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

EAI GreeNets 2021, June 06-07, Dalian, People's Republic of China

DOI 10.4108/eai.6-6-2021.2308045

algorithms.[1-6] .

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]. INnubushi 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.

Table 1 The law of encoding

rule	1	2	3	4	5	6	7	8
00	A	A	T	T	G	G	C	C
01	C	G	C	G	T	A	T	A
10	G	C	G	C	A	T	A	T
11	T	T	A	A	C	C	G	G

Table 2 Addition and Subtraction rules

+	A	C	G	T	-	A	C	G	T
A	A	C	G	T	A	A	T	G	C
C	C	G	T	A	C	C	A	T	G
G	G	T	A	C	G	G	C	A	T
T	T	A	C	G	T	T	G	C	A

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.

$$\begin{cases} a_i \neq S(a_i) \neq S\left(S(a_i)\right) \neq S\left(S\left(S(a_i)\right)\right) \\ a_i = S\left(S\left(S\left(S(a_i)\right)\right)\right) \end{cases} \tag{1}$$

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

$$\begin{aligned} &(1)\,L1\,(A)=T,\ L1\,(T)=T,\ L1\,(C)=G,\ L1\,(G)=A; \\ &(1)\,L2\,(A)=T,\ L2\,(T)=T,\ L2\,(G)=C,\ L2\,(C)=A; \\ &(1)\,L3\,(A)=C,\ L3\,(C)=T,\ L3\,(T)=G,\ L3\,(G)=A; \\ &(1)\,L4\,(A)=C,\ L4\,(C)=T,\ L4\,(G)=T,\ L4\,(T)=A; \\ &(1)\,L5\,(A)=G,\ L5\,(G)=T,\ L5\,(T)=C,\ L5\,(C)=A; \\ &(1)\,L6\,(A)=G,\ L6\,(G)=T,\ L6\,(C)=T,\ L6\,(T)=A; \end{aligned} \tag{2}$$

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

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.

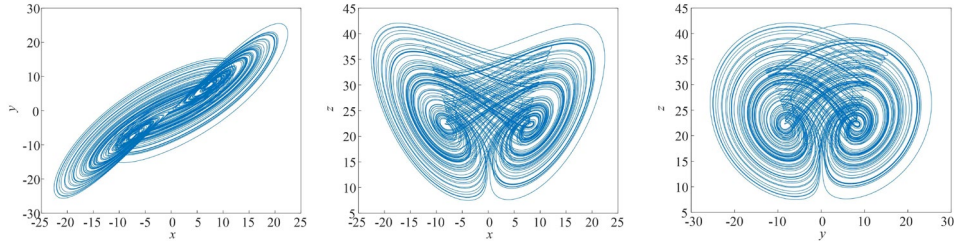
2.2 Dynamic analysis

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

$$\begin{cases} T_t^q x_1 = (25c+10)(x_2 - x_1) \\ T_t^q x_2 = (27-6c)x_2 - x_1 x_3 \\ T_t^q x_3 = x_1 x_2 - (8+c)x_3 / 3 \end{cases} \tag{3}$$

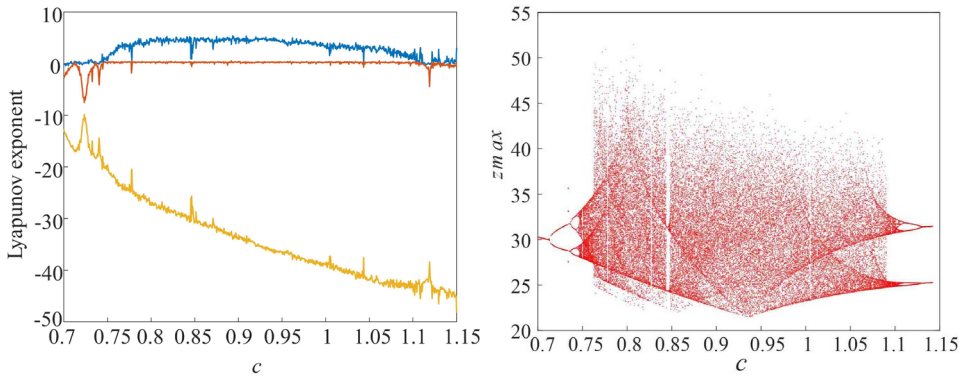
Let the system parameters c=0.9, q=0.9, the time step is t=0.001s, and the system initial value $[x_0, y_0, z_0]$ = [0.1,0.2,0.3]. At this time, the chaotic attractor phase diagram of the system is shown in Figure 1. At the same time, the Lyapunov index (L_1, L_2, L_3) = (5.0824, 0, -3.9031) can be calculated. 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.



(a)x-y plane (b)x-z plane (c)y-z plane

Fig.1. Chaotic attractor phase diagram



(a) (b)

Fig. 2. Dynamical properties analysis of quantum logistic system ($c \in [0.7,1.15]$)

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.

$$\hat{s} = \sqrt{\frac{\hat{s}(1-\hat{s})}{i}}, \tag{4}$$

where P=1-α, 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)

$$x^2 = \sum_{i=1}^{10} \frac{(Fi - 0.1s)^2}{0.1s}, \tag{5}$$

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

Test name		Test sequence x		
		$p\text{-value}_{mean}$	$p\text{-value}_T$	Pass Rate
Frequency		0.4845	0.5913	0.98
Block Frequency		0.5251	0.5433	0.97
Runs		0.5254	0.2489	1
Longest Run		0.6738	0.3578	1
FFT		0.4701	0.3186	1
Universal		0.4772	0.1456	0.99
Approximate Entropy		0.5197	0.4586	0.99
Linear Complexity		0.5123	0.3986	1
Non Overlapping Template		0.4934	0.3895	0.98
Overlapping Template		0.5186	0.3188	0.99
Cumulative Sums	Forward	0.5071	0.9558	1
	Reverse	0.4627	0.9458	0.99
Serial	p-value[1]	0.4903	0.4980	0.99
	p-value[2]	0.5265	0.4286	1
Random Excursions	x=-4	0.3844	0.8728	0.9776
	x=-3	0.2798	0.5964	0.9776
	x=-2	0.2751	0.2279	0.9776
	x=-1	0.2721	0.6584	0.9833
	x=1	0.2639	0.4862	0.9811
	x=2	0.2946	0.1058	0.9777
	x=3	0.2778	0.3368	0.9814
	x=4	0.3301	0.0587	1

Table 4. Random excursions variant

Test name		Test sequence x		
		p-value$_{mean}$	p-value$_T$	Pass Rate
Random excursions variant	x=-9	0.1987	0.2015	1
	x=-8	0.3548	0.1950	1
	x=-7	0.3578	0.4859	0.9667
	x=-6	0.3484	0.1056	1
	x=-5	0.3587	0.1056	1
	x=-4	0.3015	0.4584	1
	x=-3	0.2954	0.6584	1
	x=-2	0.3150	0.2189	0.98
	x=-1	0.3018	0.4150	0.9867
	x=1	0.2979	0.4587	0.99
	x=2	0.2916	0.1950	0.99
	x=3	0.3254	0.1958	0.99
	x=4	0.3589	0.1245	1
	x=5	0.3152	0.4680	1
	x=6	0.3114	0.3842	1
	x=7	0.2986	0.6890	0.9667
	x=8	0.2956	0.7654	0.9866
	x=9	0.3015	0.4958	0.9866

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.

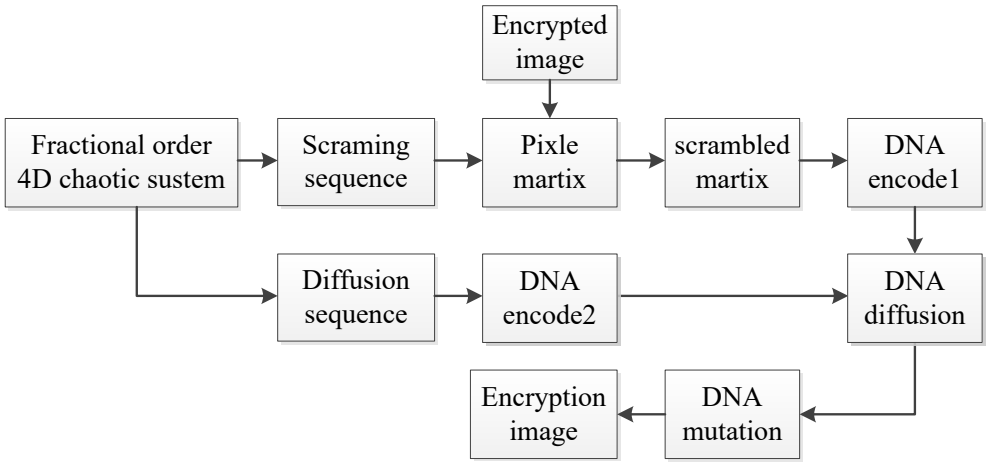


Fig.3. The architecture of encryption algorithm

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:

$$s=\frac{\sum_{i=1}^{H} I(i,j)}{10^{10}} \tag{6}$$

$$\begin{cases} x_0^{'} = x_0 + s \\ y_0^{'} = y_0 + s \\ z_0^{'} = z_0 + s \end{cases} \tag{7}$$

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

$$\begin{cases} Cx=\mathrm{x}\times 10^{16},\mathrm{i}\times\mathrm{z} \\ Cy=\mathrm{y}\times 10^{16},\mathrm{i}\times\mathrm{z} \\ Cz=\mathrm{z}\times 10^{16},\mathrm{i}\times\mathrm{z} \end{cases} \tag{8}$$

$$\mathrm{k}=\mathrm{mod}\left(\begin{bmatrix} 1 & Ax(a,b) \\ Ay(a,b) & Ax(a,b)\times Ay(a,b)+1 \end{bmatrix}\times[a;b],[H;W]+[1;1]\right) \quad (9)$$

Where: C_x,, C_y, 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 tk. 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)

$$\begin{cases} a_1 = \mathrm{mod}\left(\left(\left\lfloor |x_i| \right\rfloor\right)\times 10^{16}, 256\right) \\ a_2 = \mathrm{mod}\left(\left(\left\lfloor |y_i| \right\rfloor\right)\times 10^{16}, 256\right) \\ a_3 = \mathrm{mod}\left(\left(\left\lfloor |z_i| \right\rfloor\right)\times 10^{16}, 256\right) \end{cases} \quad (10)$$

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.

$$N(a,b)=\begin{cases} TGA & N(a,b)=(A), N(a,b+1)=(C), N(a,b+2)=(G) \\ ACG & N(a,b)=(T), N(a,b+1)=(G), N(a,b+2)=(A) \end{cases}$$

(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.

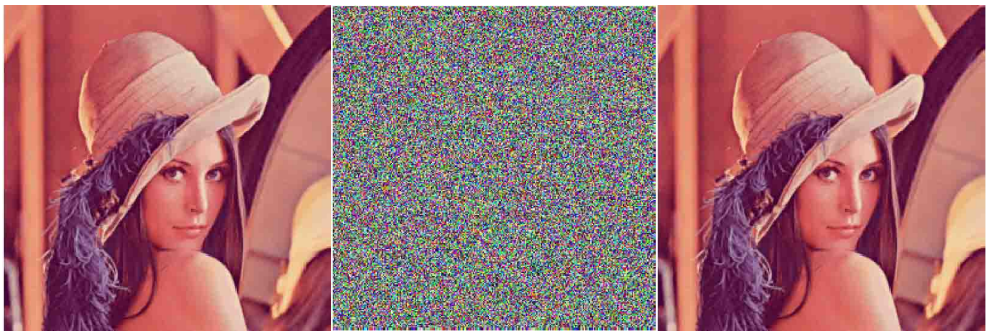
Step 5: Reverse scrambling for reverse operation is performed, and the specific operation process is shown in the encryption process.

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.



(a) (b) (c)

Fig.4. Encryption and decryption test (a)original image (b)encrypted image (c)decrypt the 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 $2^2\times2^6\times2^{20}=2^{28}$. The key space of the proposed algorithm is 2^{277}, therefore, the calculation method has enough space to resist brute force guessing attacks.

Table 5. Table of key space

	Proposed algorithm	Chen's [23]	Luo's [31]	Li's [33]	Shu's [41]	Wang's [46]
Key space	2^{277}	2^{266}	2^{213}	2^{267}	2^{248}	2^{215}

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%.

(a) (b)

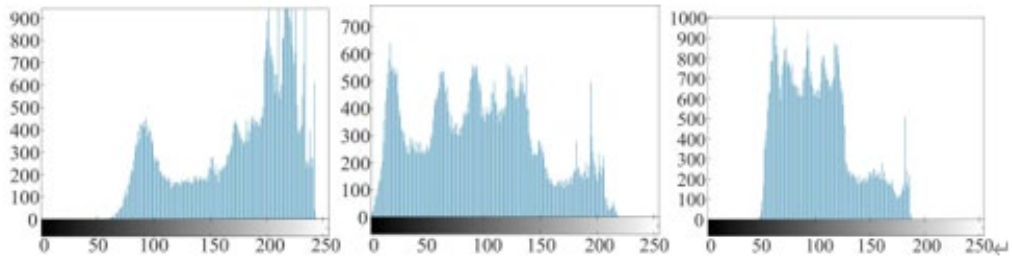
(b) (d)

Fig.5. Sensitivity to initial value (a) Decrypt the complete image (b) x_0+10^{-15} (c) y_0+10^{-15} (d) z_0+10^{-15}

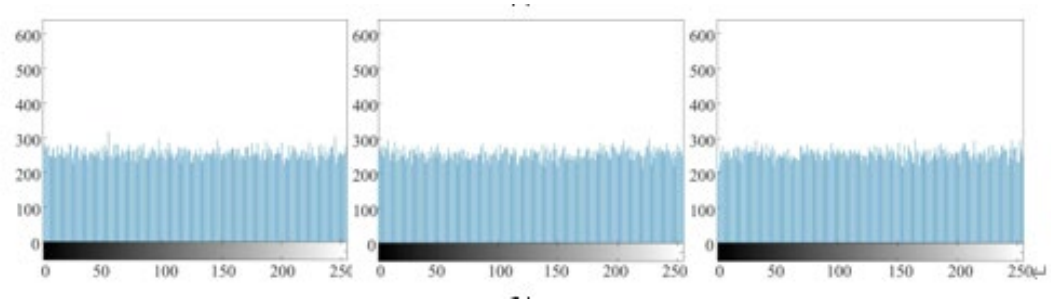
4.4 Statistical performance analysis

4.4.1 Histogram analysis

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



(a)



(b)

Fig.6. Histogram analysis results (a)plain image (b)permuted image

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:

$$r_{xy} = \frac{\operatorname{cov}(a,b)}{\sqrt{D(A)D(B)}}, \tag{12}$$

$$\operatorname{cov}(x,y) = E\left\{\left[\mathrm{x} - d(x)\right]\left[y - D(x)\right]\right\}, \tag{13}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{14}$$

$$D(a) = \frac{1}{N}\sum_{i=1}^{N}\left[x_i - E(a)\right]^2. \tag{15}$$

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

Channel	Direction	Plain image	Cipher image	Ref [7]
R Channel	Horizontal	0.9556	0.0024	0.0095
	Vertical	0.9780	6.3593×10^{-4}	-0.0026
	Diagonal	0.9434	-0.0010	0.0078
G Channel	Horizontal	0.9443	0.0067	0.0183
	Vertical	0.9711	2.8685×10^{-4}	0.0001
	Diagonal	0.9301	-9.3236×10^{-4}	-0.0039
B Channel	Horizontal	0.9280	-8.7964×10^{-4}	0.0034
	Vertical	0.9575	3.9657×10^{-4}	-0.0035
	Diagonal	0.9093	0.0044	0.0052

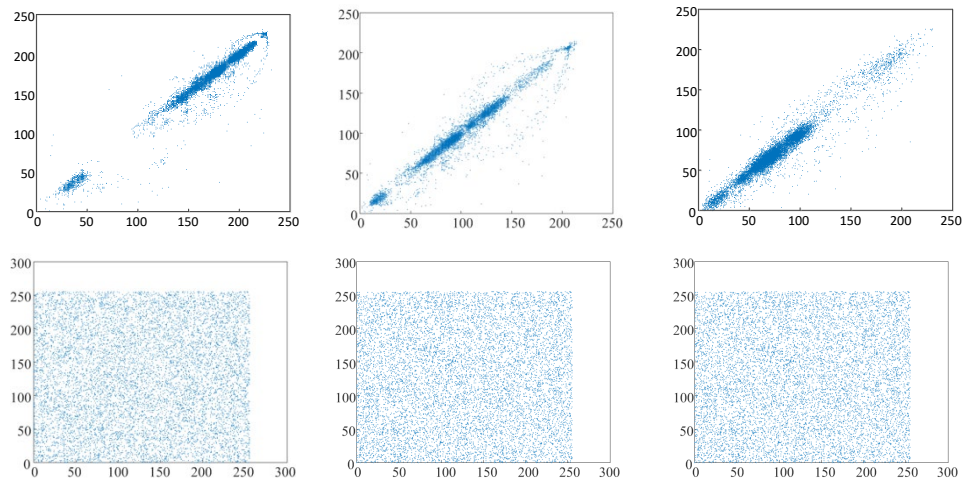


Fig.7. The correlation coefficient analysis: (a) “Lenna” image (b) “Fruits” image (c) “Flowers” image (d) “Pepper” image

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):

$$H(m)=\sum_{i=1}^{L-1} I(m_i)\times\log\frac{1}{I(m_i)}. \tag{16}$$

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 his 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 8. information entropy

Image name	Information entropy
Lena	7.9972

Table 9. Another scheme

Encryption scheme	IE
Proposed scheme	7.9975
Liu's [5]	7.9964
Li's [19]	7.9973
Sun's [30]	7.9967
Liu's [47]	7.9971
Yang's [48]	7.9981

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:

$$NPCR=\frac{\sum_{j=1}^{L} E(i,j)}{L}\times 100\%, \tag{17}$$

$$UCAI = \frac{1}{L}\sum_{\substack{i=1\\j=1}}^{L}\frac{I(i,j)-I_1(i,j)}{255}\times 100\%. \tag{18}$$

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

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

$$N_{\alpha}^{*}=\frac{F-\Phi^{-1}(\alpha)\sqrt{F/L}}{F+1}. \tag{20}$$

The UCAI thresholds (U_{α}^{*-}, U_{α}^{*+}) are obtained as

$$\begin{cases}D_{\alpha}^{*-}=\mu_u-c^{-1}(a/2)b_u\\ D_{\alpha}^{*+}=\mu_u+c^{-1}(a/2)b_u\end{cases}, \tag{21}$$

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 10. NPCR Values

Image name	NPCR (mean)	Eligibility boundary $D_{0.05}^{*-}$=99.5963%	$D_{0.01}^{*-}$=99.5527%	$D_{0.001}^{*-}$=99.5341%
Lena	99.67%	effective	effective	effective

Table 11.UACI Values

Image name	UCAI (mean)	Critical Value		
Lena	33.45%	effective	effective	effective

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)

Encryption scheme	NPCR	UACI
Proposed scheme	99.67%	33.45%
Liu's [5]	99.62%	33.38%
Khwvana's [18]	99.64%	33.46%
Luo's [31]	99.63%	33.42%
Sun's [30]	99.61%	33.45%
Yang's [48]	99.61%	33.44%

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

[1] Lai Q, Kuate P D K, Liu F, et al. An Extremely Simple Chaotic System with Infinitely Many Coexisting Attractors[J]. Circuits and Systems II: Express Briefs, IEEE Transactions on, 2019, PP(99):

1-1.

[2] Lai Q, Wan Z, Kuate P D K, et al. Coexisting attractors, circuit implementation and synchronization control of a new chaotic system evolved from the simplest memristor chaotic circuit[J]. Communications in Nonlinear ence and Numerical Simulation, 2020: 105341.

[3] Murillo-Escobar M A, Cruz-Hernández C, Abundiz-Pérez F, et al. A RGB image encryption algorithm based on total plain image characteristics and chaos[J]. Signal Processing, 2015, 109: 119-131.

[4] Hikal N A, Eid M M. A new approach for palmprint image encryption based on hybrid chaotic maps[J]. Journal of King Saud University - Computer and Information Sciences, 2018.

[5] Liu H, Nan H. Color image security system using chaos-based cyclic shift and multiple-order discrete fractional cosine transform[J]. Optics & Laser Technology, 2013, 50: 1-7.

[6] Chen X, Hu C J. Adaptive medical image encryption algorithm based on multiple chaotic mapping[J]. Saudi J Biol Sci, 2017, 24(8): 1821-1827.

[7] Yang F, Mou J, Luo C, et al. An improved color image encryption scheme and cryptanalysis based on a hyperchaotic sequence[J]. Physica Scripta, 2019, 94(8): 085206.

[8] Wang Y, Chang Y, Wu Q, et al. Fuzzy model of hyperchaotic laser systems with parameters perturbation[J]. High Power Laser & Particle Beams, 2012, 24(09): 2063-2067.

[9] Glushkov A V, Buyadzhi V V, Kvasikova A S, et al. Non-Linear Chaotic Dynamics of Quantum Systems: Molecules in an Electromagnetic Field and Laser Systems[J], 2017.

[10] Zhang L W, Shao M. Chaotic Synchronization with Single-Ring Erbium-Doped Fiber Laser Systems[C]. International Conference on Computational Intelligence & Security, 2010.

[11] Louis, M., Pecora, et al. Synchronization of chaotic systems[J]. Chaos An Interdisciplinary Journal of Nonlinea, 2015.

[12] Rosenbluh M, Aviad Y, Cohen E, et al. Spiking Optical Patterns and Synchronization[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2007, 76(4 Pt 2).

[13] Stoffels E, Kieft I E, Sladek R E J, et al. Plasma needle for in vivo medical treatment: recent developments and perspectives[J]. Plasma Sources Ence & Technology, 2006, 15(4): S169.

[14] Chen H K. Global chaos synchronization of new chaotic systems via nonlinear control[J]. Chaos Solitons & Fractals, 2005, 23(4): 1245-1251.

[15] Yassen M T. Chaos synchronization between two different chaotic systems using active control[J]. Chaos Solitons & Fractals, 2005, 23(1): 131-140.

[16] Inubushi M, Yoshimura K, Arai K, et al. Physical random bit generators and their reliability: focusing on chaotic laser systems[J]. Nonlinear Theory & Its Applications Ieice, 2015, 6(2): 133-143.

[17] Natiq H, Said M R M, Al-Saidi N M G, et al. Dynamics and Complexity of a New 4D Chaotic Laser System[J]. Entropy, 2019, 21(1): 34.

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

encryption and authentication using digital signatures[J]. Multimedia Tools and Applications, 2019, (3).

[19] Li P, Xu J, Mou J, et al. Fractional-order 4D hyperchaotic memristive system and application in color image encryption[J]. EURASIP Journal on Image and Video Processing, 2019, 2019(1).

[20] Vilardy J M, Torres C O, Jimenez C. Fractional convolution and nonlinear operations applied to the image encryption[J]. Journal of Physics Conference, 2019.

[21] Li G-D, Wang L-L. Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform[J]. Visual Computer, 2019, 35(9): 1267-1277.

[22] Chen L, Hao Y, Huang T, et al. Chaos in fractional-order discrete neural networks with application to image encryption[J]. Neural Networks, 2020, 125: 174-184.

[23] Chen G, Mao Y, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals, 2004, 21(3): 749-761.

[24] Zhou N, Wang Y, Gong L. A Novel Scheme of Image Encryption Based on Synchronization of Fractional Order Chaotic Systems[J]. Optics Communications, 2011, 284(13): 3234-3242.

[25] Sajasi S, Eftekhari Moghadam A-M. An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method[J]. Applied Soft Computing, 2015, 30: 375-389.

[26] Wang X-Y, Zhang Y-Q, Zhao Y-Y. A novel image encryption scheme based on 2-D logistic map and DNA sequence operations[J]. Nonlinear Dynamics, 2015, 82(3): 1269-1280.

[27] Chai X, Gan Z, Lu Y, et al. A novel image encryption algorithm based on the chaotic system and DNA computing[J]. International Journal of Modern Physics C, 2017, 28(05): 1750069.

[28] Zhang L-M, Sun K-H, Liu W-H, et al. A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations[J]. Chinese Physics B, 2017, 26(10): 100504.

[29] Xu B, Wang G, Iu H H-C, et al. A memristor–meminductor-based chaotic system with abundant dynamical behaviors[J]. Nonlinear Dynamics, 2019, 96(1): 765-788.

[30] Suryadi M T, Satria Y, Fauzi M. Implementation of digital image encryption algorithm using logistic function and DNA encoding[J]. Journal of Physics: Conference Series, 2018, 974: 012028.

[31] Luo Y, Du M, Liu J. A symmetrical image encryption scheme in wavelet and time domain[J]. Communications in Nonlinear Science and Numerical Simulation, 2015, 20(2): 447-460.

[32] Silva-García V M, Flores-Carapia R, Rentería-Márquez C, et al. Substitution box generation using Chaos: An image encryption application[J]. Applied Mathematics and Computation, 2018, 332: 123-135.

[33] Li X, Zhou C, Xu N. A secure and efficient Image encryption algorithm based on DNA coding and spatiotemporal chaos[J]. International Journal of Network Security, 2018, 20: 110-120.

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

Document on Waterway Transport with Steganographic Means by Embedding Digital Watermarks into Images[J]. Procedia Engineering, 2017, 178: 507-514.

[35] Qin Y, Wang Z, Wang H, et al. Robust information encryption diffractive-imaging-based scheme with special phase retrieval algorithm for a customized data container[J]. Optics and Lasers in Engineering, 2018, 105: 118-124.

[36] Zhang S, Liu H, Li S. Robust adaptive control for fractional-order chaotic systems with system uncertainties and external disturbances[J]. Advances in Difference Equations, 2018, 2018(1).

[37] Farwa S, Muhammad N, Bibi N, et al. RETRACTED: Fresnelet approach for image encryption in the algebraic frame[J]. Applied Mathematics and Computation, 2018, 334: 343-355.

[38] Khan A, Bhat M A. Projective synchronization via feedback controller of fractional-order chaotic systems[J]. International Journal of Modelling and Simulation, 2019, (4): 1-9.

[39] Peng Y, Sun K, He S, et al. Parameter Identification of Fractional-Order Discrete Chaotic Systems[J]. Entropy, 2019, 21(1): 27.

[40] Khennaoui A-A, Ouannas A, Bendoukha S, et al. On fractional–order discrete–time systems: Chaos, stabilization and synchronization[J]. Chaos, Solitons & Fractals, 2019, 119: 150-162.

[41] Shukla M K, Siva D, Mahajan A, et al. A Novel Scheme of Image Encryption Based on Synchronization of Fractional Order Chaotic Systems[C]. 2018 International Conference on Intelligent Circuits and Systems (ICICS), 2018.

[42] Sun S. A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling[J]. IEEE Photonics Journal, 2018, 10(2): 1-14.

[43] Wang X, Li P, Zhang Y. A novel color image encryption scheme using DNA permutation based on the Lorenz system[J]. CrossMark, 2018, 77: 6243-6265.

[44] Ye X, Wang X, Gao S, et al. A new chaotic circuit with multiple memristors and its application in image encryption[J]. Nonlinear Dynamics, 2019.

[45] Chen C, Sun K, He S. An improved image encryption algorithm with finite computing precision[J]. Signal Processing, 2020, 168: 107340.

[46] Wang X, Zhang Y, Zhao Y. A novel image encryption scheme based on 2-D logistic map and DNA sequence operations[J]. CrossMark, 2015, 82: 1269-1280.

[47] Liu W, Sun K, He Y, et al. Color Image Encryption Using Three-Dimensional Sine ICMIC Modulation Map and DNA Sequence Operations[J]. International Journal of Bifurcation and Chaos, 2017, 27(11): 1750171.

[48] Yang F, Mou J, Ma C, et al. Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application[J]. Optics and Lasers in Engineering, 2020, 129: 106031.