A novel colour image encryption based on fractional order Lorenz system

Shixu Li, Yongjin Yu, Xingquan Ji and Qi Sun

College of Electrical Engineering and Automation, Shandong University of Science and Technology, People’s Republic of China

ABSTRACT
A colour image encryption algorithm based on fractional Lorenz system has been developed in this paper. Firstly, the colour image has been divided into three layers: R, G, and B, and Arnold map has been used for scrambling the three layers separately, and the plaintext pixel has been selected as the scrambling parameter. The Tent map has been used to associate the plain text to generate the initial values of the fractional Lorenz system, which has been iterated by the system to generate a pseudo-random sequence that can be used for two pixel diffusions. The first pixel diffusion is to diffuse the pixels of each layer to the other two layers, and the second pixel diffusion is to add modulus diffusion inside the layer. Simulation results illustrate that the plaintext image is encrypted into a meaningless noise image. The superior performance of proposed algorithm has been proved by the key space analysis, histogram analysis, correlation test, sensitivity analysis and information entropy analysis, and it can resist various common attack methods.

1. Introduction
In recent years, with the continuous development of science and technology, information communication methods and transmission channels are also increasingly rich, information security has become an important issue. But image information, as a kind of special data, are transmitted through the Internet in the form of plaintext, and its security needs to be solved urgently. In order to prevent the image information from being stolen, tampered and intercepted during transmission, it is necessary to encrypt it to a certain extent. At present, the common data encryption algorithms include symmetric algorithms such as AES, DES and asymmetric algorithms such as RSA. The commonly used encryption protocol in the Internet is TLS, which is used in the HTTPS communication protocol. These algorithms are widely used, but the image information is a kind of information with large amount of data, strong correlation and high redundancy. It is necessary to design a targeted encryption algorithm based on these characteristics of the image information.

Chaotic systems are characterized by unpredictability, pseudo-randomness and sensitivity to initial conditions, so they have unique advantages in generating pseudo-random sequences and transforming images (Simin et al., 2013). Since J. Fridrich proposed the image cryptosystem for chaotic systems in 1998 (Jiri, 1998), in the application of chaotic systems to image encryption, the pseudo-random sequence generated by chaotic systems has become the mainstream of chaotic system encryption. When chaotic image encryption algorithm into the mature period, plaintext correlation encryption algorithm had become the focus of work. For example, Zhang W et al proposed an encryption algorithm that optimized the diffusion process with associating plaintext image, so that different ciphers can be generated when the same key was used to encrypt different images (Zhang et al., 2013). Zhang Y et al proposed a plaintext associated two-level key chaotic image encryption algorithm. Different chaotic sequences can be generated for different plaintext images, but the algorithm is too complex to influence encryption efficiency (Zhang Yong, 2016b; Zhang, 2014; Zhang et al., 2012). In recent years, colour image has become a mainstream research object. For example, a colour image encryption algorithm based on ‘scrambling-diffusing-scrambling’ was proposed by Liu et al. (2016) and Niyat et al. (2017), which divided the colour image into different layers and generates different encryption sequences for encryption respectively. Nowadays, more and more scholars have applied DNA coding to image encryption algorithms. Both Guesmi et al. (2016) and Jiyun and Hao (2018) proposed using dynamic DNA coding to scramble images. And a fast image encryption scheme with block permutation and block diffusion was introduced in 2017 (Chai et al., 2017). In 2019, a novel
chaotic image encryption algorithm based on a content-sensitive dynamic function switching mechanism was proposed by Yavuz (2019).

However, this method does not carry out diffusion or scrambling between layers, so it is at risk of suffering from chosen-plaintext attack. With the development of nonlinear theory, fractional order chaotic systems have become a research hotspot due to their rich dynamic characteristics. In fact, fractional order systems can better describe natural phenomena than integer orders systems (Kehui, 2015). Therefore, it is of great practical significance to design an image encryption algorithm using fractional order chaotic system.

In this essay, a plaintext related colour image encryption algorithm based on fractional order chaotic system was proposed. Firstly, the plaintext image was expanded into a one-dimensional vector from top to bottom and from left to right. The Tent map was used to select the plaintext pixel points to generate chaotic sequence as the initial value of the fractional order Lorenz system. Then, the colour plain image was divided into three layers of RGB. R layer was scrambled by Arnold map. G layer was scrambled by Arnold map whose parameters was determined by the scrambled R layer. And the B layer was operated with the same way. Aimed at the insufficient diffusion in (Liu et al., 2016) and (Niyat et al., 2017), the chaotic sequence generated by the fractional Lorenz system was converted into a password for diffusion. In the diffusion process, the RGB three layers were cross-diffused so that the information of this layer was diffused to the other two layers. After that, the RGB layer was diffused twice to spread the information of each pixel to other pixels. Encrypted with the simulation experiment and result analysis, the plaintext image had been encrypted adequately, There was no useful information can be obtained from cipher text images. Finally, our algorithm was proved to resist various common attack means and have high security through analyzing the key space, histogram, correlation coefficient and NPCR, UACI.

The rest of this paper is organized as follows. Section 2 introduces three chaotic systems, and characters of the fractional order Lorenz system are analyzed. A colour image encryption algorithm based on fractional Lorenz system is developed in section 3. Section 4 carries on the simulation that the plaintext image is encrypted and decrypted with error key. The encryption effect of our algorithm is analyzed in section 5. Finally, conclusions drawn from the study are given in the section 6.

2. Several chaotic systems

2.1. Arnold map

Arnold map, also called cat map is a nonlinear 2D map, the Arnold map is defined as

\[
\begin{pmatrix}
    x_{n+1} \\
    y_{n+1}
\end{pmatrix} = \begin{pmatrix}
    1 & a \\
    b & ab + 1
\end{pmatrix} \begin{pmatrix}
    x_n \\
    y_n
\end{pmatrix} \mod 1
\] (1)

where \(a\) and \(b\) are real numbers, \(x_n, y_n \in [0, 1)\).

Arnold map is often used in scrambling process of image encryption, in which \(x_n, y_n\) represents pixel position of original image, \(x_{n+1}, y_{n+1}\) represents pixel position of scrambled image. But the generalized Arnold map is not efficient, so an optimized Arnold map scrambling method is introduced (Zhang Yong, 2016a).

\[
\begin{pmatrix}
    p \\
    q
\end{pmatrix} = \begin{pmatrix}
    1 & a \\
    b & ab + 1
\end{pmatrix} \begin{pmatrix}
    1 \\
    j
\end{pmatrix}
\] (2)

In this way, the position of pixel (1,j) and pixel (1,q) can be exchanged.

2.2. Tent map

The Tent map is defined as

\[
x_{n+1} = \begin{cases} 
    ax_n & 0 \leq x_n < 0.5 \\
    a(1-x_n) & 0.5 \leq x_n \leq 1
\end{cases}
\] (3)

where, \(x_n \in (0,1)\), when \(1 < a < 2\), the system is chaos. The bifurcation diagram of the Tent map is shown in Figure 1.

![Figure 1. The bifurcation diagram of the Tent map.](image-url)
2.3. Fractional order Lorenz system

The fractional order Lorenz system is defined as

\[
\begin{align*}
\frac{d^\alpha x}{dt^\alpha} &= a(y - x) \\
\frac{d^\beta y}{dt^\beta} &= cx - xz + dy \\
\frac{d^\gamma z}{dt^\gamma} &= xy - bz
\end{align*}
\] (4)

Where \(a, b, c, d\) are system parameters, \(\alpha, \beta, \gamma\) are fractional order, \(a = 40, b = 3, c = 10, d = 25, \alpha = \beta = \gamma = 0.95\). Figure 2 shows the 3d phase diagram of the fractional order Lorenz system. At this time, the lyapunov exponent of the system is 0.4515. The fractional Lorenz system is chaotic.

2.3.1. Complexity analysis

Complexity analysis is a commonly used method for the analysis of chaotic systems. It can quantitatively measure the dynamic characteristics of the system, and has the same effect as Lyapunov exponent, bifurcation diagram, dissipation character, phase diagram observation and other methods. The SE (spectral entropy) complexity and C0 complexity were analyzed for the fractional order Lorenz system. Figure 3 shows the result of complexity analysis.

As shown in Figure 3, the SE complexity develops steadily with the increase of \(q\), while the C0 complexity soon reaches a high point and gradually decreases. Figure 3 shows that the fractional order Lorenz system has higher complexity than the integer order Lorenz system.

2.3.2. Autocorrelation analysis

In this essay, autocorrelation analysis was carried out for sequences generated by integer order and fractional order Lorenz system respectively, and the results are shown in Figure 4. As can be seen from Figure 4, the amplitude of autocorrelation analysis of the fractional order Lorenz system is smaller and more concentrated around 0, and the z-sequence correlation is greatly reduced comparing with the integer Lorenz system. Therefore, the pseudo-randomness of the sequence generated by the fractional order Lorenz system is better.
Based on the above dynamic analysis of the fractional order Lorenz system, it can be seen that the fractional order Lorenz system has high complexity, and the chaotic sequence generated by the fractional order Lorenz system has better pseudo-randomness than the integer Lorenz system, which is more suitable for the design of image encryption algorithm.

3. Fractional order Lorenz image encryption algorithm

Combining the above three chaotic systems, a new colour image encryption algorithm based on fractional order chaotic systems was proposed in this paper. Firstly, the colour plaintext image was divided into three layers R, G and B. In the scrambling stage, three layers were scrambled with Arnold map, among which the initial value of the first scrambling Arnold map was from the key, and the initial value of the other two scrambling are from the R and G layers after scrambling. In the plaintext selection stage, the Tent map was iterated to obtain two sets of state values, which were used to locate the plaintext pixel position. The RGB gray value of this pixel is moulded and then used as the initial value of the fractional Lorenz system. In the diffusion stage, a part of the pseudo-random sequence generated by fractional Lorenz system was used to cross-diffuse the three layers of RGB. Then add-mode diffusion was been done in each layer. Finally the encrypted image was obtained. The plaintext image is denoted as \( A \), the pixel matrix size is \( M \times N \times 3 \), and the encryption process is shown in Figure 5.

The specific encryption steps are as:

**Step 1:** Enter the plaintext image \( P \) and the key \( K \), and assume the size of \( A \) is \( M \times N \times 3 \). Read the initial value and parameters of Arnold map in \( K \), then use Arnold map to scramble the plaintext image R layer. Expand the R layer into a one-dimensional vector. The diffusion process used the method introduced in section 2.1.

Select the last two pixels of R layer after scrambling, and take its gray value as the parameter of Arnold map when scrambling G layer, and use the same operation to scrambling B layer to get image \( P_1 \).

\[
P_1 = \begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} r(1), r(2), r(3), \cdots, r(m) \\ g(1), g(2), g(3), \cdots, g(m) \\ b(1), b(2), b(3), \cdots, b(m) \end{bmatrix}
\]

\[m = MN.\]  

**Step 2:** Read the initial value of the Tent map \( x_t(0) \) from the key \( K \). The Tent map is iterated 800 times, and the first 300 transition states were discarded, and taking the state value of the next 200, 300, 400, 500 iterations which marked as \( K_t \).

\[
K_t = [x_t(200), x_t(300), x_t(400), x_t(500)]
\]

**Step 3:** Use the formula (7) to make the \( K_t \) into a coordinate \( s_1 \) and \( s_2 \) which used for positioning the pixels in \( P_1 \). And read its RGB values as the second key \( K_a \) used as the initial value of fractional order Lorenz system. Adomian algorithm is used to solve fractional order Lorenz system to generate chaotic sequence and abandon the first 500 transition state. The fractional Lorenz system is iterated \( MN \) times and \( 2MN \) times respectively, tiny perturbation of system every 3000 times to get the size of \( 3 \times MN \) and \( 3 \times 2MN \) of the original pseudo random sequence \( S_1 \) and \( S_2 \) that

![Figure 5. Flow chart of our algorithm.](image)
are transformed by formula (8) to password \( K_1 \) and \( K_2 \).

\[
\begin{align*}
S_1 &= (X_t(300) \times 100 - \text{floor}(X_t(300) \times 100)) \\
S_2 &= (X_t(500) \times 100 - \text{floor}(X_t(500) \times 100)) \\
K_1 &= \begin{bmatrix} K_{a1} & K_{b1} \\ K_{a2} & K_{b2} \end{bmatrix} = \begin{bmatrix} R_{s1}, G_{s1}, B_{s1} \\ R_{s2}, G_{s2}, B_{s2} \end{bmatrix} \\
K_2(i) &= (\text{floor}(S_1(i) \times 2^{16}) \mod 256) + 1 \\
K_2(j) &= (\text{floor}(S_2(j) \times 2^{16}) \mod 256) + 1
\end{align*}
\]

(7)

**Step 4:** Aim at the problem of insufficient diffusion in (Liu et al., 2016; Niyat et al., 2017) and vulnerability to chosen-plaintext attack, our algorithm does the following processing in this step: Use the password \( K_1 \) to spread the information between the layers of the image. The specific calculation method is shown in equation (10):

\[
\begin{align*}
\begin{cases}
    r'(i) &= r(i) \oplus k_1(1, i) \oplus b(i) \\
g'(i) &= g(i) \oplus k_1(2, i) \oplus r'(i) \\
b'(i) &= b(i) \oplus k_1(3, i) \oplus g'(i)
\end{cases}
\end{align*}
\]

where \( i = 1, 2, \ldots, MN \)

(10)

Where, the \( r'(i) \), \( g'(i) \), \( b'(i) \) are the pixel values after diffusing for the first time. After pixel diffusion between layers, the plaintext information of each layer is diffused to the other two layers. This step can enhance the algorithm’s ability to resist the chosen-plaintext attack.

The password \( K_2 \) is used for the information diffusion inside the each layers, and the forward and backward diffusion is calculated according to formula (11) and (12) respectively:

**Forward diffusion:**

\[
\begin{align*}
\begin{cases}
    r''(i) &= (r'(i-1) + k_2(1, i) + r'(i)) \mod 256 \\
g''(i) &= (g'(i-1) + k_2(2, i) + g'(i)) \mod 256 \\
b''(i) &= (b'(i-1) + k_2(3, i) + b'(i)) \mod 256
\end{cases}
\end{align*}
\]

(11)

**Backward diffusion:**

\[
\begin{align*}
\begin{cases}
    r''(j) &= (r'(j+1) + k_2(1, k) + r'(j)) \mod 256 \\
g''(j) &= (g'(j+1) + k_2(2, k) + g'(j)) \mod 256 \\
b''(j) &= (b'(j+1) + k_2(3, k) + b'(j)) \mod 256
\end{cases}
\end{align*}
\]

(12)

That’s the final ciphertext image \( C \).

The decryption process is the inverse operation of the encryption process of this algorithm.

### 4. Simulation results

All experiments of this algorithm were carried out in Matlab R 2014a environment. Matlab was used on a computer with Intel Core i5, 2.40 GHz CPU, 8GB of memory and 250 GB of SSD with Windows 10. The experimental image of this algorithm was standard 512 \times 512 Lena colour images. The key was set as \([X_t, p, a, b, X_a, Y_a, q]\), Where, \( X_t, X_a, Y_a \) were the initial values of the Tent map and Aronld map, \( p \) was the parameter of the Tent map, \( a \) and \( b \) were the parameters of the Aronld map, and \( q \) was the fractional order of the fractional Lorenz system. The encrypted image with key \([0.23, 0.85, 3, 5, 1, 1, 0.995]\) is shown in Figure 6.

It can be seen from Figure 6 that the Lena image encrypted by our algorithm can no longer show the original image and is distributed evenly without special texture. Therefore, this algorithm can protect the original image well and has a good application prospect in image encryption.

### 5. Security analysis

#### 5.1. Key space

The size of key space has an important reference value for judging the result of encryption algorithms. Encryption algorithms with a large enough key space can well resist various violent attacks such as exhaustive attacks (Kehui, 2015). When the key changed a small amount, the decrypted image is completely different. For the image encryption algorithm is proposed in this article, according to the set of section3 for \([X_t, p, a, b, X_a, Y_a, q]\), in which the scope of \( X_t, p, X_a, Y_a \) are in \((0, 1)\), the step length of \( X_t, X_a \) and \( Y_a \) is \(10^{-14}\): the step length of \( p \) is \(10^{-13}\). The parameters \( a \) and \( b \) can theoretically take any real number, and the order of magnitude is \(10^{10}\) in consideration of calculation accuracy and algorithm running speed. If \( q \) uses double precision parameter, its precision magnitude can be set as \(10^{-14}\).

![Figure 6. Encryption and decryption results.](image)
**Table 1.** Key space comparison.

| Algorithm            | Key space       |
|----------------------|-----------------|
| Our algorithm        | $10^{84} \approx 2^{279}$ |
| Niyat et al. (2017)  | $2^{128}$       |
| Xie G. (2019)        | $2^{230}$       |
| Guesmi et al. (2016) | $2^{267}$       |
| Xue et al. (2018)    | $10^{75} \approx 2^{249}$ |

In conclusion, the key space size of the whole algorithm is $10^{84}$. When the key space of an encryption algorithm is greater than $2^{128}$, the algorithm is considered safe (Ye & Huang, 2017), while the key space of the algorithm designed in this essay reaches $10^{84} \approx 2^{279}$, which is far greater than the theoretical security value. In addition, in this algorithm, the key image with the size of $M \times N$ is used for encryption. The space size is $2^8 \times MN$, and the key space is greatly increased. Therefore, this algorithm can effectively resist exhaustive attack. Compare with other literatures is shown in Table 1.

### 5.2. Speed performance analysis

The evaluation of an encryption algorithm not only includes security and effectiveness, but the efficiency of the algorithm is also important. Since our algorithm have used an improved Arnold map, there was no need for multiple cycles to scramble the image, which greatly improved computational efficiency. By comprehensively considering the diffusion process, the average time complexity of this algorithm is $O(n)$. In this article, we have encrypted images of different sizes, and recorded the running time. The results of comparison with other algorithms are shown in Table 2.

### 5.3. Correlation analysis of adjacent pixels

The correlation of adjacent pixels in the image reflects the diffusion degree of the image pixels. The adjacent pixels in the plaintext image have a strong correlation while the adjacent pixels in the effectively encrypted image have no correlation (Zhang Yong, 2016a). As shown in Figure 7, layer R was taken as an example. Figure a, c and e are the adjacent correlation of the plaintext layer R while b, d, f are the correlation of the adjacent ciphertext layer R.

**Table 2.** Encryption speed comparison.

| Algorithm            | Image size | Encryption time (s) |
|----------------------|------------|---------------------|
| Our algorithm        | $256 \times 256$ | 0.663               |
| –                    | $512 \times 512$ | 1.172               |
| –                    | $1024 \times 1024$ | 2.83               |
| Chai et al. (2017)   | $512 \times 512$ | 1.26                |
| Guobo and Zhaoxi (2019) | $512 \times 512$ | 1.35                |
| Wu et al. (2018)     | $512 \times 512$ | 1.553               |

**Figure 7.** Correlation analysis of adjacent pixels.

**Table 3.** Correlation analysis of adjacent pixels.

| Algorithm          | Horizontal | Vertical | Diagonal |
|--------------------|------------|----------|----------|
| Plaintext imag     | 0.9725     | 0.9606   | 0.9488   |
| Our algorithm      | 0.0024     | 0.0013   | 0.0064   |
| Guobo and Zhaoxi (2019) | 0.0056   | 0.0100   | 0.0246   |
| Guesmi et al. (2016) | 0.0265   | 0.0792   | 0.0625   |
| Yongju and Shijie (2020) | 0.0080   | 0.0059   | 0.0051   |
| Yao et al. (2017)  | 0.0373     | 0.0228   | −0.0221  |

It can be seen that the pixel points of plaintext image have a strong correlation in all directions when they are concentrated near the line $y = x$, while ciphertext image has no correlation in all directions. At the same time, the correlation coefficient can be calculated to intuitively compare the correlation (Zhang et al., 2012) as Table 3. The correlation coefficient of the image tends to 1 before encryption and 0 after encryption. Compared with the encryption results in another literatures (Guesmi et al., 2016; Guobo & Zhaoxi, 2019), except for the slightly lower diagonal correlation in literature (Yongju & Shijie, 2020), the image correlation encrypted by our algorithm is lower.
5.4. The histogram analysis

Histogram is a statistical chart representing the gray distribution of an image, and counts the occurrence times of each gray value (Hong et al., 2013). When the histogram of an image has obvious distribution characteristics, it is easier to obtain information in the image, while the image with messy and evenly distributed histogram is less likely to show any valuable information (Zhang Yong, 2016a). Therefore, histogram analysis can be used as a criterion for evaluating encryption algorithms. It is the comparison between plaintext image and ciphertext image histogram shown in Figure 8. Figure a, c and e are the histogram of plaintext image, while b, d and f are the histogram of ciphertext image. It can be seen that the encrypted histogram no longer has obvious characteristics, and the number of pixel values differs very little, which qualitatively indicates that the encrypted image by the algorithm in this paper has a uniform diffusion of pixel values.

One side hypothesis test was carried out to measure the distribution of the histogram, as Table 4.

In the data obtained after one side hypothesis test, the chi-square statistics of the three layers were all smaller than $\chi^2_{0.01}(255)$, so it can be considered that the ciphertext images are evenly distributed (Zhang Yong, 2016a). It shows that our algorithm can resist statistical attack effectively.

5.5. Statistical randomness analysis

The randomness of the algorithm is very important to the password generator and ciphertext, and it affects the algorithm’s ability to resist statistical attacks. This article uses the randomness detection kit provided by the National Bureau of Technology and Standards to conduct statistical randomness analysis of the algorithm in this article. In order to accept the randomness of the bit sequence, it is hoped that the significance level p of each test is above 0.01. The analysis results are shown in Table 5.

5.6. Ability of resisting differential attacks

In order to measure the sensitivity of image encryption algorithm, two indexes NPCR and UACI have been proposed. NPCR and UACI describe the ability of image encryption system against differential attack (Chen et al., 2004; Mao et al., 2004). They are defined as: suppose that the plaintext image $A_1$ and $A_2$ are identical except that the

![Figure 8](image-url)
value at one pixel point \((i,j)\) is different of 1, the plaintext image \(A_1\) and \(A_2\) are encrypted by the same image cryptography system and the same key. \(C_1\) and \(C_2\) are the ciphertext image encrypted from \(A_1\) and \(A_2\), define,

\[
D(i,j) = \begin{cases} 
0, & C_1(i,j) = C_2(i,j) \\
1, & C_1(i,j) \neq C_2(i,j)
\end{cases}
\]

(13)

\[
NPCR = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%
\]

(14)

\[
UACI = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%
\]

(15)

The expected values of NPCR and UACI were 99.6094% and 33.4635%, respectively.

The experimental method in this paper was that change one pixel value of image \(A\) or key value to obtain two different plaintext image \(A_1\) and \(A_2\). Obtain the ciphertext image \(C_1\) and \(C_2\) by encrypting \(A_1\) and \(A_2\). The change value of the keys were shown in eq (16). The UACI and NPCR of \(C_1\) and \(C_2\) were calculated. Repeat this step 50 times.

\[
\Delta X_t = 10^{-13} \\
\Delta p = \Delta X_q = \Delta Y_q = \Delta q = 10^{-14} \\
\Delta a = \Delta b = 1
\]

(16)

It can be seen from Tables 6–8, that the values of NPCR and UACI are close to ideal values, which proves that the algorithm has high plaintext and key sensitivity. Compared with literature [Guesmi et al., 2016; Guobo & Zhaoxi, 2019; Niyat et al., 2017], the algorithm in this essay has stronger plaintext sensitivity and can resist differential attack more effectively.

Generally, higher NPCR and UACI scores represent higher resistance to differential attacks. However, for different images or images of different sizes, NPCR and UACI have different scoring standards. Therefore, simply calculating the values of NPCR and UACI is not very good. Explain the performance of the algorithm. Yue Wu in [Wu et al., 2011], the expectations, variance and hypothesis tests of NPCR and UACI (randomness test) were derived to measure whether the algorithm really has a high resistance to differential attacks. According to the formula (16)-(19), we have tested three sizes and three pictures of each. If the NPCR score of the encrypted image is above \(N_a^\alpha\), it can be considered a truly random image. If the UACI score of the encrypted image is between \(U_a^\alpha\) and \(U_a^\beta\), it proves that the image has passed the UACI test. The results are shown as Tables 9 and 10, all the images passed the test. In summary, the algorithm proposed in this paper can effectively resist differential attacks.

| Key | NPCR/% | UACI/% |
|-----|--------|--------|
| \(X_1(10^{-13})\) | 99.6065 | 33.4471 |
| \(a(10^{-14})\) | 99.6121 | 33.4566 |
| b(10^{-14}) | 99.6109 | 33.4611 |
| \(X_q(10^{-14})\) | 99.5984 | 33.4724 |
| \(Y_q(10^{-14})\) | 99.6047 | 33.4660 |
| \(q(10^{-14})\) | 99.6142 | 33.4519 |

Table 8. Key sensitive analysis.

| Test image | Qualitative NPCR analysis | Theoretical NPCR (0.05) | Result |
|------------|---------------------------|-------------------------|--------|
| 1(256×256) | Pass | 99.5904 | 99.5693 |
| 2(256×256) | Pass | 99.5881 | Pass |
| 3(256×256) | Pass | 99.5912 | Pass |
| 4(512×512) | Pass | 99.6133 | 99.5893 |
| 5(512×512) | Pass | 99.6063 | Pass |
| 6(512×512) | Pass | 99.6038 | Pass |
| 7(1024×1024) | Pass | 99.6157 | 99.5994 |
| 8(1024×1024) | Pass | 99.6193 | Pass |
| 9(1024×1024) | Pass | 99.6029 | Pass |

Table 9. Qualitative NPCR analysis.

| Test image | Qualitative UACI analysis | Theoretical UACI (0.05) | Result |
|------------|---------------------------|-------------------------|--------|
| 1(256×256) | Pass | 33.4471 | 33.2824 |
| 2(256×256) | Pass | 33.4646 | 33.6447 |
| 3(256×256) | Pass | 33.4570 | Pass |
| 4(512×512) | Pass | 33.4660 | 33.3730 |
| 5(512×512) | Pass | 33.4796 | 33.5541 |
| 6(512×512) | Pass | 33.4533 | Pass |
| 7(1024×1024) | Pass | 33.4726 | 33.4183 |
| 8(1024×1024) | Pass | 33.4609 | 33.5088 |
| 9(1024×1024) | Pass | 33.4507 | Pass |

Table 10. Qualitative UACI analysis.
\[
\begin{align*}
U_{a^-} &= \mu_U - \Phi^{-1}\left(\frac{a}{2}\right)\sigma_U \\
U_{a^+} &= \mu_U + \Phi^{-1}\left(\frac{a}{2}\right)\sigma_U
\end{align*}
\]  

(20)

where \( F \) is the largest supported pixel value compatible with the ciphertext image format. \( M \) and \( N \) are the size of the image. \( \Phi^{-1} \) is the inverse of CDF of the standard Normal distribution \( N(0,1) \).

### 5.7. Information entropy analysis

Information entropy can be regarded as the probability of occurrence of discrete random events in mathematics (Fengming & Li, 2015). The larger the information entropy of an image, the higher the degree of confusion of the image, the less information it shows. Information entropy is defined by the formula (20),

\[
H(P) = - \sum_{i=1}^{n} P(m_i) \log_2 P(m_i)
\]

(21)

Where, \( H(P) \) denotes the information entropy of an information source \( P \), \( P(m_i) \) is the probability of symbol \( m_i \) and the entropy is presented in bits.

For an encrypted 8-bit gray-scale image, its ideal entropy value is 8. The information entropy of the algorithm in this paper and other algorithms encrypted color 512 × 512 Lena image is shown in Table 11.

It can be seen from the Table 11 that the information entropy of the Lena image encrypted by our algorithm is very close to the ideal value of 8, which proves that the image is very chaotic on the global level.

We used \((k, T_B)\)-local entropy test to measure the local randomness of the image, and combine different images to verify the effectiveness of the algorithm. The definition of local entropy was: for an image \( P \), select \( k \) non-overlapping image blocks \( S_1, S_2, \cdots S_k \), a total of \( T_B \) pixels, and the calculation formula for local entropy is as follows,

\[
\bar{H}_{k,T_B}(m) = \frac{1}{k} \sum_{i=1}^{k} H(S_i)
\]

(22)

Where \( S \) is the non-overlapping pixel block in the test image. \( H(S_i) \) is the information entropy of the pixel block.

We set the parameter \((k, T_B) = (30, 1936)\) and the significance level alpha = 0.05, then the ideal local entropy is 7.902469317 (Wu et al., 2013). If the local entropy of the test image is between \((7.901901305, 7.903037329)\), we think it has passed the test. As shown in Table 12, the local entropy of the ciphertext image is all greater than 7.9 and the test proves that our algorithm is safe and has the ability to resist entropy attacks.

### 5.8. Cut and tamper attack test

During the transmission of the ciphertext image, the attacker will cut and tamper with the ciphertext image, which will affect the decrypted image. In this paper, we cut 100 × 100 area of the ciphertext image and decrypt it. And add 2% salt and pepper noise to the ciphertext image and decrypt it. The results is shown in Figure 9. From the experimental results, the cut and tampered images can still reflect the original information after being revealed, which proves that our algorithm has a good ability to resist cut and tampering attacks.

### 6. Conclusion

In this paper, we have proposed a novel colour image encryption algorithm based on fractional order Lorenz system. In our algorithm, the colour image was divided into three layers and scrambled respectively, and the three scrambled images were not repeated by selecting...
clear pixels. Secondly, our algorithm conducted pixel diffusion twice. The first time, the information diffusion was carried out between layers, and the second time, the inside of each layer was add-mode diffusion twice. The pixel values were uniformly distributed at different positions of different layers. In addition, two plaintext associations were made in the algorithm. The Tent map was used to control the initial iteration values of fractional Lorenz system, which greatly improved the algorithm’s ability to resist plaintext attack and known plaintext attack. Simulation results and analysis show that the key space of our algorithm is large enough, ciphertext correlation and plaintext sensitivity are close to theoretical values, and it can effectively resist exhaustive attack, differential attack, entropy attack and other attack methods.

**Disclosure statement**

No potential conflict of interest was reported by the author(s).

**References**

Chai, X., Gan, Z., & Zhang, M. (2017). A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. *Multimed Tools Appl.*, 76, 15561–15585. https://doi.org/10.1007/s11042-016-3858-4

Chen, G., Mao, Y., & Chui C. K. (2004). A symmetric image encryption scheme based on chaotic 3D cat maps. *Chaos Solitons & Fractals*, 21(3), 749–761. https://doi.org/10.1016/j.chaos.2003.12.022

Dong, H., Chunhua, W., & Min, X. (2018). Color image encryption based on chaotic mapping and secondary residual cipher. *Application Research of Computers*, 35(9), 203–207. https://doi.org/10.3969/j.issn.1001-3695.2018.09.046

Fengming, G., & Li, T. (2015). Application of chaos theory in cryptography. Beijing Institute of Technology Press.

Guesmi, R., Farah M, A. B., Kachouri, A., & Samet, M. (2016). A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. *Nonlinear Dynamics*, 83(3), 1–14. https://doi.org/10.1007/s11071-015-2392-7

Guobo, X., & Zhaoxi, G. (2019). Plaintext associated multi-chaos color image encryption algorithm. *Computer Engineering and Design*, 40(4), 920–930. https://doi.org/10.16208/j.issn1000-7024.2019.04.004

Hong, Z., Xiaoguang, C., & Fengying, X. (2013). *Digital image processing and analysis*. Machinery Industry Press.

Jiri, F. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation & Chaos*, 8(6):1259. https://doi.org/10.1142/S021812749800098X

Jiyun, Y., & Hao, W. (2018). Color image encryption algorithm based on chaotic system and dynamic DNA coding and operation. *Computer Engineering*, 44(2), 151–157.

Kehui, S. (2015). *Principle and technology of chaotic secure communication*. Tsinghua University Press.

Liu, H., Kadir, A., & Li, Y. (2016). Asymmetric color pathological image encryption scheme based on complex hyper chaotic system. *Optik-International Journal for Light and Electron Optics*, 127, 5812–5819. https://doi.org/10.1016/j.ijleo.2016.04.014

Mao, Y., Chen, G., & Lian, S. (2004). A novel fast image encryption scheme based on 3D chaotic baker maps. *International Journal of Bifurcation & Chaos*, 14(10), 3613–3624. https://doi.org/10.1142/S021812740401151X

Niyat, A. Y., Moattar, M. H., & Torshiz, M. N. (2017). Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Optics & Lasers in Engineering*, 90(March), 225–237. https://doi.org/10.1016/j.optlaseng.2016.10.019

Simin, Y., Jinhu, L., & Guanrong, C. (2013). Dynamic system anti-control method and application. Science Press.

Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications*, April Edition, 2011.

Wu, X., Wang, K., Wang, X., Kan, H., & Kurths, J. (2018). Color image DNA encryption using NCA map-based CML and one-time keys. *Signal Processing*, 148(July), 272–287. https://doi.org/10.1016/j.sigpro.2018.02.028

Wu, Y., Zhou, Y., Saveriades, G., Agaian, S., Noonan, J. P., & Natarajan, P. (2013). Local Shannon entropy measure with statistical tests for image randomness. *Information Sciences*, 217(3), 361–377.

Xue, H. W., Du, J., Li, S. L., & Ma, W.-j. (2018). Region of interest encryption for color images based on a hyperchaotic system with three positive Lyapunov exponents. *Optics & Laser Technology*, 106, 506–516. https://doi.org/10.1016/j.optlastec.2018.04.030

Yao, L., Yuan, C., Qiang, J., Feng, S., & Nie, S. (2017). An asymmetric color image encryption method by using deduced gyrator transform. *Optics & Lasers in Engineering*, 89(February), 72–79. https://doi.org/10.1016/j.optlaseng.2016.06.006

Yavuz, E. (2019). A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme. *Optics & Laser Technology*, 114:224–239. https://doi.org/10.1016/j.optlastec.2019.01.043

Ye, G., & Huang, X. (2017). An efficient symmetric image encryption algorithm based on an intertwining logistic map. 251:45–53. https://doi.org/10.1016/j.neucom.2017.04.016

Yong, Z. (2016a). *Chaotic digital image encryption*. Tsinghua University Press.

Yong, Z. (2016b). The image encryption algorithm with plaintext-related shuffling. *IETE Technical Review* (Taylor & Francis Ltd). 33(3):310. https://doi.org/10.1080/02564602.2015.1087350.

Yongju, X., & Shijie, X. (2020, June 19). A bigraph association encryption algorithm based on hyperchaotic system. *Computer Application Research*, 37(8), 1–5. https://doi.org/10.19734/j.issn.1001-3695.2019.02.0071

Zhang, Y. (2014). Plaintext related image encryption scheme using chaotic map. Telkomnika Indonesian Journal of Electrical Engineering, 12(1), 635–643. https://doi.org/10.11591/telkomnika.v12i1.3482

Zhang, W., Wong, K. W., Yu, H., & Zhu, Z.-l. (2013). An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Communications in Nonlinear Science & Numerical Simulation*, 18(8), 2066–2080. https://doi.org/10.1016/j.cnsns.2012.12.012

Zhang, Y., Xia, J., Cai, P., & Chen, B. (2012). Plaintext related Two-level secret key image encryption scheme. *Telkomnika Indonesian Journal of Electrical Engineering*, 10(6), 1254–1262. https://doi.org/10.11591/telkomnika.v10i6.1599