A Novel Color Image Encryption Scheme Based on
Chaotic Sequence and DNA Mutation Principle

Jin Hao, Miao Miao, HuiZhen Yan

{miaomiao@dlpu.edu.cn}

School of Information Science and Engineering, Dalian polytechnic University, Dalian, 116034, China

ABSTRACT: Based on the simplified three-dimensional fractional unified chaotic system and the principle of DNA mutation, this paper proposes a color image encryption method to further improve the security of image information transmission. On the other hand, the pseudorandom sequence generated by the 3D score simplified unified chaotic system uses the DNA mutation principle algorithm to scramble the color image and expand the pixel value. Finally, the security of the proposed cryptographic algorithm is analyzed using key space, correlation, information entropy, etc. Numerical simulation results show that the algorithm has good security. The results of this paper provide a theoretical basis for the unification of the chaotic system applying the principle of fractional simplification and DNA mutation to image security.

Keywords: Chaotic System; Image Encryption Scheme;DNA Mutation Principle

1.Introduction

With the rapid development of networks and communication technologies, data transmission methods have undergone tremendous changes, and the demand for data transmission security is also increasing. However, Some existing encryption designs are no longer sufficient to support the encryption operation of huge information pictures, let alone achieve good results. Therefore, the research on digital image encryption algorithms has become one of the research topics. Because chaotic systems are random or uncertain motions in a specific system, they have many unique characteristics, such as inherent randomness and sensitivity to initial values, making them suitable for designing image encryption
People are actively researching fractional chaotic systems that reflect natural phenomena more accurately than integer chaotic systems\[7,8\]. Compared with traditional fractional-order system solving algorithms, the Adomian decomposition method has the advantages of fast convergence. It consumes fewer resources, and the calculation speed is faster\[8-15\]. For example, Wang et al. study the connection between image encryption and chaotic system with memristor, and put it into practice \[8\]. Zhang et al. analyzed the synchronization and adaptation problems of fractional-order chaotic systems \[10\]. Inubushi et al. studied the dynamics of fractional feedback control\[16\]. Natiq et al. study the connection between image encryption and fractional chaotic system, and put it into practice \[17\]. This paper proposes a three-dimensional fractional-order simplified unified system, and analyzes the dynamic characteristics of its fractional-order system.

At present, a variety of image encryption algorithms have been proposed based on chaotic systems\[18-22\]. For example, literature \[19,23-25\] proposed an image encryption algorithm based on discrete chaotic system, and literature \[26-30\] used hyperchaotic system image encryption algorithm. Literature \[7,31-45\] proposed a new image encryption algorithm based on chaotic system and DNA manipulation. Improve the security performance of image encryption algorithms this paper introduces the DNA mutation theory into the encryption algorithm.

The structure of the text is as follows. The second part introduces the operation rules of DNA sequence and the simplified 3D score calculation unified system. The third part gives the concrete steps of the image plus decoding scheme. The fourth part gives the simulation results and analyzes the security characteristics of the improved image encryption algorithm. Finally, Section 5 summarizes the research.

2. Basic principle

2.1 DNA mutation principle

Table 1 shows that only 8 of the 24 coding rules meet the Watson click to complete rule. In addition to the regular double addition/subtraction, the addition/subtraction of DNA is also obtained. So on the basis of the existing, we designed eight addition and subtraction rules based on the principle of subdivision. Table 2 shows DNA addition rule 1 and subtraction rule 1 taking DNA coding rule 1 as an example.
Therefore, according to the selection and matching of the actual DNA double-strand complementary, we designed the pairing principle. As shown in the formula, in the encryption process, the existing information is paired according to the pairing principle.

\[
\begin{align*}
    a_i &\neq S(a_i) \neq S(S(a_i)) \neq S(S(S(a_i))) \\
    a_i &= S(S(S(a_i)))
\end{align*}
\]  

(1)

From the equation, we can find the appropriate combination of six complementary base pairs, as shown in (2).

(1) L1 (A) = T, L1 (T) = T, L1 (C) = G, L1 (G) = A;
(1) L2 (A) = T, L2 (T) = T, L2 (G) = C, L2 (C) = A;
(1) L3 (A) = C, L3 (C) = T, L3 (T) = G, L3 (G) = A;
(1) L4 (A) = C, L4 (C) = T, L4 (G) = T, L4 (T) = A;
(1) L5 (A) = G, L5 (G) = T, L5 (T) = C, L5 (C) = A;
(1) L6 (A) = G, L6 (G) = T, L6 (C) = T, L6 (T) = A;

(2)

In the actual operation and matching process of DNA double-strands, special changes

<table>
<thead>
<tr>
<th>rule</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>A</td>
<td>A</td>
<td>T</td>
<td>T</td>
<td>G</td>
<td>G</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>01</td>
<td>C</td>
<td>G</td>
<td>C</td>
<td>G</td>
<td>T</td>
<td>A</td>
<td>T</td>
<td>A</td>
</tr>
<tr>
<td>10</td>
<td>G</td>
<td>C</td>
<td>G</td>
<td>C</td>
<td>A</td>
<td>T</td>
<td>A</td>
<td>T</td>
</tr>
<tr>
<td>11</td>
<td>T</td>
<td>T</td>
<td>A</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>G</td>
<td>G</td>
</tr>
</tbody>
</table>
will occur, that is, they will not happen according to the predetermined design. One form of this is that mismatched bases are matched and individual mutations occur. Therefore, mutations in this will appear randomly, individuals with specific mutations, and specific mutations in genes, all are the results of random mutations. This kind of sudden application can meet the requirements of high randomness and high change rate of image information encryption.

2.2 Dynamic analysis

This paper proposes a fractional three-dimensional simplified unified system based on Lu system and Chen system. Here, \( x_1, x_2, x_3 \) are the chaotic state variables \( q (q \leq 1) \) is the rank of the fractional equation, \( c \) is the system parameter

\[
\begin{align*}
T^q_t x_1 &= (25c + 10)(x_2 - x_1) \\
T^q_t x_2 &= (27 - 6c)x_2 - x_1x_3 \\
T^q_t x_3 &= x_1x_2 - (8 + c)x_3 / 3
\end{align*}
\]  

(3)

Let the system parameters \( c=0.9 \), \( q=0.9 \), the time step is \( t=0.001s \), and the system initial value \([x_0, y_0, z_0] = [0.1, 0.2, 0.3] \). At this time, the chaotic attractor phase diagram of the system is shown in Figure 1. At the same time, the Lyapunov index \((L_1, L_2, L_3) = (5.0824, 0, -3.9031)\) can be calculated. Since the system has only one positive Lyapunov index value, and the sum of all Lyapunov indexes is negative, so the system is in a chaotic state under current conditions. When the system parameters \( q=0.9 \) and \( c \in [0.7:1.15] \), the period window is only close to \( c=0.84 \). Figure 3 shows the Lyapunov exponent spectrum and bifurcation diagram of the system parameter \( c=0.9 \), \( c \in [4.4: 1.15] \). It can be seen from Figure 3 that the system is mostly chaotic in the range of \( q \in [0.4, 1.15] \), and there is only a periodic window near \( q=0.84 \).

It can be seen from the above that the chaotic regions of the unified system with simplified scores are distributed in a larger region.

![Fig.1. Chaotic attractor phase diagram](image-url)
2.3 Test the chaos of the chaotic system

The international standard NIST test is used to verify the randomness of the chaotic sequence generated by the laser chaotic system. Pre-set the initial value of the system and each parameter. We extract samples from the values generated by the chaotic system, perform corresponding tests on the series, and compare the results with international standards.

The NIST test contains two standards to measure the randomness of the sequence. The first method is to test the pass rate of random sequence samples and count the test results.

\[ \hat{s} = \frac{s(1-s)}{i}, \]  

where \( P = 1 - \alpha \), \( i \) represents the number of samples in this series of numbers. If the calculation result falls within the critical value of \( s \), it means that the chaotic system is very chaotic. Another equation (5)

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

This is an international test, a chaotic test of the random number sequence generated by the chaotic system. The evaluation results are given below. After comparing the results with international standards, it can be seen that the chaos of the system is very suitable for practical applications that require this feature.
Table 3. The randomness test result

<table>
<thead>
<tr>
<th>Test name</th>
<th>p-value\textsubscript{mean}</th>
<th>p-value\textsubscript{in}</th>
<th>Pass Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0.4845</td>
<td>0.5913</td>
<td>0.98</td>
</tr>
<tr>
<td>Block Frequency</td>
<td>0.5251</td>
<td>0.5433</td>
<td>0.97</td>
</tr>
<tr>
<td>Runs</td>
<td>0.5254</td>
<td>0.2489</td>
<td>1</td>
</tr>
<tr>
<td>Longest Run</td>
<td>0.6738</td>
<td>0.3578</td>
<td>1</td>
</tr>
<tr>
<td>FFT</td>
<td>0.4701</td>
<td>0.3186</td>
<td>1</td>
</tr>
<tr>
<td>Universal</td>
<td>0.4772</td>
<td>0.1456</td>
<td>0.99</td>
</tr>
<tr>
<td>Approximate Entropy</td>
<td>0.5197</td>
<td>0.4586</td>
<td>0.99</td>
</tr>
<tr>
<td>Linear Complexity</td>
<td>0.5123</td>
<td>0.3986</td>
<td>1</td>
</tr>
<tr>
<td>Non Overlapping Template</td>
<td>0.4934</td>
<td>0.3895</td>
<td>0.98</td>
</tr>
<tr>
<td>Overlapping Template</td>
<td>0.5186</td>
<td>0.3188</td>
<td>0.99</td>
</tr>
<tr>
<td>Cumulative Sums</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forward</td>
<td>0.5071</td>
<td>0.9558</td>
<td>1</td>
</tr>
<tr>
<td>Reverse</td>
<td>0.4627</td>
<td>0.9458</td>
<td>0.99</td>
</tr>
<tr>
<td>Serial</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forward</td>
<td>0.5265</td>
<td>0.4286</td>
<td>1</td>
</tr>
<tr>
<td>Reverse</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random Excursions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forward (x=\text{-}4)</td>
<td>0.3844</td>
<td>0.8728</td>
<td>0.9776</td>
</tr>
<tr>
<td>Forward (x=\text{-}3)</td>
<td>0.2798</td>
<td>0.5964</td>
<td>0.9776</td>
</tr>
<tr>
<td>Forward (x=\text{-}2)</td>
<td>0.2751</td>
<td>0.2279</td>
<td>0.9776</td>
</tr>
<tr>
<td>Forward (x=\text{-}1)</td>
<td>0.2721</td>
<td>0.6584</td>
<td>0.9833</td>
</tr>
<tr>
<td>Forward (x=1)</td>
<td>0.2639</td>
<td>0.4862</td>
<td>0.9811</td>
</tr>
<tr>
<td>Forward (x=2)</td>
<td>0.2946</td>
<td>0.1058</td>
<td>0.9777</td>
</tr>
<tr>
<td>Forward (x=3)</td>
<td>0.2778</td>
<td>0.3368</td>
<td>0.9814</td>
</tr>
<tr>
<td>Forward (x=4)</td>
<td>0.3301</td>
<td>0.0587</td>
<td>1</td>
</tr>
<tr>
<td>Test name</td>
<td>Test sequence x</td>
<td>p-value mean</td>
<td>p-value</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------</td>
<td>--------------</td>
<td>---------</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>-9</td>
<td>0.1987</td>
<td>0.2015</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>-8</td>
<td>0.3548</td>
<td>0.1950</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>-7</td>
<td>0.3578</td>
<td>0.4859</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>-6</td>
<td>0.3484</td>
<td>0.1056</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>-5</td>
<td>0.3587</td>
<td>0.1056</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>-4</td>
<td>0.3015</td>
<td>0.4584</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>-3</td>
<td>0.2954</td>
<td>0.6584</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>-2</td>
<td>0.3150</td>
<td>0.2189</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>-1</td>
<td>0.3018</td>
<td>0.4150</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>0</td>
<td>0.2979</td>
<td>0.4587</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>1</td>
<td>0.2916</td>
<td>0.1950</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>2</td>
<td>0.3254</td>
<td>0.1958</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>3</td>
<td>0.3589</td>
<td>0.1245</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>4</td>
<td>0.3152</td>
<td>0.4680</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>5</td>
<td>0.3114</td>
<td>0.3842</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>6</td>
<td>0.2986</td>
<td>0.6890</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>7</td>
<td>0.2956</td>
<td>0.7654</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>8</td>
<td>0.3015</td>
<td>0.4958</td>
</tr>
</tbody>
</table>

3. Image encryption and decryption scheme

3.1 Encryption method

The first part uses a three-dimensional fractional chaotic graph to generate a random chaotic sequence, which will interfere with channels of the image. The second part uses three-dimensional fractional chaos coupled with DNA coding operations to obtain a series of very chaotic numbers. The scrambled channel perform diffusion operations, that is, complement, addition, and mutation operations. Figure 3 shows the main encryption process.
The specific procedures we designed are listed here:

Step 1: The picture is decomposed into three primary colors and three pixel matrices. Set the key value and use the expression algorithm to calculate the new initial value conditions of the fractional three-dimensional chaotic system:

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

$$\begin{cases} x_0^' = x_0 + s \\ y_0^' = y_0 + s \\ z_0^' = z_0 + s \end{cases}$$  \hspace{1cm} (7)

Step 2: Set $L$. Subsequently, we stipulated that the setting of the disturbance step should be in accordance with the following standards:

$$\begin{cases} C_x = x \times 10^{16}, i \times z \\ C_y = y \times 10^{16}, i \times z \\ C_z = z \times 10^{16}, i \times z \end{cases}$$  \hspace{1cm} (8)
\[ k = \text{mod} \left[ \frac{1}{A_x(a,b)} Ax(a,b), A_y(a,b) \times A_y(a,b) + 1 \right] \times [a; b], [H; W] + [1; 1] \] (9)

Where: \( C_x, \quad C_y, \quad C_z \) are matrix replacement coefficients, \( k(1), k(2) \) are the coordinates of the obtained random exchange values.

Step 3: We stipulate that any point in the matrix must be moved, but the movement of each point is prescribed. Calculate the corresponding exchange points according to the equation, and exchange them one by one. The matrix is reconstructed to obtain the scrambled image matrix \( t_k \). Among them, the rules we designed for pixel disturbance are evolved from genetic principles. Including a series of numerical operations, double-chain collocation operations, and burst collocation operations. The specific arrangements are as follows

Step 4: Replace the scrambled matrix with binary, so that the resulting matrix is enlarged. Using the encryption rules specified in the previous article, the binary matrix is compiled from a matrix defined by genetic letters.

Step 5: Set the initial values of the chaotic system \( x_0, y_0, z_0 \) to obtain the chaotic sequence, then, by repeating \( (1) n + h \times w \) times, the first \( n \) values are discarded. equation (10)

\[
\begin{align*}
    a_1 &= \text{mod} \left( \left\lfloor \frac{x_1}{10^6} \right\rfloor, 256 \right) \\
    a_2 &= \text{mod} \left( \left\lfloor \frac{y_1}{10^6} \right\rfloor, 256 \right) \\
    a_3 &= \text{mod} \left( \left\lfloor \frac{z_1}{10^6} \right\rfloor, 256 \right)
\end{align*}
\] (10)

Step 6: Use the base substitution mutation rule in gene mutation to increase the randomness of image information encryption. The specific operation is that after the DNA diffusion operation, the value of each pixel has been expressed as an encrypted combination of four bases (such as ATCG), and the bases in each group are randomly exchanged. Get a new encrypted image pixel matrix \( C_1 \).

\[
\begin{align*}
    N(a,b) &= \begin{cases} 
    \text{T} \text{G} \text{A} & N(a,b) = (A), N(a,b+1) = (C), N(a,b+2) = (G) \\
    \text{A} \text{C} \text{G} & N(a,b) = (T), N(a,b+1) = (G), N(a,b+2) = (A)
    \end{cases}
\end{align*}
\] (11)

Step 7: Convert gene encoding matrix back to digital matrix

Step 8: Output the final finished image result to the finished process.
3.2 Decryption method

The decoding algorithm: First, reverse encoding, we use the calculation principle and gene double-strand operation principle specified in the previous article to change the encrypted information back to the gene letter sequence, and then use the encryption design to change the letter sequence back to the lion sequence, use the three-dimensional system to generate chaotic sequences and transform them into pseudo-random sequences to restore the scrambling steps of the encrypted image, obtain the original decrypted pixel matrix, and encode it into a digital matrix, and restore the original image through these three matrices.

Step 1: The encrypted image is still divided into three matrices according to the previous operation, and genetic coding is carried out according to the pre-set coding rules.

Step 2: Use gene mutation base substitution mutation to carry out reverse mutation change. Generate the encrypted matrix of the original DNA.

Step 3: Convert the chaotic sequence. Use subtraction to recover the DNA sequence that encrypts the image to obtain the encrypted diffusion sequence. Then, according to the predetermined base pair principle, the chaotic sequence generated by the chaotic system is also coded into a gene matrix using the coding rules.

Step 5: Reverse scrambling for reverse operation is performed, and the specific operation process is shown in the encryption process.

Step 6: The three primary color pixel matrixes restore the digital matrix, and the solved image is obtained through the three matrices.

4. Simulation and performance analysis

4.1 Algorithm simulation results

Verify the validity of the proposed cryptographic algorithm. 256x256 Lena images are used for algorithm testing. Set the parameters, initial values and levels of the fractional chaotic system. Based on the MATLAB platform, the corresponding experimental test results are shown in Figure 3.
Fig. 4. Encryption and decryption test (a) original image (b) encrypted image (c) decrypted image

4.2 Key space analysis

A good image encryption algorithm needs enough key space to resist brute force cracking. In our cryptography, the key space size corresponding to the key will be given. \( c, q, x_0, y_0, z_0 \) is about \( 2^{249} \), for the other parameter, because DNA has four kinds of acids and bases, the key space is \( 2^2 \times 2^6 \times 2^{20} = 2^{28} \). The key space of the proposed algorithm is \( 2^{277} \), therefore, the calculation method has enough space to resist brute force guessing attacks.

<table>
<thead>
<tr>
<th></th>
<th>Proposed algorithm</th>
<th>Chen’s [23]</th>
<th>Luo’s [31]</th>
<th>Li’s [33]</th>
<th>Shu’s [41]</th>
<th>Wang’s [46]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key space</td>
<td>2^{277}</td>
<td>2^{266}</td>
<td>2^{213}</td>
<td>2^{267}</td>
<td>2^{248}</td>
<td>2^{215}</td>
</tr>
</tbody>
</table>

4.3 Key sensitivity analysis

In this experiment, the keys \( (x_0+10^{-15}), (y_0+10^{-15}), (z_0+10^{-15}), (c+10^{-15}) \) of the decryption algorithm were changed, and then the encryption Table 6 shows the comparison results. We compare, and the comparison result clearly proves that the correctly decrypted image is very different from the decrypted result with slightly modified initial value, which proves that our design is very sensitive to the initial setting, and the similarity rate is less than 0.1%.
4.4 Statistical performance analysis

4.4.1 Histogram analysis

The histogram test is shown in the figure, and the experiment proves that the performance is good.
4.4.2 Image correlation coefficient

There is a strong correlation between adjacent pixels of the information it stores. The purpose of the image encryption algorithm to break the correlation between adjacent pixels. The calculation formula for judging the pixel correlation coefficient is:

\[ r_{xy} = \frac{\text{cov}(a,b)}{\sqrt{D(A)D(B)}}, \]  
\[ (12) \]
\[ \text{cov}(x, y) = E \{[x - \mu(x)][y - \mu(y)]\}, \]  
\[ (13) \]
\[ E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i, \]  
\[ (14) \]
\[ D(a) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(a))^2. \]  
\[ (15) \]

The table data shows that the original image has significant correlation, while the small correlation of the encrypted image indicates that the effect of the encryption algorithm meets the requirements.

In order to see more directly whether there is a correlation. Figure 7 shows the correlation distribution between the level of the Lena image and the adjacent pixels. The result proves that the surroundings of each pixel of the image before encryption are very related, which makes the encryption process full of difficulties. And the arrangement of the pixels is on the diagonal line. However, as shown in the second half of Figure 7, the pixel distribution of the encrypted image is very uniform and will not be counted, which greatly reduces the
relationship between different encrypted images in the encrypted image.

### Table 6. Correlation coefficients in R, G, B channels

<table>
<thead>
<tr>
<th>Channel</th>
<th>Direction</th>
<th>Plain image</th>
<th>Cipher image</th>
<th>Ref [7]</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>Horizontal</td>
<td>0.9556</td>
<td>0.0024</td>
<td>0.0095</td>
</tr>
<tr>
<td></td>
<td>Vertical</td>
<td>0.9780</td>
<td>6.3593×10⁻⁴</td>
<td>-0.0026</td>
</tr>
<tr>
<td></td>
<td>Diagonal</td>
<td>0.9434</td>
<td>-0.0010</td>
<td>0.0078</td>
</tr>
<tr>
<td>G</td>
<td>Horizontal</td>
<td>0.9443</td>
<td>0.0067</td>
<td>0.0183</td>
</tr>
<tr>
<td></td>
<td>Vertical</td>
<td>0.9711</td>
<td>2.8685×10⁻⁴</td>
<td>0.0001</td>
</tr>
<tr>
<td></td>
<td>Diagonal</td>
<td>0.9301</td>
<td>-9.3236×10⁻⁴</td>
<td>-0.0039</td>
</tr>
<tr>
<td>B</td>
<td>Horizontal</td>
<td>0.9280</td>
<td>-8.7964×10⁻⁴</td>
<td>0.0034</td>
</tr>
<tr>
<td></td>
<td>Vertical</td>
<td>0.9575</td>
<td>3.9657×10⁻⁴</td>
<td>-0.0035</td>
</tr>
<tr>
<td></td>
<td>Diagonal</td>
<td>0.9093</td>
<td>0.0044</td>
<td>0.0052</td>
</tr>
</tbody>
</table>

**Fig. 7.** The correlation coefficient analysis: (a) “Lenna” image (b) “Fruits” image (c) “Flowers” image (d) “Pepper” image

### 4.5 Information entropy

We often use this characteristic value to judge whether the information is chaotic. We take the average of the average chaos of the input information. As shown in Eq. (16):
\[ H(m) = \sum_{i=1}^{L-1} I(m_i) \times \log \frac{1}{I(m_i)}. \]  

(16)

where, \( I(m_i) \) is the probability of \( m_i \) appearing, \( L \) is the number of statistical feature points \( m_i \).

Table 10 shows the average information entropy of each image, and the test value of the new algorithm meets the theoretical requirements. This result shows that the obtained image has completely lost the possibility of discrimination, and its information entropy is very close to the theoretical value. The results show that the encrypted image can be approximately regarded as a random image. This proves the superiority of the algorithm.

<table>
<thead>
<tr>
<th>Image name</th>
<th>Information entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>7.9972</td>
</tr>
</tbody>
</table>

Table 8. information entropy

<table>
<thead>
<tr>
<th>Encryption scheme</th>
<th>IE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed scheme</td>
<td>7.9975</td>
</tr>
<tr>
<td>Liu’s [5]</td>
<td>7.9964</td>
</tr>
<tr>
<td>Li’s [19]</td>
<td>7.9973</td>
</tr>
<tr>
<td>Sun’s [30]</td>
<td>7.9967</td>
</tr>
<tr>
<td>Liu’s [47]</td>
<td>7.9971</td>
</tr>
<tr>
<td>Yang’s [48]</td>
<td>7.9981</td>
</tr>
</tbody>
</table>

Table 9. Another scheme

4.6 Differential attack analysis

In order to verify the sensitivity of the ciphertext to the plaintext, we use differential attacks to test. Usually, two standards, pixel change rate (NPCR) and uniform average change rate (UACI), are commonly used to judge the performance of encryption algorithms.

The values of NPCR and UACI values are calculated by:

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

(17)
\[ UCAI = \frac{1}{L} \sum_{i,j=1}^{L} \frac{|I(i,j)-I_0(i,j)|}{255} \times 100\%. \]  
(18)

\[ D(x,y) = \begin{cases} 1 & C(x,y) \neq C(x,y) \\ 0 & C(x,y) = C(x,y) \end{cases}. \]  
(19)

We use the following two reference values to distinguish the performance of the system. One of the criteria for judging is as follows:

\[ N^*_{\alpha} = \frac{F - \Phi^{-1}(\alpha) \sqrt{F / L}}{F + 1}. \]  
(20)

The UCAI thresholds \((U^-_{\alpha}, U^+_{\alpha})\) are obtained as

\[ \begin{cases} D^-_{\alpha} = \mu_a - c^{-1}(\alpha / 2)b_u \\ D^+_{\alpha} = \mu_a + c^{-1}(\alpha / 2)b_u \end{cases}. \]  
(21)

We analyze this algorithm from the perspective of three-color pixels, and the results obtained are averaged to show the advantages of the system. The results are obtained by comparing with other algorithms. A detailed comparison is given in Table 10.11.12, which proves that the algorithm has classic information theory security and good performance beyond classic image encryption algorithms.

<table>
<thead>
<tr>
<th>Image name</th>
<th>NPCR (mean)</th>
<th>Eligibility boundary</th>
<th>Critical Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>99.67%</td>
<td>effective</td>
<td>effective</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(D^-_{\alpha} = 99.5963%)</td>
<td>(D^+_{\alpha} = 99.5527%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Image name</th>
<th>UCAI (mean)</th>
<th>Critical Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>33.45%</td>
<td>effective</td>
</tr>
<tr>
<td></td>
<td></td>
<td>effective</td>
</tr>
</tbody>
</table>

4.7 Anti-noise attack performance analysis

The intensity of 0.05, 0.06, 0.07 Gaussian noise was added in the encryption process. And decrypt the contaminated image, the experimental results are shown in Figure 8. The test results prove that the algorithm has the ability to resist noise pollution.
Table 12. compare with another scheme (Take Lena image as an example)

<table>
<thead>
<tr>
<th>Encryption scheme</th>
<th>NPCR</th>
<th>UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed scheme</td>
<td>99.67%</td>
<td>33.45%</td>
</tr>
<tr>
<td>Liu’s [5]</td>
<td>99.62%</td>
<td>33.38%</td>
</tr>
<tr>
<td>Khwvana’s [18]</td>
<td>99.64%</td>
<td>33.46%</td>
</tr>
<tr>
<td>Luo’s [31]</td>
<td>99.63%</td>
<td>33.42%</td>
</tr>
<tr>
<td>Sun’s [30]</td>
<td>99.61%</td>
<td>33.45%</td>
</tr>
<tr>
<td>Yang’s [48]</td>
<td>99.61%</td>
<td>33.44%</td>
</tr>
</tbody>
</table>

Fig.8. Anti-pollution attack test.

5. Conclusion

We analyzed the dynamic characteristics of the simplified unified system based on the 3D fractional scale of the ADM algorithm. The data showed that the chaotic system has very good advantages, and we used his principle in the practical application of encrypted images, which indicates that they are suitable for chaotic cipher systems. In this paper, we propose a new image encryption method using fractional chaotic system. This paper analyzes the security of the encryption algorithm, and applies the fractional simplified unified system and the principle of DNA mutation to the image encryption algorithm. Need to be improv. It provides a theoretical and practical basis for cryptography confidential communication and information security.

References


[18] Khurana M, Singh H. Two level phase retrieval in fractional Hartley domain for secure image


[34] Bukharmetov M, Nyrkov A, Sokolov S, et al. Robust Method for Protecting Electronic


