A New Fractional Chaotic System and Its Application in Image Encryption With DNA Mutation

JIN HAO, HONGJIE LI, HUIZHEN YAN, AND JUN MOU
School of Information Science and Engineering, Dalian Polytechnic University, Dalian 116034, China

Corresponding author: Hongjie Li (lihj@dlpu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62061014, and in part by the Natural Science Foundation of Liaoning Province under Grant 2020-MS-274.

ABSTRACT In this paper, a color image encryption algorithm based on the fractional-order multi-scroll Chen chaotic system and DNA mutation principle is proposed. The dynamical performances of the fractional-order multi-scroll Chen chaotic system are analyzed by phase diagram, Lyapunov exponential spectrum and bifurcation diagram. Meanwhile, we realized the hardware circuit simulation of the chaotic system on the DSP platform. Based on comprehensive analysis, an image encryption algorithm is designed. In particular, a DNA algorithm with mutation effect has been introduced into the encryption algorithm. Finally, the performances of the designed encryption scheme are analyzed by key space, correlation coefficients, information entropy, histogram, differential attacks and robustness analysis. The experimental results prove that the algorithm has strong encryption capabilities and can withstand multiple decryption methods. The new color image encryption scheme proposed in this paper can realize the secure communication of digital images.

INDEX TERMS Image encryption, fractional-order chaotic system, DNA mutation.

I. INTRODUCTION

With the rapid development of computer technology and network communication technology, a new platform is provided for us to achieve a more secure color image encryption algorithm design. So the data encryption methods have undergone tremendous changes. Since the color image contains a lot of information, and there are information associations between adjacent pixel, the existing encryption algorithms often cannot fully meet the requirements of digital image encryption. Therefore, the need to improve the performance of color image encryption has become a hot research now [1]–[6].

A chaotic system refers to a deterministic system with random irregular motion. It has unique characteristics such as initial value sensitivity, ergodicity and randomness [7], [8]. Therefore, algorithm design based on chaotic systems is very popular in the field of encryption algorithms [3]–[8]. Compared with general chaotic systems, multi-scroll Chen chaotic systems have greater advantages such as variety of complex dissipative system phenomena: bistable state, pulse reproduction, close to ideal model, easy to design, noise like and unpredictability [9]–[15]. For these reasons, Liu et al. analyzed the fuzzy model of parametric perturbation multi-scroll Chen chaotic system [16]. Chaotic Synchronization in Chen system was proposed by Ma et al. in [17]. Bai et al. analyzed Physical random bit generator based on multi-scroll chaotic system and its reliability [18]. Therefore, this paper proposes a new multi-scroll Chen chaotic system and analyzes its dynamical characteristics.

In addition, compared with integer-order chaotic systems, fractional-order systems can reflect natural phenomena more accurately and have more complex dynamical characteristics [19]. This makes fractional chaotic systems have been extensively studied [20]–[24]. For example, Xu et al. analyze the dynamic properties of fractional-order and applied it to image encryption [21]. Vilaridy et al. investigate the fractional convolution and nonlinear operations applied [22]. At this stage, the algorithms commonly used to analyze fractional chaotic systems include: frequency domain method, prediction correction method, ADM decomposition and CADM decomposition, etc. Among them,
ADM decomposition algorithm has the advantages of high computing efficiency and low resource consumption. Therefore, this decomposition method is widely used to solve chaotic systems [23]–[27]. At present, the analysis of the fractional-order multi-scroll Chen chaotic system is still insufficient, and the research on the decomposition method has great research value. Therefore, the ADM decomposition method is used to analyze the fractional-order dynamical characteristics of the new multi-scroll Chen chaotic system and applies it to the image encryption scheme. In addition, the signal from DSP board is more stable, easy to get, and the process is simpler [28]–[31]. Therefore, DSP components are used to generate the fractional-order chaotic signal in this paper.

At the same time, the image encryption scheme is designed based on the fractional-order multi-scroll Chen chaotic system. Recently, many image encryption algorithms based on chaotic systems have emerged in the encryption field [24], [32]–[34]. For instance, An RGB imaged encryption algorithm based on total plain image characteristics and chaos was proposed by Zhang [35]. A fast color imaged encryption scheme using one-time S-Boxes based on complex chaotic system and random noise was proposed by Liu [36]. Moreover, in encryption algorithms, researchers use genetic coding to improve the performance of the algorithms [37]–[40]. For instance, Yang et al. proposed an improved color image encryption scheme based on hyperchaotic sequences and DNA principles [41]. Chai et al. propose a color image encryption algorithm based substitution box generation using Chaos and DNA coding [42]. A secure and efficient Image encryption algorithm based on DNA coding and spatiotemporal chaos by Li et al [43]. According to existing researches, there are few encryption designs based on the principle of DNA mutations [44]–[49]. Therefore, the DNA mutation phenomenon is added to the design of the algorithm, which significantly improves the performance of the encryption algorithm. Therefore, a color image encryption scheme based on the fractional-order chaos system is designed. First, in the pixel scrambling link, the chaotic sequence and Arnold matrix are used to scramble the image. Secondly, the DNA encryption algorithm and DNA mutation theory were introduced for the first time in the diffusion operation. In addition, the catastrophe theory in this work can more radically change the value of pixels, thereby resisting various cracking attacks, and also provides a new encryption idea.

For these reasons, A color image encryption algorithm with better performance is proposed, which is based on the chaotic sequence generated by the fractional-order laser chaotic system, the principle of DNA mutation is added to it. The rest of this paper is structured as follows. The second section analyzes the dynamical characteristics of the system. The third part lists the encryption process and decryption process in detail. The results of related performance indicators are in Sec. 4. In Sec. 5, the conclusions are given.

**II. FRACTIONAL-ORDER MULTI-SCROLL<br>CHEN CHAOTIC SYSTEM<br>**

**A. MATHEMATIC MODEL OF THE MULTI-SCROLL<br>CHEN CHAOTIC SYSTEM<br>**

The circuit diagram of the chaotic system is shown in Fig.1, which provides proof for the application of chaotic theory in actual engineering.

According to the circuit diagram, we get the system formula:

\[
\begin{align*}
\dot{x} &= ay - x \\
\dot{y} &= (c - a - z + d \cos z)x + cy \\
\dot{z} &= xy - bz
\end{align*}
\]  

(1)

where, \(x_1, x_2, x_3\) represents state variable, and \(a, b, c, d\) represents system parameters.

According to the circuit model, the phase diagrams of the circuit diagram are shown in Fig.2. The time domain diagrams of the simulation circuit diagram are shown in Fig.3.
C. NUMERICAL SOLUTION OF THE SYSTEM BASED ON ADM ALGORITHM

According to definition, the fractional-order multi-scroll Chen chaotic system can be written as

\[
\begin{align*}
\dot{x}_1(t) &= a(x_2 - x_1) \\
\dot{x}_2(t) &= (c - a - x_3 + d \cos x_3)x_1 + cx_2 \\
\dot{x}_3(t) &= x_1x_2 - bx_3
\end{align*}
\]  
(12)

where, \( q \) is the order of the system.

System (12) can be decomposed into linear, nonlinear terms as:

\[
\begin{bmatrix}
Lx_1 \\
Lx_2 \\
Lx_3
\end{bmatrix} =
\begin{bmatrix}
a(x_2 - x_1) \\
cx_1 - ax_1 + cx_2 \\
-bx_3
\end{bmatrix}
\]
(13)

Under the premise of guaranteeing calculation accuracy and speed. According to the decomposition formula, \( A_2 = -x_1x_2 + d \cos x_3x_1 \) and \( A_3 = x_1x_2 \) are the two nonlinear terms of this system, which can be decomposed as:

\[
\begin{bmatrix}
A_0^0 \\
A_1^0 \\
A_2^0 \\
A_3^0 \\
\end{bmatrix} =
\begin{bmatrix}
-x_3^0x_1^0 + d \cos(x_3^0)x_1^0 \\
-x_3^0x_1^0 - x_3^0x_1^0 + d[-x_3^0x_1^0 \sin(x_3^0) + x_1^0 \cos(x_3^0)] \\
-x_3^0x_1^0 - x_3^0x_1^0 - x_3^0x_1^0 + d[x_3^0 \cos(x_3^0)] \\
-x_3^0x_1^0 - x_3^0x_1^0 - x_3^0x_1^0 + d[x_3^0 \cos(x_3^0)] \\
\end{bmatrix}
\]
(14)

\[
\begin{bmatrix}
A_0^1 \\
A_1^1 \\
A_2^1 \\
A_3^1 \\
\end{bmatrix} =
\begin{bmatrix}
-x_3^1x_1^1 - x_3^1x_1^1 - x_3^1x_1^1 - x_3^1x_1^1 + d[x_3^1 \cos(x_3^0)] \\
-x_3^1x_1^1 - x_3^1x_1^1 - x_3^1x_1^1 + d[x_3^1 \cos(x_3^0)] \\
-x_3^1x_1^1 - x_3^1x_1^1 - x_3^1x_1^1 + d[x_3^1 \cos(x_3^0)] \\
-x_3^1x_1^1 - x_3^1x_1^1 - x_3^1x_1^1 + d[x_3^1 \cos(x_3^0)] \\
\end{bmatrix}
\]
(15)
Assume that the initial value $x_0$, then the first item is:

$$
\begin{align*}
\mathbf{x}_1^0 &= x_1(t_0^0) \\
\mathbf{x}_2^0 &= x_2(t_0^0) \\
\mathbf{x}_3^0 &= x_3(t_0^0)
\end{align*}
$$

(16)

Letting $c_i^0 = x_i^0$, $c_i^2 = x_i^2$, $c_i^3 = x_i^3$, then $x_0 = c_0 = [c_1^0, c_2^0, c_3^0]$, $x_i^i = I_{0}^{\alpha}Lx^0 + I_{0}^{\alpha}Ax^0(i = 1, 2, 3)$ can be obtained according to the iterate relation formula formula(17). The coefficients of the other terms are

$$
\begin{align*}
C_1 &= c_1^0 - c_1^0; \\
C_2 &= (c - a)c_1^0 + c_2^0 + dc_1^0 c_3^0; \\
C_3 &= c_1^0 c_2^0 - bc_3^0; \\
C_4 &= a(c_2^0 - c_3^0); \\
C_5 &= (c - a)c_1^0 + c_2^0 + dc_1^0 c_3^0; \\
C_6 &= (c - a)c_1^0 + c_2^0 + dc_1^0 c_3^0; \\
C_7 &= (c - a)c_1^0 + c_2^0 + dc_1^0 c_3^0; \\
C_8 &= (c - a)c_1^0 + c_2^0 + dc_1^0 c_3^0; \\
C_9 &= (c - a)c_1^0 + c_2^0 + dc_1^0 c_3^0.
\end{align*}
$$

(17)

The ADM decomposition equation of chaotic system is obtained:

$$
\begin{align*}
\mathbf{x}_1 &= c_1^0 + c_1^1(t - t_0) + c_1^2(t - t_0)^2 + c_1^3(t - t_0)^3; \\
\mathbf{x}_2 &= c_2^0 + c_2^1(t - t_0) + c_2^2(t - t_0)^2 + c_2^3(t - t_0)^3; \\
\mathbf{x}_3 &= c_3^0 + c_3^1(t - t_0) + c_3^2(t - t_0)^2 + c_3^3(t - t_0)^3; \\
\mathbf{x}_4 &= c_4^0 + c_4^1(t - t_0) + c_4^2(t - t_0)^2 + c_4^3(t - t_0)^3; \\
\mathbf{x}_5 &= c_5^0 + c_5^1(t - t_0) + c_5^2(t - t_0)^2 + c_5^3(t - t_0)^3; \\
\mathbf{x}_6 &= c_6^0 + c_6^1(t - t_0) + c_6^2(t - t_0)^2 + c_6^3(t - t_0)^3; \\
\mathbf{x}_7 &= c_7^0 + c_7^1(t - t_0) + c_7^2(t - t_0)^2 + c_7^3(t - t_0)^3; \\
\mathbf{x}_8 &= c_8^0 + c_8^1(t - t_0) + c_8^2(t - t_0)^2 + c_8^3(t - t_0)^3; \\
\mathbf{x}_9 &= c_9^0 + c_9^1(t - t_0) + c_9^2(t - t_0)^2 + c_9^3(t - t_0)^3.
\end{align*}
$$

(18)

**D. DYNAMICAL CHARACTERISTICS OF THE FRACTIONAL-ORDER MULTI-SCROLL CHEN CHAOTIC SYSTEM**

Setting system parameters: $a = 35$, $b = 1.5$, $c = 28$, $d = 8$, $q = 0.9$ and the initial value is $(1,1,1)$. Fig.4 is the phase diagram under current parameters. When the step size is set to 0.01, the corresponding Lyapunov exponent are
LE₁ = 5.8462, LE₂ = 0, LE₃ = −10.1386 and the Lyapunov dimension is d_L = 2.5766. It can be proved that the system is in chaos at this time.

Setting a as the system variable with the range of [34, 37], and the other parameters b = 5, c = 28, d = 8, q = 0.9. Analysis of system dynamics are shown in Fig.5(a) and Fig.5(b). It can be seen that when a ∈ [34.3, 35.7], the system is in chaotic state. In other regions, the system behaves periodically.

Similarly, when b change with the range of [2.5, 6], setting the size of other parameters as a = 35, c = 28, d = 8, q = 0.9. The results are shown in Fig.6, which proves that the system can produce good random sequences.

Setting a = 35, c = 28, d = 8, b = 5, and varying q from 0.7 to 1, the resulting diagram is shown in Fig.7. It is found that system is chaotic over most of the range q ∈ (0.75, 1). Experiments show that the fractional-order system has a larger Lyapunov value than the integer phase, which proves that the system is more random. The order variable is increased, thereby increasing the degree of freedom of the system, and the dynamical characteristics of the system are more complicated.

E. RANDOMNESS ANALYSIS OF THE MULTI-SCROLL CHEN CHAOTIC SEQUENCES

The NISTSP800-22 test package is used to test the randomness of the new fractional-order multi-scroll Chen chaotic sequences. Presetting the initial values and parameters of chaotic system, then extract about 200 million values from the chaotic sequence obtained. Use the method of integer redundancy to convert each integer value into an 8-bit binary number. When the binary sequence is obtained, the NIST test can be performed on the binary sequence. The test results need to be compared with the STS standard proposed by the National Bureau of Technology and Standards.

The NIST test has two methods for measuring randomness of sequence. The first method is the pass proportion of the statistical test. Given the result of a statistical test, compute the pass proportion of test sample. For instance, if 1000 binary sequences were tested, the significance level α = 0.01, and 998 binary sequences had P-value 0.1. The pass proportion is 0.9960. The range of acceptable proportions is determined using the confidence interval defined as:

\[ \hat{p} = \sqrt{\frac{\hat{p}(1 - \hat{p})}{m}} \]  

(24)

where \( P = 1 - \alpha \), and m represents the size of the random sequence drawn. If the ratio falls into the interval of \( P \), it means that the sample is random.

Another method is the P-value of statistical test. From formula(15).

\[ x^2 = \sum_{i=1}^{10} \frac{(F_i - 0.1s)^2}{0.1s} \]  

(25)

The sequence can be considered randomness when the P-value ≥ 0.001.

The NIST test evaluates the roughly 200 million records produced by the system in this paper. Table 1 and Table 2 list the test results of the NIST test. NIST test results show that the randomness of the system is good. There are suitable for encryption algorithms.

F. DSP IMPLEMENTATION OF THE MULTI-SCROLL CHEN CHAOTIC SYSTEM

Digital circuits have many unique advantages, such as fast response speed, high calculation accuracy, convenient operation, and little influence from the outside world, so they
TABLE 1. The randomness test result.

| Test Name          | $P - \mu_{\text{mean}}$ | $P - \mu_{\text{exp}}$ | $\text{Pass Rate}$ |
|--------------------|--------------------------|--------------------------|--------------------|
| Frequency          | 0.3958                   | 0.5642                   | 0.97               |
| Block Frequency    | 0.3959                   | 0.6125                   | 1                  |
| Cumulative Sums    | 0.2469                   | 0.2106                   | 0.98               |
| Runs               | 0.4869                   | 0.3102                   | 0.99               |
| Longest Run       | 0.3859                   | 0.2958                   | 1                  |
| Rank              | 0.2369                   | 0.5103                   | 1                  |
| FFT               | 0.3952                   | 0.4302                   | 0.99               |
| Non Overlapping Template | 0.3986   | 0.4103                   | 0.97               |
| Overlapping Template | 0.2936   | 0.3209                   | 0.99               |
| Universal         | 0.2490                   | 0.9516                   | 0.99               |
| Approximate Entropy | 0.4361  | 0.9462                   | 1                  |
| Random Excursions | 0.3469                   | 0.5123                   | 1                  |
| Random Excursions Variant | 0.3489 | 0.4236                   | 1                  |
| Serial            | 0.3568                   | 0.8462                   | 0.9886             |
| Linear Complexity | 0.2385                   | 0.5686                   | 0.9886             |

TABLE 2. Random excursions variant.

| Random excursions variant | $P - \mu_{\text{mean}}$ | $P - \mu_{\text{exp}}$ | $\text{Pass Rate}$ |
|---------------------------|--------------------------|--------------------------|--------------------|
| x=-9                      | 0.2395                   | 0.1568                   | 0.99               |
| x=-8                      | 0.4595                   | 0.4586                   | 1                  |
| x=7                       | 0.3469                   | 0.3489                   | 1                  |
| x=6                       | 0.3468                   | 0.2024                   | 0.99               |
| x=5                       | 0.3128                   | 0.2368                   | 0.98               |
| x=4                       | 0.3439                   | 0.4685                   | 1                  |
| x=3                       | 0.3058                   | 0.6568                   | 1                  |
| x=2                       | 0.3528                   | 0.4695                   | 1                  |
| x=1                       | 0.4056                   | 0.4526                   | 0.98               |
| x=0                       | 0.3058                   | 0.4463                   | 0.97               |
| x=2                       | 0.3156                   | 0.2168                   | 1                  |
| x=3                       | 0.3695                   | 0.2036                   | 1                  |
| x=4                       | 0.3486                   | 0.2068                   | 0.99               |
| x=5                       | 0.3486                   | 0.5132                   | 0.98               |
| x=6                       | 0.3698                   | 0.6088                   | 0.99               |
| x=7                       | 0.3152                   | 0.6563                   | 1                  |
| x=8                       | 0.3645                   | 0.4686                   | 0.99               |
| x=9                       | 0.3468                   | 0.4582                   | 0.98               |

FIGURE 8. DSP simulation result.

are widely used as signal generators for chaotic systems. The experimental operating station is shown in Fig. 8. Setting parameters are consistent with the Settings shown in Fig. 2 above. The simulation diagram of the oscilloscope is shown in Fig. 8. The result is consistent with the preset result. The results show that the chaotic signal of the four-dimensional laser chaotic system is easy to obtain and can be effectively practiced in the field of communications.

III. IMAGE ENCRYPTION AND DECRYPTION SCHEME

A. PRINCIPLE OF DNA MUTATION

The DNA sequence consists of four nucleic acid bases: ATCG (adenine, thymine, cytosine, guanine), where A and T are complementary, C and G are complementary. In the current DNA code theory, all information is represented by four nucleotides A, T, C, and G. According to the complementary rule of computer binary 0 and 1, 00 and 11 are complementary, and 01 and 10 are complementary. Therefore, the DNA bases A, T, C, and G are encoded as 00, 01, 10, and 11 respectively during the encoding process. Obviously, there are 4! = 24 encoding rules, but only 8 encoding methods satisfy the Watson-Crick complementary rule, as shown in Table 3. On the basis of traditional binary addition and subtraction, DNA addition and subtraction can be obtained. Therefore, according to the eight DNA code rules, there are corresponding eight DNA addition and subtraction rules. For example, on the basis of DNA code rule 1, DNA addition rule 1 and subtraction rule 1 are shown in Table 4.

\[
\begin{align*}
(1) R(00) &= A, R(01) = C, R(10) = G, R(11) = T; \\
(2) R(00) &= A, R(01) = G, R(10) = C, R(11) = T; \\
(3) R(00) &= T, R(01) = C, R(10) = G, R(11) = A; \\
(4) R(00) &= T, R(01) = G, R(10) = C, R(11) = A; \\
(5) R(00) &= G, R(01) = T, R(10) = A, R(11) = C; \\
(6) R(00) &= G, R(01) = A, R(10) = T, R(11) = C; \\
(7) R(00) &= C, R(01) = T, R(10) = A, R(11) = G; \\
(8) R(00) &= C, R(01) = A, R(10) = T, R(11) = G; \\
\end{align*}
\]

In the process of DNA sequence formation, A (guanine) is paired with T (thymine), and C (adenine) and G (cytosine) are paired. At the same time, when \( L(x_i) \) is a complementary pair of \( x_i \), each base \( x_i \) and its paired base pair satisfy the following formula.

\[
\begin{align*}
&x_i \neq T(x_i) \neq T(T(x_i)) \neq T(T(T(x_i))) \\
&x_i = T(T(T(x_i))))
\end{align*}
\]

According to the formula, there are six effective rules for base pairing, as shown in Table 4. In the encryption process, On the premise of randomly selecting a coding method, a mutual matching principle is randomly selected to implement the diffusion link.

In the process of DNA complementary pairing, there will be DNA mutations. One of them is called base mismatches.
due to tautomism, which refers to the mutation caused by the substitution of one base in the DNA sequence by another base. The principle is shown in Figure 9. Convert its principle into a formula as shown in formula (28), when the base sequence has a specific arrangement, the structure will be unstable, and then one base in the DNA sequence will be replaced by another base. This phenomenon is also called point mutation. Because the occurrence of gene mutations is affected by specific gene combinations, mutations are the result of random mutations. The occurrence of this mutation can improve the randomness of the encryption algorithm.

The specific encryption steps are listed as follows:

Step 1: Inputting the color original image I with the size of $H \times W$. Setting the key values $a, b, c, d, x_1, x_2, x_3, m, n, \alpha, \beta, L_i$, the new initial value conditions of the fractional-order multi-scroll Chen chaotic system can be obtained according to the formula algorithm:

$$s = \frac{\sum_{i=1}^{H} f(i, j)}{10^{10}}$$

$$x_0 = x_0 + s$$

$$y_0 = y_0 + s$$

$$z_0 = z_0 + s$$

Step 2: Setting $L = \max(H, W)$, let the chaotic system iterate $(m+L)$ times according to the new initial condition, and discard the previous $m$ values to increase the sensitivity of the initial value. At the same time, the matrix replacement coefficients of the scrambling algorithm are determined by formula (31).

$$C_x = \text{mod}(\text{floor}(a x \times 10^{16}), H \times W))$$

$$C_y = \text{mod}(\text{floor}(b y \times 10^{16}), H \times W))$$

$$C_z = \text{mod}(\text{floor}(c z \times 10^{16}), H \times W))$$

Step 3: Decomposing the color image I into Right, Green, and Blue three pixels matrix, each pixel with the size of $H \times W$, and perform shift processing on the points of the three pixel matrix elements respectively. The specific operation is: each coordinate point in the matrix is uniquely opposed to the replacement point $C(k1)k2)$. After reconstructing the matrix, the scrambled image matrix $TK$ is obtained. The scrambling rule of the algorithm is determined by formula (32).

$$k1; k2) = \text{mod}(\frac{1}{C_y(i, j)} C_x(i, j) \times [i; j], [H; W]) + [1; 1].$$

where $k1, k2$ are the coordinates of the corresponding replacement points.

The scrambled pixel matrix is diffused by DNA operation rules, including addition operation, complementary operation and mutation operation. Specific steps are as follows:

Step 4: Converting the values in the matrix $TK$ to binary, and then getting binary matrices of size $H \times W \times 8$: $R_1$, $G_1$, and $B_1$. Then according to the DNA coding rules, the binary matrix is converted into $H \times W \times 4$ DNA sequence matrices $ST_1$, $ST_2$ and $ST_3$.

Step 5: In advance to get the chaotic sequence through the iterative system $n+H \times W$ times, and discarding the first $n$ values. According to formula (33), we get three chaotic sequences: $ST_1$, $ST_2$ and $ST_3$.

$$k1 = \text{mod}((||x1||) \times 10^{16}, 256)$$

$$k2 = \text{mod}((||y1||) \times 10^{16}, 256)$$

$$k3 = \text{mod}((||z1||) \times 10^{16}, 256)$$
After shaping the obtained sequences, DNA coding is performed to obtain a new set of DNA sequence matrices $K_1$, $K_2$, and $K_3$. The matrix size is the same as the pixel matrix size.

Step 6: Performing the diffusion operation on the pixel matrix $S_1$ with the obtained pseudo-random number sequence matrix $K_1$. The specific method is: add the pixel $S_1$ matrix and the $K_1$ matrix, and then generate an image pixel matrix $N_1$. During the diffusion process, a coding rule is randomly selected from Table 3. Then select a DNA addition and subtraction rule in Table 4.

Step 7: Add DNA point mutations to image information encryption. When a particular base arrangement appears, genetic mutations occur. The law of gene mutation occurs according to formula (28).

Step 8: Using DNA coding rules to reverse-encode the $C_1$ matrix and restore it to a pixel matrix $C$ expressed in decimal numbers.

Step 9: Outputting the final encrypted image.

C. DECRYPTION ALGORITHM

The decryption algorithm is the process of restoring the original image. Firstly, the encrypted image is re-encoded into a DNA sequence matrix, and then the mutation principle is used for reverse reduction. After the reduction, the principle of DNA subtraction and the principle of DNA complementation are used to obtain the original DNA sequence of the encrypted image. Reverse DNA encoding is performed on the sequence to obtain the binary sequence of the image. The fractional-order multi-scroll Chen chaotic system is used to generate chaotic sequences and perform reverse scrambling. Convert it to a decimal pixel matrix and restore the decrypted image. The main encryption process is shown in Fig. 11.

Step 1: Loading the original image $O$, and decomposing into $Right$, $Green$, and $Blue$ three pixels matrix. According to the set DNA coding rules, transform the pixel matrix, and then get $R_1$, $G_1$, and $B_1$ with the size of $H \times W \times 4$.

Step 2: Using DNA gene mutation to reverse mutation change. Generate a diffused matrix.
### TABLE 5. Number of keys.

| Encryption scheme | Proposed algorithm | Ref. [22] | Ref. [26] | Ref. [30] | Ref. [36] | Ref. [40] | Ref. [48] |
|-------------------|-------------------|-----------|-----------|-----------|-----------|-----------|-----------|
| Key space         | $2^{379}$         | $2^{372}$ | $2^{368}$ | $2^{386}$ | $2^{382}$ | $2^{387}$ | $2^{313}$ |

Step 3: Generating random sequence through the fractional-order multi-scroll Chen chaotic system and converting it into DNA coding sequence. Using DNA subtraction calculation and base pairing rules, the diffusion matrix is reversed with the generated pseudo-random sequence. To obtain the DNA element matrix $S_1$, which is not fully decrypted.

Step 4: Reshaping $S_1$ into a matrix of size $H \times W \times 4$ and perform binary encoding to form an element matrix $TK$. The sequence is generated by the multi-scroll Chen chaotic system, and the point permutation rule is generated by formula (28). Reverse scrambling to restore the disrupted matrix.

Step 5: Perform dot scrambling reverse operation on the matrix to obtain the decrypted pixel matrix.

Step 6: Restore the three binary pixel matrixes to decimal, and output the decrypted image through combination. Fig.11 shows the decryption process.

### IV. SECURITY ANALYSIS AND STATISTICAL ANALYSIS

In order to verify the image encryption algorithm proposed in this paper, a simulation experiment was carried out based on MATLAB software, which directly proved the effectiveness and safety of the algorithm.

#### A. ENCRYPTION ALGORITHM SIMULATION RESULTS

Setting parameters with $a = 35, b = 5, c = 28, d = 8, q = 0.9$ for the initial conditions $x_1 = 1, x_2 = 1, x_3 = 1$; thirty sets of $256 \times 256$ color sample images are tested as original digital images to verify the security of the image encryption algorithm. Fig.12 shows three representative images (Yacht, Baboon and Boat), which visually display part of the experimental results. Tests show that the original image information can be completely hidden after being encrypted.

#### B. KEY SPACE ANALYSIS

In order to resist brute force attacks, encryption algorithms should have a huge key space. The proposed image encryption scheme uses $x_1, x_2, x_3, a, b, c, d$ as the key of the pixel scrambling step. If the calculation accuracy is $10^{-15}$, The corresponding key space size is about $2^{379}$. In addition, for the other part of the key $m, n, c_0, \alpha, \beta, L_i$. The encryption algorithm contains four bases, eight preset encoding methods and six complementary rules. So in the expansion process, the size of the key space is $2^2 \times 2^3 \times 2^{20} = 2^{38}$. Therefore, the key space of this algorithm is $2^{407}$. The results show that the proposed algorithm space is large enough.

In Table 5, the key space size of some existing DNA encryption algorithms is given. The comparison shows that the encryption algorithm proposed in this paper has a larger key space.

#### C. KEY SENSITIVITY ANALYSIS

Key sensitivity means that the key has been slightly changed, and the decrypted image should not display plain text information. In this experiment, making small changes to the decryption keys separately, then the decryption Boat images show in Fig.13. The simulation results show that the incorrectly decrypted image completely hides the plaintext information. Subsequently, we compare the pixel value of the incorrectly decrypted image with the original image, and the difference rate is shown in Table 6. The error-decrypted image...
differs from the original image by more than 99%. These results show that the algorithm is very sensitive to keys.

D. STATISTICAL PERFORMANCE ANALYSIS
In this chapter, a number of tests are used to evaluate the performance of image encryption algorithms.

1) HISTOGRAM ANALYSIS
An image is composed of pixels of different values (colors). The distribution of pixel values in the entire image is an important attribute of the image. We often use histograms to visualize this attribute. A good encryption algorithm needs to make the histogram of the encrypted image flat, so as to resist statistical attacks. We take the R pixel channel of multiple images as an example to verify the proposed encryption algorithm. Tests show that the encrypted image completely breaks the correlation of the original image. The result is shown in Fig.14. The smooth histogram can effectively resist statistical attacks and will not allow attackers to obtain useful information by analyzing encrypted images.

2) CHI-SQUARE TEST
Chi-square test is often used to compare two or more sample rates and the correlation of two categorical variables. As shown in formula (34):

$$x^2 = \sum_{n} \frac{(C_n - G)^2}{G}$$

(34)

A small chi-square value indicates that the data change is small, which means that the encryption technology can conceal all information, and the pixels on the image are randomly distributed. For a good encryption algorithm, when the confidence level is 0.05, the chi-square value of the encrypted image should not exceed 293.247. By testing different images (R channel), the results are shown in Table 7, all exceeding the critical value. These results prove that the image encryption scheme can resist statistical analysis attacks.

3) IMAGE CORRELATION COEFFICIENT
Before the image information is encrypted, there is a great correlation between two adjacent pixels. This association should be minimized when designing encryption algorithms.
### TABLE 8. Correlation coefficients in channels.

| Channel | Direction | Plain image | Cipher image | Ref. [34] | Ref. [40] |
|---------|-----------|-------------|--------------|-----------|-----------|
| R Channel | Horizontal | 0.9486 | 0.0019 | 0.0034 | 0.0045 |
|         | Vertical  | 0.9287 | 6.6495 x 10^{-4} | -0.0053 | 0.0051 |
|         | Diagonal  | 0.9684 | -0.0012 | -0.0023 | 0.0078 |
|         | Horizontal | 0.9354 | 0.0056 | 0.0143 | -0.0025 |
| G Channel | Vertical  | 0.9159 | 4.2595 x 10^{-4} | 0.0091 | -0.0011 |
|         | Diagonal  | 0.9368 | -8.4562 x 10^{-4} | -0.0039 | 0.0039 |
|         | Horizontal | 0.9280 | -8.7595 x 10^{-4} | 0.0086 | -0.0131 |
| B Channel | Vertical  | 0.9259 | 7.2658 x 10^{-4} | 0.0539 | 0.0599 |
|         | Diagonal  | 0.9436 | 0.0044 | -0.0385 | 0.0048 |

### TABLE 9. Information entropy.

| Image name | Information entropy | $H_{0.05}^0 = 7.9019$ | $H_{0.01}^0 = 7.9017$ | $H_{0.001}^0 = 7.9015$ |
|------------|---------------------|-----------------------|---------------------|-----------------------|
| Yacht      | 7.9977              | Qualified             | Qualified            | Qualified             |
| Baboon     | 7.9969              | Qualified             | Qualified            | Qualified             |
| Boat       | 7.9979              | Qualified             | Qualified            | Qualified             |

The relevant formula is as follows:

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{ \text{D}(X) \text{D}(Y)}}$$  \hspace{1cm} (35)

$$\text{cov}(x, y) = E [(x - E(x))(y - E(y))]$$  \hspace{1cm} (36)

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i$$  \hspace{1cm} (37)

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2$$  \hspace{1cm} (38)

Among them, $x, y$ represents the corresponding pixels between the two images, $\text{cov}(x, y)$, $E(x)$ and $D(x)$ represent covariance, mean and variance, respectively, and $N$ represents the total number of image pixels.

Taking the Boat with instance, the correlation coefficients of different channels before and after encryption. The results were shown in Table 8. Table 9 lists the experimental effects of other encryption schemes. Through comparison with other encryption algorithms, the algorithm proposed in this paper has a good ability to reduce the correlation between pixels.

In order to visually see the correlation of the image before and after encryption, the relative distribution level of adjacent pixels of image are shown in Fig.15. Before the image is encrypted, there is a strong correlation between adjacent pixels, most of the pixels of the original image are on the $y = x$ line, which was shown in Fig.15(a). After encryption, the pixels of the image are scattered very uniformly as shown in Fig.15(b). The performance test results show that the correlation between adjacent pixels of the encrypted image is greatly reduced, and the encryption algorithm can resist statistical attacks.

### 4) INFORMATION ENTROPY

Information entropy describes the uncertainty of the source, the average amount of information of all targets in the source, and is often used to test the confusion of the image. As shown in formula(39):

$$H(m) = \sum_{i=1}^{L-1} P(m_i) \times \log \frac{1}{P(m_i)}$$  \hspace{1cm} (39)

where, $P(m_i)$ represents the probability of the appearance of symbol $m_i$, $L$ represents the number of all feature points $m_i$.

For the $L = 256$ images, the theoretical value of information entropy is 8. Table 9 lists the information entropy of the pixel channels of the three colors, and the calculation results are all close to 8. The results prove that the encrypted image has good randomness. The information entropy values of other encryption algorithms are shown in Table 10 (Taking Yacht images for example). The results show that the encryption algorithm proposed in this paper can make the encrypted image approximate to a random image.
5) DIFFERENTIAL ATTACK ANALYSIS

We usually use two differential attack methods to verify the sensitivity of ciphertext to plaintext: pixel number change rate (NPCR) and uniform average change rate (UACI).

NPCR value and UACI value are calculated by the following formula

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

\[
\text{UACI} = \frac{1}{L} \sum_{i,j} \frac{C(a,b) - C_1(a,b)}{H} \times 100
\]

where \( L \) is the number of image pixels. \( C \) and \( C_1 \) respectively represent the pixel value at the same position. The \( E(i,j) \) is obtained as:

\[
E(i,j) = \begin{cases} 
1 & I(i,j) \neq I(i,j) \\
0 & I(i,j) = I(i,j)
\end{cases}
\]

Recently, NPCR and UACI criterion values have become the standard for performance evaluation. The critical NPCR values for the significance level \( \alpha \) are obtained as

\[
N^{\alpha}_{\text{NPCR}} = \frac{F - \Phi^{-1}(\alpha/2)\sqrt{F/L}}{F+1}
\]

The critical UACI values for the are obtained as

\[
\begin{align*}
U^-_{\alpha} &= \mu_u - \Phi^{-1}(\alpha/2)\sigma_u \\
U^+_{\alpha} &= \mu_u + \Phi^{-1}(\alpha/2)\sigma_u
\end{align*}
\]

where

\[
\mu_u = \frac{F + 2}{3F + 3}
\]

\[
\sigma_u = \frac{(F + 2)(F^2 + 2F + 3)}{18(F + 1)^2FL}
\]

We test the three pixels channels of the image separately, and average the results obtained. Tables 11 and 12 list the results, and Table 13, the algorithm in this paper is compared with the existing encryption algorithm, which proves that the algorithm improves the encryption performance theoretically.

E. ANTI-NOISE ATTACK PERFORMANCE ANALYSIS

During the decryption process, some redundant information will interfere with the algorithm. This section will add some noise to the decryption link to test the algorithm’s anti-noise pollution attack ability, and then analyze the robustness of the proposed algorithm. In the decryption process, Gaussian noise with intensities of 0.05, 0.06 and 0.07 are added, and then the contaminated ciphertext image is decrypted. The result is shown in Fig.16. The experimental results show that the image information is still clear, and the algorithm in this paper can effectively resist noise attacks and restore encrypted images.

V. CONCLUSION

A novel color image encryption algorithm based on multi-scroll Chen chaotic system and DNA mutation principle has been proposed in this paper. The ADM algorithm is used to decompose the system, and the dynamical analysis shows that, compared with the integer order, the fractional-order multi-scroll Chen chaotic system has

---

### TABLE 11. NPCR Values of different plaintext images.

| Image name | NPCR(%) | Critical Value |
|------------|---------|----------------|
| Yacht      | 99.69%  | Qualified      |
| Baboon     | 99.71%  | Qualified      |
| Boat       | 99.60%  | Qualified      |

### TABLE 12. Anti-difference attack analyze.

| Image name | UACI(%) | Critical Value |
|------------|---------|----------------|
| Yacht      | 33.41%  | Qualified      |
| Baboon     | 33.45%  | Qualified      |
| Boat       | 33.48%  | Qualified      |

### TABLE 13. Compare with another scheme (Take Lena image as an example).

|                  | Proposed algorithm | Ref. [22] | Ref. [25] | Ref. [33] | Ref. [38] | Ref. [59] |
|------------------|--------------------|-----------|-----------|-----------|-----------|-----------|
| NPCR             | 99.69%             | 99.61%    | 99.62%    | 99.61%    | 99.64%    | 99.63%    |
| UACI             | 66.46%             | 33.41%    | 33.38%    | 33.45%    | 33.42%    | 33.41%    |
good performance dynamic characteristics such as complex parameter changes and rich dynamic characteristics. At the same time, the fractional-order multi-scroll Chen chaotic system realizes the simulation based on the DSP platform, which will be able to apply the chaotic system to practical applications, theoretical support is provided. Meanwhile, through the NIST test, it is proved that the fractional-order chaotic sequence has good randomness, which is suitable for image encryption. In the color image encryption algorithm, the principle of DNA coding and DNA mutation are used to make the pixel more random. The performance test results show that the encryption algorithm not only has a better image encryption effect, but also improves the anti-attacking ability. Therefore, the new chaotic system proposed in this paper has good performance and is applied to color image encryption. It also provides relevant theoretical basis and practical application basis for the application of chaos theory in the field of communication and information encryption.

REFERENCES

[1] Y. Luo, R. Zhou, J. Liu, Y. Cao, and X. Ding, “A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map,” *Nonlinear Dyn.*, vol. 93, no. 3, pp. 1165–1181, Aug. 2018.

[2] L. Gong, C. Deng, S. Pan, and N. Zhou, “Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform,” *Opt. Laser Technol.*, vol. 103, pp. 48–58, Jul. 2018.

[3] N. Zhou, A. Zhang, J. Wu, D. Pei, and Y. Yang, “Novel hybrid image compression-encryption algorithm based on compressive sensing,” *Optik*, vol. 125, no. 18, pp. 5075–5080, Sep. 2014.

[4] X. Chai, H. Wu, Z. Gan, Y. Zhang, and Y. Chen, “Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy,” *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107525.

[5] S. Amina and F. K. Mohamed, “An efficient and secure chaotic cipher algorithm for image content preservation,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 60, pp. 62–12, Jul. 2018.

[6] A. Kiani-B, K. Fallahi, N. Pariz, and H. Leung, “A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 14, no. 3, pp. 863–879, Mar. 2009.

[7] S. Bhalerao, “Dynamical analysis of fractional order Ucar prototype delayed system,” *Signal, Image Video Process.*, vol. 6, no. 3, pp. 513–519, Sep. 2012.

[8] X. Wu, Y. Li, and J. Kurths, “A new color image encryption scheme using CML and a fractional-order chaotic system,” *PLoS ONE*, vol. 10, no. 3, Mar. 2015, Art. no. e0119660.

[9] L. Zhang, K. Sun, S. He, H. Wang, and Y. Xu, “Solution and dynamics of a fractional-order 5-D hyperchaotic system with four wings,” *Eur. Phys. J. Plus*, vol. 132, no. 1, p. 31, Jan. 2017.

[10] J. Ruan, K. Sun, J. Mou, S. He, and L. Zhang, “Fractional-order simplest memristor-based chaotic circuit with new derivative,” *Eur. Phys. J. Plus*, vol. 133, no. 1, pp. 1–12, Jan. 2018.

[11] Y. Xu, K. Sun, S. He, and L. Zhang, “Dynamics of a fractional-order simplified unified system based on the Adomian decomposition method,” *Eur. Phys. J. Plus*, vol. 131, no. 6, pp. 1–12, Jun. 2016.

[12] F. Yang, J. Mou, K. Sun, Y. Cao, and J. Jin, “Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit,” *IEEE Access*, vol. 7, pp. 58751–58763, 2019.

[13] J. Zhao, S. Wang, Y. Chang, and X. Li, “A novel image encryption scheme based on an improper fractional-order chaotic system,” *Nonlinear Dyn.*, vol. 80, no. 4, pp. 1721–1729, Jun. 2015.

[14] X. Huang, T. Sun, Y. Li, and J. Liang, “A color image encryption algorithm based on a fractional-order hyperchaotic system,” *Entropy*, vol. 17, no. 1, pp. 28–38, Dec. 2014.

[15] Z. Wang, X. Huang, N. Li, and X.-N. Song, “Image encryption based on a delayed fractional-order chaotic logistic system,” *Chin. Phys. B*, vol. 21, no. 5, May 2012, Art. no. 050506.
[40] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, “A chaotic image encryption algorithm based on perceptron model,” *Nonlinear Dyn.*, vol. 62, no. 3, pp. 613–621, Nov. 2010.

[41] 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.

[42] D. L. Donoho, “Compressed sensing,” *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[43] E. J. Candes, J. Romberg, and T. Tao, “Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information,” *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[44] Y. Rachlin and D. Baron, “The secrecy of compressed sensing measurements,” in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 813–817.

[45] M. Ramezani Mayiami, B. Seyfe, and H. G. Bafghi, “Perfect secrecy via compressed sensing,” in *Proc. Iran Workshop Commun. Inf. Theory*, May 2013, pp. 1–5.

[46] H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, “A visually secure image encryption scheme based on parallel compressive sensing,” *Signal Process.*, vol. 155, pp. 218–232, Feb. 2019.

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

[48] S. Dai, K. Sun, W. Ai, and Y. Peng, “Novel discrete chaotic system via fractal transformation and its DSP implementation,” *Mod. Phys. Lett. B*, vol. 34, Dec. 2020, Art. no. 2050429.

[49] Y. Peng, K. Sun, and S. He, “An improved return maps method for parameter estimation of chaotic systems,” *Int. J. Bifurcation Chaos*, vol. 30, no. 4, Mar. 2020, Art. no. 2050058.

[50] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, “Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing,” *Opt. Laser Technol.*, vol. 82, pp. 121–133, Aug. 2016.

**JIN HAO** received the B.S. degree from Dalian Polytechnic University, Dalian, China, in 2018, where he is currently pursuing the Ph.D. degree in control science and engineering. His main research interests include chaos theory and chaotic digital image cryptosystem.

**HONGJIE LI** received the M.S. degree in signal and information processing from the Dalian University of Technology, Dalian, China. She is currently a Lecturer with the School of Information Science and Engineering, Dalian Polytechnic University, China. Her main research interests include digital image processing, and non-Gaussian and non-stationary signal processing theory.

**HUIZHEN YAN** received the B.S. and M.S. degrees from Xi’an Jiaotong University (XJU), Xi’an, China, and the Ph.D. degree in applied mathematics from Northeastern University (NEU), Shenyang, China, in 2000. She is currently a Professor with the School of Information Science and Engineering, Dalian Polytechnic University. Her research interests include game theory and its application, and ecological mathematics.

**JUN MOU** received the B.S., M.S., and Ph.D. degrees in physics and electronics from Central South University, Changsha, China. He is currently an Associate Professor with the School of Information Science and Engineering, Dalian Polytechnic University, China. His main research interests include nonlinear system control, secure communication, power system automation, and smart grid research.