, such as high parallelization, massive storage capacity, far lower energy consumption than ordinary computers, abundant and cheap resources, and strong economy.

The core idea of DNA encryption is to use the base as the carrier of the plaintext information and realize information encryption with the aid of DNA molecular manipulation technology. Encryption methods based on DNA include DNA probe, one-time pad, those based on DNA computing model, DNA-hidden approaches, and those based on pseudo DNA computing. The first four methods can only realize text information encryption. Most image encryption schemes based on DNA computing adopt pseudo DNA computing to realize encryption of image information. This method is also used in this study to achieve image encryption.

In a computer, information is represented by binary numbers 0 and 1. The four kinds of binary numbers with two bits are 00, 01, 10, and 11, where 0 and 1, 01 and 10, and 00 and 11 are complementary. A DNA molecule has exactly four bases. If these bases are matched one by one, then 2^4 coding schemes can be obtained according to the calculation method of arrangement and combination in mathematics. However, because A-T and C-G are complementary pairs, only eight valid DNA encoding rules are available, as shown in Table 2. Each pixel value of a digital image is an integer between 0 and 255, which can be represented by a binary sequence of 8 bits. In accordance with DNA coding rules, each pixel value of the image can be converted into a DNA molecular sequence of 4 bits. Moreover, for the same binary sequence, different DNA sequences can be obtained with different coding rules. Different encoding and decoding rules are used to obtain different binary sequences.

In the encryption scheme, the plaintext image and chaotic sequence used for encryption are generally converted into DNA molecular sequences in accordance with DNA coding rules. Then, the two sets of DNA sequences perform the DNA operation to achieve the diffusion operation. The encrypted DNA sequence is decoded and restored to the pixel level to obtain the final ciphertext image using the DNA coding rules. In the proposed encryption scheme, the encoding rules are determined by the average pixel value of each component image and the average value of each chaotic sequence. Thus, the operation of this step is related to the plaintext information.

B. DNA SEQUENCE OPERATION

DNA sequence operations mainly include addition, subtraction, and XOR operations. Tables 3 to 5 show that the bases of any row or column are unique. Thus, the uniqueness of the...
bases after operation is guaranteed. To improve the security of the encryption algorithm, we use different DNA operation rules to encrypt the three components of the color image.

### IV. IMAGE SHUFFLING

We cannot encrypt color images directly. Therefore, we need to standardize the size of the experimental images and separate the gray images of R, G, and B components of the color images. For example, in Fig. 6, we reset the color Lena image to a color image of $128 \times 128$; b, c, and d are gray images of the R, G, and B components of a, respectively.

To improve the security of the algorithm in terms of resistance to anti-noise attack and the ability to reduce attacks, we use Formula (6) to perform the Arnold shuffling operation on the R, G, and B components of the color image to scramble the position of the image pixels.

\[
\left( \begin{array}{c} p \\ q \end{array} \right) = \left( \begin{array}{c} i \\ j \end{array} \right) \left( \begin{array}{c} 1 \\ ab + 1 \end{array} \right) \mod N_a
\]

where $a$, $b$, and $N_a$ are parameters and $a_{ij}$ is the pixel value at row $i$ and column $j$ of plain image. After shuffling, this pixel will be moved to the position of row $p$, column $q$. The position of each pixel of the original image can be well distributed by using the one-to-one correspondence of the function. We set $a = 3$ and $b = 5$.

The advantage of Arnold scrambling is that every iteration is global scrambling, and iteration times $n$ of global scrambling is $n-1$ times. Arnold scrambling can hide the image information effectively, and the number of iterations as a part of the key increases the security of the encryption system.

In this study, the number of iterations of each component image is determined by its pixel average value. The three components after reset are shown in Fig. 7. Although evident differences exist among the three components of the scrambled images a, b, and c and the original image information cannot be seen, a certain correlation still exists between pixels.

### V. COLOR IMAGE ENCRYPTION AND DECRYPTION ALGORITHM BASED ON DNA COMPUTATION AND DOUBLE-CHAOS SYSTEM

In this section, we describe in detail the encryption and decryption steps of the proposed color image encryption algorithm based on DNA computation and double-chaos systems.

#### A. ENCRYPTION ALGORITHM

The complete encryption algorithm can be described by the following steps:

---

**TABLE 3. DNA addition.**

| A | T | A | C | G |
|---|---|---|---|---|
| C | A | C | G | T |
| G | C | G | T | A |
| T | G | T | A | C |

**TABLE 4. DNA subtraction.**

| A | C | G | T | A |
|---|---|---|---|---|
| C | A | C | G | T |
| G | T | A | C | G |
| T | G | T | A | C |

**TABLE 5. DNA XOR.**

| A | C | G | T |
|---|---|---|---|
| A | G | T | A |
| C | T | G | C |
| G | A | C | G |
| T | C | A | T |

---

**FIGURE 6.** Lena image of $128 \times 128$: (a) color image; (b) red component; (c) green component; (d) blue component.

**FIGURE 7.** The scrambled image: (a) R; (b) G; (c) B.
Step 1: Color plaintext image P is read. The size of color image P is reset to 256 × 256, and gray images PR, PG, and PB of the R, G, and B components of the color image are separated. The size of the three grayscale component images is 256 × 256.

Step 2: The Arnold algorithm is used to scramble the pixel positions of the three grayscale component images, and the iteration times are set as n1 = mean (PR), n2 = mean (PG), and \( n_3 = \text{mean (PB)} \).

Step 3: The parameters of Lorenz mapping are set as follows: \( x_0 = [x_{01}, x_{02}, x_{03}] \), p. The parameters of Rossler mapping are set as follows: \( Y_0 = [Y_{01}, Y_{02}, Y_{03}, Y_{04}] \), a, b, c, d, k. The three sets of parameters related to plaintext information are \( n_1 = \text{mean (PR)} \), \( n_2 = \text{mean (PG)} \), and \( n_3 = \text{mean (PB)} \).

Step 4: Three sets of chaotic sequences, namely, \( \{x_1(i)\} \), \( \{x_2(i)\} \), and \( \{x_3(i)\} \), are generated by the Lorenz chaotic system with variable parameters. Four sets of chaotic sequences, namely, \( \{Y_1(i)\} \), \( \{Y_2(i)\} \), \( \{Y_3(i)\} \), and \( \{Y_4(i)\} \), are generated by the fourth-order Rossler chaotic system.

Step 5: Three sets of random chaotic sequences, namely, \( \{z_1(i)\} \), \( \{z_2(i)\} \), and \( \{z_3(i)\} \), for diffusion operations are obtained using Formula (5).

Step 6: The scrambled images obtained in Step 2 and the three sets of random chaotic sequences obtained in Step 5 are converted into DNA sequences in accordance with the eight DNA coding rules. The encoding rules used are determined by key1, key2, and key3, where key1 = mod (n1, 8), key2 = mod (n2, 8), and key3 = mod (n3, 8). Three sets of DNA sequences \( \{C_1\} \), \( \{C_2\} \), and \( \{C_3\} \) are generated by the scrambled images, and three sets of DNA chaotic sequences \( \{Z_1(i)\} \), \( \{Z_2(i)\} \), and \( \{Z_3(i)\} \) are produced by chaotic sequences.

Step 7: DNA sequence \( \{D_1\} \) is obtained using the DNA addition operation for \( \{Z_1(i)\} \) and \( \{C_1\} \), DNA sequence \( \{D_2\} \) is obtained using the DNA subtraction operation for \( \{Z_2(i)\} \) and \( \{C_2\} \), and DNA sequence \( \{D_3\} \) is obtained using the DNA XOR operation for \( \{Z_3(i)\} \) and \( \{C_3\} \) to implement the diffusion operation.

Step 8: \( \{D_1\} \), \( \{D_1\} \), and \( \{D_3\} \) are restored to pixel values and merged into the final ciphertext image C.

Step 9: The encrypted ciphertext image C is saved.

In this encryption algorithm, because the chaotic sequences \( \{Z_1(i)\} \), \( \{Z_2(i)\} \), and \( \{Z_3(i)\} \) used for diffusion operations are pseudorandom, the encryption algorithm has good security performance and can effectively resist the selected plaintext attack. In addition, due to the use of the DNA operation, our diffusion operation is performed at the bit level, and the data volume is half of the ordinary bit calculation algorithm. This approach not only improves the security of the encryption algorithm, but also reduces the computation complexity. Fig. 8 shows the flow diagram of this encryption scheme.

**B. DECRYPTION ALGORITHM**

The decryption algorithm of image C is the inverse process of the encryption algorithm and uses the same security key as the encryption algorithm. The following algorithm is the decryption process:

Step 1: Ciphertext image C is read. The size of ciphertext image C is 256 × 256. The grayscale images CR, CG, and CB of the R, G, and B components of the color ciphertext image are separated, and the size of the three grayscale images is 256 × 256.

Step 2: The parameters of Lorenz mapping are set as follows: \( x_0 = [x_{01}, x_{02}, x_{03}] \), p. The parameters of Rossler mapping are set as follows: \( Y_0 = [Y_{01}, Y_{02}, Y_{03}, Y_{04}] \), a, b, c, d, k. The three sets of parameters related to plaintext information are \( n_1 = \text{mean (PR)} \), \( n_2 = \text{mean (PG)} \), and \( n_3 = \text{mean (PB)} \).

Step 3: Three sets of chaotic sequences \( \{x_1(i)\} \), \( \{x_2(i)\} \), and \( \{x_3(i)\} \) are generated by the Lorenz chaotic system with variable parameters. Four sets of chaotic sequences \( \{Y_1(i)\} \), \( \{Y_2(i)\} \), \( \{Y_3(i)\} \), and \( \{Y_4(i)\} \) are generated by the fourth-order Rossler chaotic system.

Step 4: Three sets of random chaotic sequences \( \{z_1(i)\} \), \( \{z_2(i)\} \), and \( \{z_3(i)\} \) for diffusion operations are obtained using Formula (5).

Step 5: The images CR, CG, and CB obtained in Step 1 and the three sets of random chaotic sequences obtained in Step 4 are converted into DNA sequences in accordance with the eight DNA coding rules. The encoding rules used are determined by key1, key2, and key3. The three sets of DNA sequences \( \{D_1\} \), \( \{D_2\} \), and \( \{D_3\} \) generated by CR, CG, and CB and the three sets of DNA chaotic sequences \( \{Z_1(i)\} \), \( \{Z_2(i)\} \), and \( \{Z_3(i)\} \) produced by chaotic sequences are obtained.

Step 6: DNA sequence \( \{C_1\} \) is obtained using \( \{Z_1(i)\} \) to recover \( \{D_1\} \) according to DNA addition. DNA sequence \( \{C_2\} \) is obtained using \( \{Z_2(i)\} \) to recover \( \{D_2\} \) according to DNA subtraction. DNA sequence \( \{C_3\} \) is obtained using \( \{Z_3(i)\} \) to recover \( \{D_3\} \) according to the DNA XOR operation.

Step 7: \( \{C_1\} \), \( \{C_2\} \), and \( \{C_3\} \) are decoded and restored to the pixel values in the interval of [0, 255] and reconstructed into images.

Step 8: The scrambled image is restored using the reversal function of Arnold scrambling, and PR, PG, and PB are obtained.

Step 9: PR, PG, and PB are merged to obtain the final decrypted image P’.
b = 3, c = 28, d = −16, and k = 0.5. In Fig. 9, a, b, c, and d are the original plaintext image, the encrypted ciphertext image, the incorrectly decrypted image, and the correctly decrypted image, respectively. In Fig. 9(b), the encrypted ciphertext image is not clear, and the plaintext image information cannot be recognized by the naked eye. In Fig. 9(c), we change only the initial value of the third bit of $Y_0$. When the decryption key used is not correct, the image cannot be restored effectively, and the plaintext image information cannot be recognized by the naked eye. In Fig. 9(d), we decrypt Fig. b with the correct key, thereby effectively restoring the plaintext image.

B. HISTOGRAM ANALYSIS

A favorable encryption algorithm must have a smooth histogram of the encrypted image. Fig. 10 shows the color histogram before (a) and after (b) encryption. The encrypted color image histogram is evenly distributed compared with the plaintext image, and the distribution probability in the interval is approximately equal. Thus, using statistical analysis to predict the original image is difficult for attackers. The results show that the algorithm can effectively prevent statistical attacks.

C. KEY SPACE

An ideal image encryption algorithm must have a sufficiently large key space and be sensitive to its key. The size of the key space is the total number of different keys that can be used in the cryptographic system; thus, the key space must be greater than $2^{128}$ to enhance the capability of this algorithm to resist violent attacks.

In the proposed scheme, the key mainly consists of the initial value $x_0 = [x_{01}, x_{02}, x_{03}]$ and the parameter $p$ of Lorenz.
mapping, the initial value $Y_0 = [Y_{01}, Y_{02}, Y_{03}, Y_{04}]$ and three sets of parameters $n_1 = \text{mean (PR)}, n_2 = \text{mean (PG)},$ and $n_3 = \text{mean (PB)}$ related to plaintext information. Therefore, in accordance with the IEEE floating point standard, the overall key space of this algorithm is

$$\text{Keyspace} = 10^{15 \times 16} \gg 2^{128}$$

This equation satisfies the security requirements that are outlined in the standard. Therefore, our encryption algorithm has a sufficiently large key space to resist various brute-force attacks.

D. CORRELATION ANALYSIS

Generally, a strong correlation exists between adjacent pixels in a plaintext image, and eliminating the correlation between adjacent pixels is the key to measuring the performance of an encryption algorithm. We select 20,000 pairs of adjacent pixels from the three components of the plaintext and ciphertext images, including the vertical, horizontal, and diagonal directions. The distribution of pixel pairs is shown in Fig. 11.

In Fig. 11, a(1)-a(3) show the original image in the horizontal direction of pixels for distribution, c(1)-c(3) show the original image pixels of the vertical direction of distribution, and e(1)-e(3) show the original image pixels in the diagonal direction for distribution. Most figures point near the diagonal direction, indicating the level of the original image and that the vertical and diagonal directions of the adjacent pixel values are close. In Fig. 11, b(1)-b(3) represent the ciphertext horizontal pixel in the image on the distribution of d(1)-d(3), which represent the cipher image pixels of the vertical direction of distribution; f(1)-f(3) represent the cipher text in the image pixel in the diagonal direction for distribution. In these figures, the cipher image points are randomly distributed in space, but the cipher images in the three directions of the adjacent pixels are distant.

In addition, we use the following formula to evaluate the correlation.

$$\text{Corr} = \frac{N \times \sum_{i=1}^{N} (x_i \times y_i) - \sum_{i=1}^{N} x_i \times \sum_{j=1}^{N} y_j}{\sqrt{(N \sum_{i=1}^{N} x_i^2 - (\sum_{i=1}^{N} x_i)^2) \times (N \sum_{i=1}^{N} y_i^2 - (\sum_{i=1}^{N} y_i)^2)}}$$

(7)

where $x_i$ and $y_i$ are two data sequences and $N$ is the sequence length. If the Corr value is approximately 1, then the two sequences are considered strongly correlated. If the Corr value is close to 0, then the correlation is very weak and the encryption is effective. Table 6 shows that the Corr values of the proposed algorithm in the horizontal, vertical, and diagonal directions are negative and better than those of other algorithms. Therefore, our encryption algorithm can effectively break the correlation between adjacent pixels of ordinary images, and the encryption effect is favorable.
TABLE 6. Correlation analysis.

| Direction | Plain image | Algorithm | Proposed Algorithm | Ref. [1] | Ref. [8] | Ref. [9] | Ref. [10] | Ref. [11] | Ref. [27] | Ref. [40] |
|-----------|-------------|-----------|-------------------|--------|--------|--------|--------|--------|--------|--------|
|           | Horizontal  | Vertical  | Diagonal          |        |        |        |        |        |        |        |
|           | 0.9806      | 0.9601    | 0.9383            |        |        |        |        |        |        |        |
| Algorithm | -0.0119     | -0.0087   | -0.0045           |        |        |        |        |        |        |        |
| Proposed Algorithm | -0.0082 | -0.0128 | -0.0012 |        |        |        |        |        |        |        |
| Ref. [9]  | 0.0265      | 0.0044    | 0.0625            |        |        |        |        |        |        |        |
| Ref. [25] | 0.0072      | 0.0058    | 0.0031            |        |        |        |        |        |        |        |
| Ref. [26] | -0.0077     | 0.0002    | 0.0055            |        |        |        |        |        |        |        |
| Ref. [34] | 0.0214      | 0.0465    | -0.0090           |        |        |        |        |        |        |        |
| Ref. [35] | 0.000002971 | -0.000001339 | -0.000003790 |        |        |        |        |        |        |        |

E. INFORMATION ENTROPY ANALYSIS

Entropy is a physical quantity in thermodynamics that indicates the degree of unnecessariness of a physical system. For a digital image, information entropy can show the distribution of each gray value. The following calculation formula is used for information entropy.

\[
H(m) = - \sum_{i=1}^{M} p(m_i) \log_2 p(m_i)
\]  

(8)

If the distribution of gray values is uniform, then the information entropy of the image is large. In general, the gray value distribution of an image is uneven, and the statistical characteristics are obvious. Therefore, the information entropy is small. A large entropy of the encrypted image information indicates that the gray value distribution of the image is uniform. Thus, obtaining image information by analyzing this information is difficult for attackers.

We analyze and calculate the information entropy of the images before and after encryption by using Formula 8. We find that the information entropy of the plaintext image is 7.9232. After encryption by the algorithm, the information entropy of the image is 7.9913, which is closer to the maximum value of 8 than the plaintext information. Table 7 shows the comparison of the information entropy of each image component before and after encryption between the proposed algorithm and other encryption algorithms. Table 7 shows that the information entropy of the three components of the encrypted image obtained by our algorithm is closer to the ideal value of 8 than that of [1], [10], [11], [27]. Therefore, from the perspective of information entropy attack, this algorithm is safe.

F. KEY SENSITIVITY ANALYSIS

A favorable encryption algorithm must have favorable sensitivity to its key. Sensitivity is divided into the following points:

1. The slight change in the key value during the encryption process causes a significant change in the encrypted image.

2. The slight change in the key value during the decryption process results in a significant difference in the decrypted image.

In test (1), we test \(x_0\) and \(Y_{03}\), one of the three initial values of Lorenz chaotic mapping and one of the four initial values of Rossler chaotic mapping in the original key. Since many references of the same type make a small change of \(10^{-15}\) to the parameter, we also make a change of \(10^{-15}\) to the parameter here. When the other parameters are exactly the same, the test results after \(x_0\) or \(Y_{03}\) changes by \(10^{-15}\) are as shown in Fig. 12, where a is the original plaintext image, b is the ciphertext image when \(x_0 = 0.5201\), \(Y_{02} = 26.8729\), c is the ciphertext image when \(x_0 = 0.5201000000001\), \(Y_{03} = 26.8729\), and d is the image difference value of b−c, e is the ciphertext image when \(x_0 = 0.5201\), \(Y_{03} = 26.8729000000001\), and f is the image difference value of b−e. A significant difference exists between b and c, b and e. The results show that the improved algorithm has good key sensitivity.

Test (2) is still performed on the same picture and same parameters. When the other parameters are unchanged and the decryption key differs from the encryption key by only \(10^{-15}\), the test results are as shown in Fig. 13. In this figure, a is the original plaintext image, b is the ciphertext image when the parameters are exactly the same with test (1), c is the decrypted image when \(x_0 = 0.5201\), d is the decrypted image when the other parameters are constant, \(x_0 = 0.5201000000001\), e is the decrypted image when \(Y_{03} = 26.8729\), and f is the decrypted image when the other parameters are constant, \(Y_{03} = 26.8729000000001\). Even when the decryption key is only slightly different from the encryption key, a remarkable difference still exists between the resulting image and the correctly decrypted image. The correctly decrypted image c successfully restores the original image, but the incorrectly decrypted image d cannot recognize any information in the original image. These results show that the improved algorithm has good key sensitivity.

G. DIFFERENTIAL ATTACK ANALYSIS

Pixel change rate (NPCR) and normalized mean change intensity (UACI) are detection factors against differential
attacks. They are important indicators of image information. NPCR represents the percentage of the number of pixels in the encrypted image that changes after randomly changing the pixel value of a pixel in the original image. UACI represents the intensity of the change in the pixel value of the encrypted image after the pixel value of the original image is randomly changed. If the pixel change of the original plaintext image is small and the encrypted image changes greatly, then the encryption algorithm can effectively resist differential attacks and the security performance of the encryption algorithm is good. The formula is as follows:

\[
NPCR = \frac{\sum_{i,j} D(i,j)}{L} \times 100\% \tag{9}
\]

\[
UACI = \frac{1}{L} \left[ \sum_{i,j} \left| \frac{C_1(i,j) - C_2(i,j)}{H} \right| \right] \times 100\% \tag{10}
\]

Using Formulas 8 and 9, we calculate the NPCR and UACI of the proposed algorithm and compare the results with those of other algorithms of the same type. The results are shown in Table 8. The NPCR and UACI analyses of the data in Table 8 and comparative results with other algorithms indicate that the experimental results are similar. Therefore, our improved encryption algorithm has good resistance to differential attacks, and the security performance of the encryption algorithm is favorable.

H. ROBUSTNESS ANALYSIS

In image transmission, the data or information in the image may be lost or changed due to transmission. Therefore, a good encryption algorithm should have a certain resistance ability to prevent data change or loss caused by attacks. First, we add salt-and-pepper noise to the encrypted image to verify the
TABLE 8. NPCR and UACI analysis.

| Algorithm     | NPCR (%) | UACI (%) |
|---------------|----------|----------|
|               | Red      | Green    | Blue     | Red      | Green    | Blue     |
| Proposed      | 99.63    | 99.60    | 99.61    | 33.42    | 31.07    | 32.10    |

TABLE 9. Computational complexity analysis.

| Algorithm     | Computational Complexity |
|---------------|--------------------------|
| Proposed      | $O(12 \times M \times N)$ |
| Ref. [22]     | $O(M \times N)$          |
| Ref. [28]     | $O(12 \times M \times N)$|
| Ref. [35]     | $O(L \times M \times N) \times L = 100$ |

4 DNA basic nucleic acid bases, so the time complexity is $O(12 \times M \times N)$. From the above analysis, the computation complexity of this algorithm is $O(12 \times M \times N)$. The following Table 9 is a comparison of our proposed algorithm with other algorithm. As can be seen from Table 9, compared with the robustness of the encryption algorithm when data changed. In Fig. 14, a adds 0.0125% salt-and-pepper noise, b decrypts the image, c adds 0.5% salt-and-pepper noise, and d decrypts the image. The comparative results show that the algorithm has a certain ability to resist the attack of salt-and-pepper noise. Although the decrypted image with added noise cannot be restored to the original image, we can still see the general information of the plaintext image. Then, we delete part of the data of the encrypted image to verify the robustness of the encryption algorithm when data loss. In Fig. 14, e is the encrypted image with 1.6% data loss, f decrypts the image, g is the encrypted image with 3.8% data loss, and h decrypts the image. The comparative results show that the algorithm also has a certain ability to resist the attack when data loss.

I. COMPUTATIONAL COMPLEXITY

This part, we analyze the computational complexity of the algorithm. The size of plain image is denoted as $M \times N$. The computational complexity of the proposed algorithm is mainly divided into three parts. The first part is the key streams generation. This part generates three key streams $z_1$, $z_2$, $z_3$ whose lengths are all $M \times N$, and the complexity of the generation algorithm is $O(3 \times M \times N)$. The second part is the shuffling operation. Since this step is performed at the pixel level of the three components of the color image, the time complexity is $O(3 \times M \times N)$. The third part is diffusion. While DNA encode and decode step need to modify the pixel matrix into the DNA matrix, each pixel can be represented...
algorithm of the same type, the computational complexity of our algorithm is more complex than that of Ref. [22], which is the same as that of Ref. [28] and better than that of Ref. [35]. However, Ref. [22] is analyzed based on the encryption algorithm for grayscale images. Therefore, the time complexity of our algorithm is competitive with other algorithms of the same type.

VII. CONCLUSION

This paper proposed an algorithm for color image encryption based on a double-chaos system and DNA computation at the bit level. For this algorithm, to ensure component extraction in advance, we used the Arnold algorithm to scramble the three color components of the plaintext image, and the number of iterations was determined by the pixel average of each component, which improved the scrambling effect of Arnold algorithm. Then, using the improved double-chaos system composed of Lorenz chaotic mapping with variable parameters and fourth-order Rossler hyperchaotic mapping, three sets of chaotic sequences were generated for the diffusion operation of three sets of scrambled components. In addition, the pseudo-randomness of the two sets of chaotic sequences was compensated by the double-chaos system. Then, we used DNA coding and DNA computing to diffuse the three groups of images and finally merged the three groups of ciphertext components to obtain the final ciphertext image. We proposed an encryption scheme for the simulation experiment. The histogram, key space, key sensitivity, relevance, information entropy, resistance to differential attacks, robustness, and computation complexity were analyzed in detail. The experimental results show that the algorithm has good safety performance and can effectively resist various attacks. Our algorithm is competitive with other chaotic image encryption algorithms. However, the algorithm still has some shortcomings, such as the low computational speed of the DNA-based image encryption scheme, which might affect the practical application of the algorithm, and needs to be improved, which is also the focus of our future work.

REFERENCES

[1] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, “Color image DNA encryption using NCA map-based CML and one-time keys,” Signal Process., vol. 148, pp. 272–287, Jul. 2018.
[2] C. Y. Song, Y. L. Qiao, and X. Z. Zhang, “An image encryption scheme based on new spatiotemporal chaos,” Optik, vol. 124, no. 18, pp. 3329–3334, Sep. 2013.
[3] C. E. Shannon, “Communication theory of secrecy Systems*,” Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.
[4] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” Int. J. Bifurcation Chaos, vol. 08, no. 06, pp. 1259–1284, Jun. 1998.
[5] N. K. Pareek, V. Patidar, and K. K. Sud, “Image encryption using chaotic logistic map,” Image Vis. Comput., vol. 24, no. 9, pp. 926–934, Sep. 2006.
[6] G. Ye and K.-W. Wong, “An efficient chaotic image encryption algorithm based on a generalized arnold map,” Nonlinear Dyn., vol. 69, no. 4, pp. 2079–2087, Sep. 2012.
[7] Y. Zhou, L. Bao, and C. L. P. Chen, “A new 1D chaotic system for image encryption,” Signal Process., vol. 97, pp. 172–182, Apr. 2014.
[8] M. Mollaeefar, A. Sharif, and M. Nazari, “A novel encryption scheme for colored image based on high level chaotic maps,” Multimedia Tools Appl., vol. 76, no. 1, pp. 607–629, Jan. 2017.
[9] A. Yaghouti Niyat, M. H. Moattar, and M. N. Torshiz, “Color image encryption based on hybrid hyper-chaotic system and cellular automata,” Opt. Lasers Eng., vol. 90, pp. 225–237, Mar. 2017.
[10] H. Liu, X. Wang, and A. Kadir, “Color image encryption using Choquet fuzzy integral and hyper-chaotic system,” Optik, vol. 124, no. 18, pp. 3527–3533, Sep. 2013.
[11] A. Kadir, A. Hamdulla, and W.-Q. Guo, “Color image encryption using skew tent map and hyper-chaotic system of 6th-order CNN,” Optik, vol. 125, no. 5, pp. 1671–1675, Mar. 2014.
[12] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, “A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system,” J. Syst. Softw., vol. 85, no. 2, pp. 290–299, Feb. 2012.
[13] Q. Zhang, L. Guo, and X. Wei, “A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system,” Optik Int. J. Light Electron Opt., vol. 124, no. 18, pp. 3596–3600, Sep. 2013.
[14] C. Li, S. Li, G. Chen, and W. A. Halang, “Cryptography of an image encryption scheme based on a compound chaotic sequence,” Image Vis. Comput., vol. 27, no. 8, pp. 1035–1039, Jul. 2009.
[15] E. Solak, R. Rhouma, and S. Belghith, “Cryptography of a multi-chaotic systems based image cryptosystem,” Opt. Commun., vol. 283, no. 2, pp. 232–236, Jan. 2010.
[16] Y. Zhang and D. Xiao, “Cryptography of S-box-only chaotic image ciphers against chosen plaintext attack,” Nonlinear Dyn., vol. 72, no. 4, pp. 751–756, Jun. 2013.
[17] U. Çavuşoğlu, S. Karac, I. Pehlivan, and A. Zengin, “Secure image encryption algorithm design using a novel chaos based S-Box,” Chaos, Solitons Fractals, vol. 95, pp. 92–101, Feb. 2017.
[18] A. A. A. El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, “A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces,” Signal Process., vol. 93, no. 11, pp. 2986–3000, Nov. 2013.
[19] J. Liu, H. Jin, L. Ma, Y. Li, and W. Jin, “Optical color image encryption based on computer generated hologram and chaotic theory,” Opt. Commun., vol. 307, pp. 76–79, Oct. 2013.
[20] D. Huo, D.-F. Zhou, S. Yuan, S. Yi, L. Zhang, and X. Zhou, “Image encryption using exclusive OR with DNA complementary rules and double random phase encoding,” Phys. Lett. A., vol. 383, no. 9, pp. 915–922, Feb. 2019.
[21] Y. Dou, X. Liu, H. Fan, and M. Li, “Cryptography of a DNA and chaos based image encryption algorithm,” Optik, vol. 145, pp. 456–464, Sep. 2017.
[22] J. Wu, X. Liao, and B. Yang, “Image encryption using 2D Hénon sine map and DNA approach,” Signal Process., vol. 153, pp. 11–23, Dec. 2018.
[23] G. Maddodi, A. Awad, D. Awad, M. Awad, and B. Lee, “A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding,” Multimedia Tools Appl., vol. 77, no. 19, pp. 24701–24725, Oct. 2018.
[24] Q. Zhang and X. Wei, “A novel couple images encryption algorithm based on DNA sequence operation and chaotic system,” Optik, vol. 124, no. 18, pp. 6276–6281, Dec. 2013.
[25] R. Enayatifar, A. H. Abdullah, and I. F. Isin, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence,” Opt. Lasers Eng., vol. 56, pp. 83–93, May 2014.
[26] T. Hu, Y. Liu, L.-H. Gong, S.-F. Guo, and H.-M. Yuan, “Chaotic image cryptosystem using DNA deletion and DNA insertion,” Signal Process., vol. 134, pp. 234–243, May 2017.
[27] L. Liu, Q. Zhang, and X. Wei, “A RGB image encryption algorithm based on DNA encoding and chaos map,” Comput. Electr. Eng., vol. 38, no. 5, pp. 1240–1248, Sep. 2012.
[28] X.-Y. Wang, H.-L. Zhang, and X.-M. Bao, “Color image encryption scheme using CML and DNA sequence operations,” Biosystems, vol. 144, pp. 18–26, Jun. 2016.
[29] H. Liu, X. Wang, and A. Kadir, “Image encryption using DNA complementary rule and chaotic maps,” Appl. Soft Comput., vol. 12, no. 5, pp. 1457–1466, May 2012.
Q. Liu, L. Liu: Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System

[30] A. R. Rehman, X. Liao, M. A. Hahsmi, and R. Haider, “An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos,” Optik Int. J. Light Electron Opt., vol. 153, pp. 117–134, Jan. 2018.

[31] J. Chen, Z.-L. Zhu, L.-B. Zhang, Y. Zhang, and B.-Q. Yang, “Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption,” Signal Process., vol. 142, pp. 340–353, Jan. 2018.

[32] Y. Zhang, D. Xiao, W. Wen, and K.-W. Wong, “On the security of symmetric ciphers based on DNA coding,” Inf. Sci., vol. 289, pp. 254–261, Dec. 2014.

[33] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, “A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2,” Nonlinear Dyn., vol. 83, no. 3, pp. 1123–1136, Feb. 2016.

[34] P. Zhen, G. Zhao, L. Min, and X. Jin, “Chaos-based image encryption scheme combining DNA coding and entropy,” Multimedia Tools Appl., vol. 75, no. 11, pp. 6303–6319, Jun. 2016.

[35] Y.-Q. Zhang, X.-Y. Wang, J. Liu, and Z.-L. Chi, “An image encryption scheme based on the MLNCML system using DNA sequences,” Opt. Lasers Eng., vol. 82, pp. 95–103, Jul. 2016.

[36] A. Awad and A. Miri, “A new image encryption algorithm based on a chaotic DNA substitution method,” in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2012, pp. 1011–1015, doi: 10.1109/icc.2012.6363965.

[37] M. Mahmud, A. R. Rahman, M. Lee, and J.-Y. Choi, “Evolutionary-based image encryption using RNA codons truth table,” Opt. Laser Technol., vol. 121, Jan. 2020, Art. no. 105818.

[38] Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, “A chaos-based symmetric image encryption scheme using a bit-level permutation,” Inf. Sci., vol. 181, no. 6, pp. 1171–1186, Mar. 2011.

[39] Y.-Q. Zhang and X.-Y. Wang, “A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice,” Inf. Sci., vol. 273, pp. 329–351, Jul. 2014.

[40] G. Ye and X. Huang, “An efficient symmetric image encryption algorithm based on an intertwining logistic map,” Neurocomputing, vol. 251, pp. 45–53, Aug. 2017.

QIAN LIU was born in Jiangxi, China, in January 1996. She received the bachelor’s degree in information security from Nanchang University, Nanchang, China, where she is currently pursuing the master’s degree in software engineering.

From 2017 to 2020, she worked at the laboratory of her mentor, Prof. L. Liu. Her research interests include the area of chaos, image encryption, and secure communications. She has won the School Principal Scholarship, the School Class Scholarship, the School Excellence Scholarships, and the School National Scholarship.

LINGFENG LIU was born in Nanchang, China, in 1986. He received the B.S. degree in mathematics, the M.Sc. degree in information science, and the Ph.D. degree in information science from the Huazhong University of Science and Technology, China, in 2007, 2009, and 2014, respectively.

He is currently working with the School of Software, Nanchang University, China. He is funded by the National Natural Science Foundation of China and selected into the double thousand talents plan of Jiangxi Province. He has published more than 40 scholar articles and got more than 400 citations. His research interests include the area of chaos, secure communications, synchronization, optical communications, and chaos-based cryptography. He is a member of the Chaos Secure Communication Committee of China.

* * *