A Hyper-Chaotic Color Image Encryption Algorithm and Security Analysis

Fangzheng Zhao[1*], Chenghai Li[2], Chen Liu[2]

[1] Graduate School, Air Force Engineering University, Xi'an, Shanxi, China.
[2] Air and Missile Defense College, Air Force Engineering University, Xi'an, Shanxi, China.

* Corresponding author: Tel: 13201619730; email: zhaofz1020@163.com
Manuscript submitted March 10, 2019; accepted June 20, 2019.
doi: doi: 10.17706/jcp.14.7.496-506

Abstract: According that the current color image encryption algorithms of "scrambling – diffusion" mode have many problems, such as the small key space, the tedious encryption process, the security vulnerability and so on, this paper proposes a new color image encryption algorithm based on the hyperchaotic system, which adopts "transforming - scrambling - diffusion" model. Before scrambling, in accordance with the image itself attributes, the number of iterations is calculated, all the pixel values of color image gray code iterative transformation, then the chaotic sequence generated from the four-dimensional hyper-chaotic system and pixel matrix converted to gray code are transformed to one dimensional matrixes .The former is sorted and the later change correspondingly to complete the image pixel matrix of the whole domain scrambling. And then, bit operation is executed to complete image diffusion. the ciphertext is obtained by matrix transformation. The key sensitivity histogram information entropy correlation and other evaluation indexes are calculated and analyzed through the simulation experiment, and compared with other algorithms, proving that the encryption algorithm has strong anti-attack ability.

Key words: Hyper-chaotic system, color image encryption, gray code key space.

1. Introduction

With the rapid development of multimedia information industry, the security requirements of information are gradually improved [1], and image encryption plays an increasingly important role in military, medical, meteorological and other fields, and has become a hot topic of many domestic. Due to its strong initial value and parameter sensitivity, chaos system shows good randomness, which has been widely used in image encryption [2]. Zhang Yonghong and Zhang Bo *et al.* proposed an image encryption algorithm based on Logistic chaotic system [3]. The algorithm has a simple process, but the ciphertext distribution is not uniform, making it difficult to resist statistical attacks. Gao Fei and Fan Qingyu proposed an image encryption algorithm based on Arnold transformation [4], which is easy to realize and understand, but only applicable to square images with certain limitations. Ran Wei et al. proposed an image encryption algorithm combining DNA encoding of various chaotic maps [5], which is highly sensitive to plaintext and keys and has strong scrambling effect, but the algorithm process is complex. Compared with low-dimensional chaos, high-dimensional chaos has stronger dynamic characteristics and randomness. Zhao Feng et al proposed an image encryption algorithm based on two-dimensional chaotic system [6], and Chai Xiuli et al proposed a color image encryption algorithm based on Chen's hyperchaotic system [7], both of which achieved good encryption results. This paper proposes a new color image encryption algorithm based on four - dimensional hyperchaotic system. This algorithm is different from the traditional "scrambling - diffusion" encryption

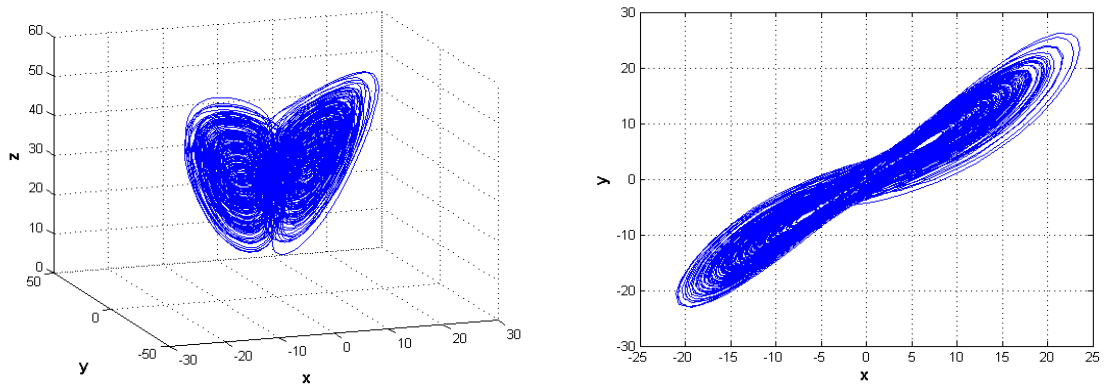
mode. Before scrambling, the pixel value is first converted into gray code, forming a new "transformation-scrambling - diffusion" mode, which expands the key space and improves the security of encryption. During the scrambling process, the global pixel position is scrambled according to the chaotic sequence generated by the hyperchaotic system, which reduces the correlation between adjacent elements and each color component. The scrambled sequences and chaotic sequences are bitwise manipulated to complete image diffusion. After the whole encryption process is iterated, the ciphertext image is obtained by matrix transformation. With this algorithm, the security and cryptography characteristics of the encrypted color image are improved.

2. Hyperchaotic System

The equation of state of the 4-dimensional autonomous hyperchaotic system used in this paper is [8]:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = bx - xz - u \\ \dot{z} = -cz + xy \\ \dot{u} = m(x + y) \end{cases} \tag{1}$$

where x, y, z and u are the state variables of the system, a, b, c and m are the real value parameters of the system, and the dynamic characteristics of the chaotic system depend on the change of parameters. When $a = 33, b = 33, c = 2,$ and $m = 9$, chaotic attractors exist in system (1), as shown in Fig. 1.



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

Fig. 1. Chaotic attractors of the system (1).

At this point, the system has two positive Lyapunov exponentials and hyperchaotic characteristics [9]. Compared with low-dimensional chaotic systems, high-dimensional hyperchaotic systems show more complex dynamic characteristics, and have more complex phase space, the randomness of the system is greatly increased, so it is more suitable for the process of color image encryption.

3. Image Encryption and Decryption Algorithm

The traditional image encryption process mostly adopts the method of "scrambling - diffusion". Before scrambling, this algorithm firstly converts the pixel value of the image into gray code, improving the new encryption process of "transformation-scrambling - diffusion" to further expand the key space.

3.1. Gray Code Conversion

Gray code is a common binary communication coding format. Its encoding rule is that two adjacent codes have only one binary number different. The method of converting the natural binary code of bit j into a typical gray code is as follows:

$$\begin{cases} G(i) = B(i) & i = j-1 \\ G(i) = B(i+1) \oplus B(i) & 0 \le i < j-1 \end{cases} \quad (2)$$

Among them, $G(i)$ and $B(i)$ respectively typical gray code and natural binary code of the ith, $\oplus$ means exclusive or (Xor)operation. The method of converting a typical n-bit gray code into a natural binary code is as follows:

$$\begin{cases} B(i) = G(i) & i = N-1 \\ B(i) = G(i) \oplus B(i+1) & 0 \le i < N-1 \end{cases} \quad (3)$$

In this algorithm, the first encrypted gray code iteration conversion times are calculated according to the size of the color image r_0:

$$r_0 = mod((L+W), 7) + 1 \quad (4)$$

where, L and W are respectively the length and width represented by color image size pixels.

3.2. Pixel Position Scrambling

Based on the chaotic sequence generated by hyperchaotic system, this algorithm can scramble the pixel positions of n-by-m color images. The steps of pixel position scrambling are as follows:

1) According to the given system parameters a, b, c, m and initial values x_0, y_0, z_0, u_0, Runge-Kutta algorithm was used to iterate the chaotic system (1), and the four chaotic real value sequences of x,y,z and u were obtained.
2) Converting the four chaos real value sequences into a one-dimensional matrix, to reduce the impact of the initial value on the system, and give up the previous n_0 results, we get a one-dimensional chaos sequence C_i, i = 1,2, … , N × M × 3,

$$n_0 = [(\bar{R} + \bar{G} + \bar{B}) \times r_0] \quad (5)$$

Among them, $\bar{R}$、$\bar{G}$ and $\bar{B}$ are respectively the average pixel values of three color components, $[\cdot]$ represents the fetch operation.

3) Convert the three-dimensional matrix which has been converted to gray code to a one-dimensional matrix P_i, arrange the one-dimensional chaotic matrix C_i in step (2) by size and P_i change positions synchronously. This completes the whole-field pixel scrambling.

For color images, there is a strong correlation between adjacent pixels and each color component of a color image. The whole-field pixel scrambling method not only disrupts the correlation between adjacent pixels, but also changes the correlation among *R, G* and *B* color components to achieve a better scrambling effect. Although the histogram statistics of each color component have changed to some extent, the histogram statistics of the image as a whole have not changed, and the histogram statistics of each component are not uniform, which still needs to be further encrypted.

3.3. Pixel Value Diffusion

In order to improve the security of image encryption, this algorithm uses the sequence generated by hyperchaotic system to diffuse the pixel value of image. The hyperchaotic sequence transformed into one dimension is discretized as follows to obtain the key flow D_i:

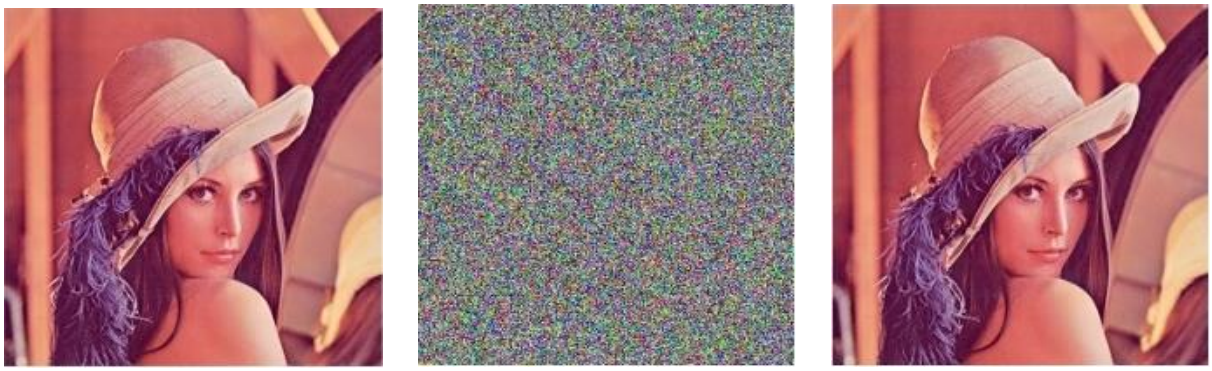
$$D_i = mod(round(abs(C_i)), 256) \quad (6)$$

Converting the matrix generated by the XOR operation of scrambled image sequence and discreted chaotic sequence as the final output sequence.

Decryption algorithm is the inverse process of encryption algorithm, decryption image can be obtained by decryption according to the key r、a、b、c、m、x_0、y_0、z_0 and u_0.

4. Simulation Experiment

In this experiment, color image "lena.jpg" of size 256 by 256 was selected as the encrypted plaintext image. The parameter values of the four-dimensional hyperchaotic system (1) were $a = 33$,$b = 33$,$c = 2$,$m = 9$and the initial values were $x_0 = 6.1$, $y_0 = 7.6$, $z_0 = 19.8$, and $u_0 = 16.2$. The total number of iterations in the image encryption process $t = 5$. According to the formula (4) and (5), the first round of encryption, the times of gray code conversion of iterations is $r_0 = 2$, the selection of chaotic sequence starts from $n_0 = 768$, and then , in each subsequent iteration, $r_i = r_{i-1} + 1$, $n_i = n_{i-1} + r_i^2$. The encryption key includes a、b、c、m、x_0、y_0、z_0、u_0、t and n_0, the decryption key is same as the encryption key. The encryption and decryption results of the image are shown in the figure. The ciphertext image is disordered and the decrypted image is exactly the same as the plaintext image.



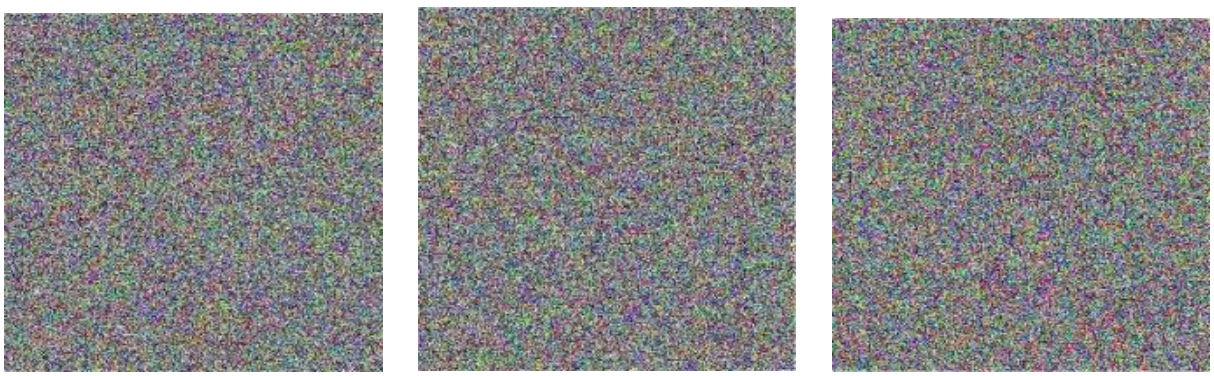
(a)Plaintext (b)Ciphertext (c)Decrypted Image

Fig. 2. Plaintext, ciphertext & decrypted image.

5. Analysis of Simulation Results

5.1. Key Sensitivity

To detect the key sensitivity of the algorithm, only one key is changed during decryption. The initial value of the chaotic system, the number of iterations and the order number selected at the beginning of the chaotic sequence are changed respectively and slightly. In proper order, let $u_0 = 16.2000001$, $t = 4$, $n_0 = 769$, The decrypted images are as follows:

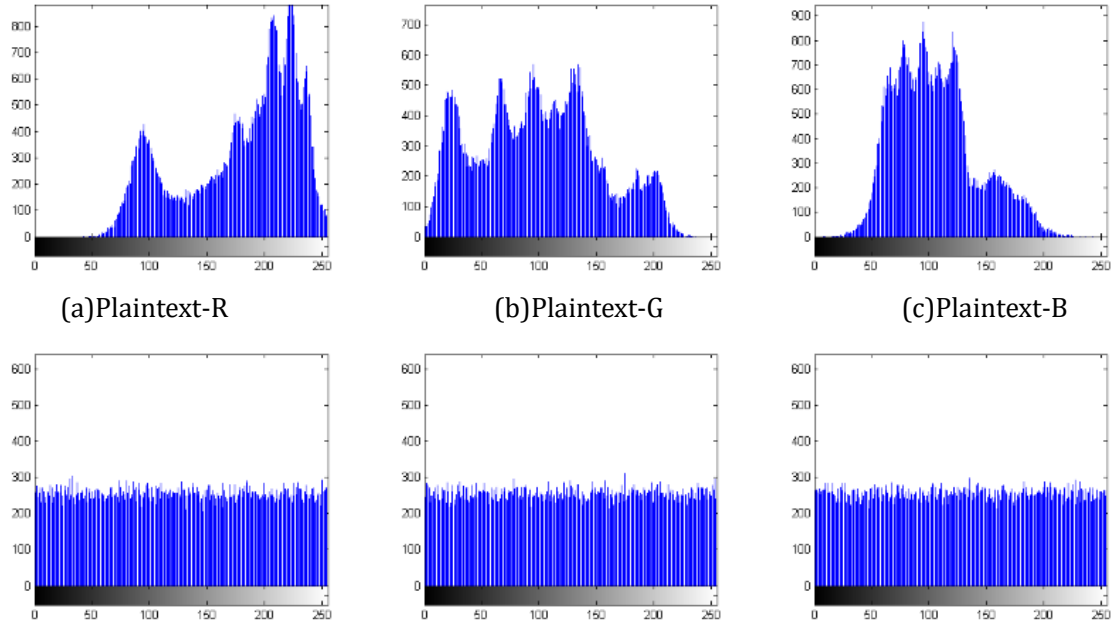


(a) $u_0 = 16.2000001$ (b) $t = 4$ (c) $n_0 = 769$

Fig. 3. 3 Error decrypted images.

5.2. Histogram

Histogram shows the frequency of different pixel values appearing in images. It has been widely used in image retrieval, classification and other fields. Image encryption increases the difficulty of extracting image histogram features by histogram equalization and generalization [10]. The histograms of the images before and after encryption are shown in Fig. 4.



(a)Plaintext-R (b)Plaintext-G (c)Plaintext-B

(d)Ciphertext-R (e)Ciphertext-G (f)Ciphertext-B

Fig. 4. Histogram of plaintext & ciphertext.

The histogram of color components tends to be uniform distribution, which is completely different from the plaintext distribution. This shows that the transformation-scrambling-diffusion mode of the algorithm has good scrambling and statistical characteristics, and meets the requirements of image encryption.

5.3. Relevance of Adjacent Elements

There is often a high correlation between adjacent pixels in plaintext, which is the inherent feature of the image. Therefore, the encryption algorithm should try to reduce the correlation between adjacent pixels. In this paper, 10,000 pixels are randomly extracted from plaintext and ciphertext, and the correlation coefficients in horizontal, vertical and diagonal directions are calculated according to the following formulas.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{7}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{8}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{9}$$

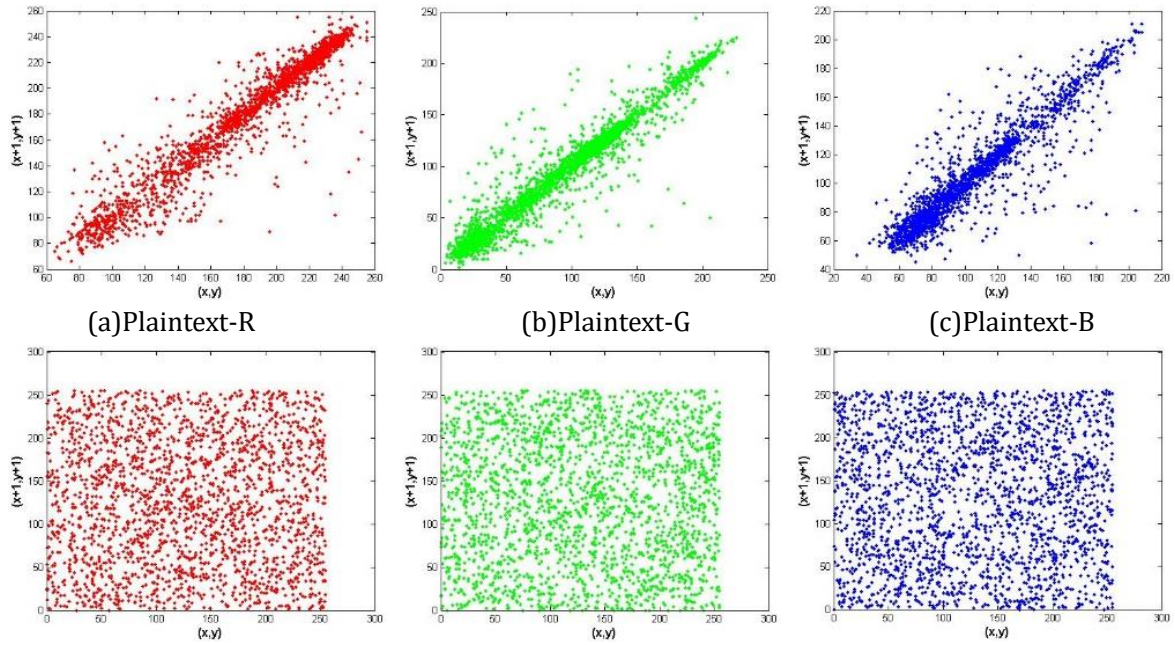
$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{10}$$

x and y are the pixel values of adjacent pixels, and r_{xy} is the correlation coefficient. The results are shown in Table 1.

Table 1. Adjacent Element Correlation

Correlation Coefficient	Horizontal	Vertical	Diagonal
Plaintext	0.9372	0.9458	0.9681
Ciphertext	0.0013	0.0015	-0.0024
Ciphertext [11]	-0.0102	0.0076	-0.0153
Ciphertext [12]	0.0129	0.0065	0.0013
Ciphertext [13]	0.0034	0.0050	0.0056

2500 pixels were randomly selected from the three primary color components of the original image and the encrypted image respectively. The element distribution in the diagonal direction is shown in Fig. 5:



(a)Plaintext-R (b)Plaintext-G (c)Plaintext-B

(d)Ciphertext-R (e)Ciphertext-G (f)Ciphertext-B

Fig. 5. Correlation of pixel components in the diagonal direction of plaintext and ciphertext.

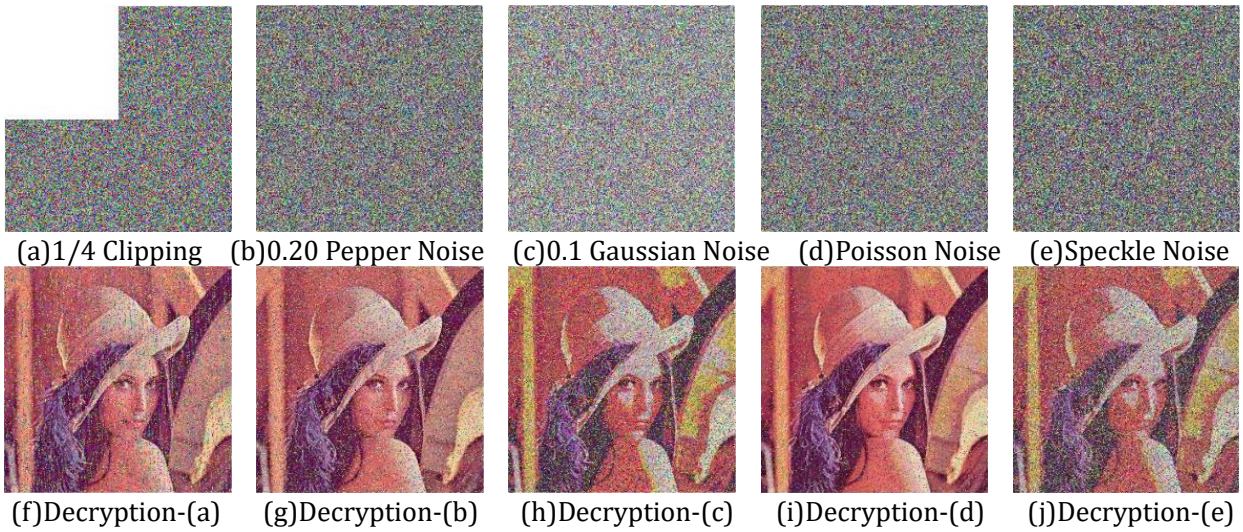
Adjacent elements of plaintext images tend to have a strong correlation, and the distribution of elements and their adjacent elements is concentrated around $x = y$, as shown in Fig. 5 (a) - (c). The scrambling operation is aimed at reducing this correlation, which is shown as nearly uniform distribution in the region [0, 255], as shown in Fig. 5 (d) - (f).

Both Table 1 and Fig. 5 show that this encryption algorithm has good diffusion characteristics.

5.4. Robustness

In the process of image transmission or decoding, pepper and salt noise, gaussian noise and other noises as well as image clipping are often generated. Therefore, the image encryption and decryption algorithm should adapt to clipping and noise to a certain extent. Fig. 6 shows the images decrypted after a 1/4 clipping, adding 0.20 pepper noise, 0.1 gaussian noise, Poisson noise and speckle noise.

It can be seen from the image that ciphertext has been recovered well and plaintext information can be basically restored, indicating that this algorithm has good robustness.



(a)1/4 Clipping (b)0.20 Pepper Noise (c)0.1 Gaussian Noise (d)Poisson Noise (e)Speckle Noise

(f)Decryption-(a) (g)Decryption-(b) (h)Decryption-(c) (i)Decryption-(d) (j)Decryption-(e)

Fig. 6. Decrypted images of 1/4 clipping and noises.

6. Anti-attack Analysis

6.1. Anti-exhaustive Attack

This algorithm based on gray code and hyperchaos system of 4 d, parameters and initial value, the number of iterations, and image size as the encryption key, set the precision to 10^{14}, key space more than 10^{86}, far more than Lian puts forward the key space of at least 2^{64} to be effective against violent attacks [14]. Therefore, the key space of this encryption algorithm can effectively resist exhaustive attack.

6.2. Anti-entropy Attack

Image information entropy is used to represent the aggregation feature of image pixel value distribution. The calculation method is as follows:

$$H = -\sum_{i=0}^{255} p(i)\, log_2\, p(i) \tag{11}$$

$p(i)$ is the frequency of each greyscale. This formula is mainly used to calculate the information entropy of gray image. In this paper, the calculation method of the information entropy of color image is defined as follows:

$$H = \frac{1}{3}\sum H_k \tag{12}$$

$k \in \{R, G, B\}$, $H_k$represents the information entropy of each color component of RGB.

Table 2. Comparison of Information Entropy

Image	Information Entropy
plaintext	7.4481
ciphertext	7.9991
ciphertext [3]	7.8556
ciphertext [11]	7.8534
ciphertext [15]	7.9551

As shown in Table 2, by comparing the information entropy of plaintext, ciphertext of this algorithm and ciphertext image of references [3], [11] and [15], it can be concluded that the information entropy value of the encrypted image of this algorithm is closer to the ideal value 8, and the encrypted image is closer to the

random signal source, which can effectively resist entropy attack.

6.3. Anti-plaintext Attack

Since the starting sequence number of gray code and chaotic sequence is related to the attribute of plaintext image itself, the key obtained by selecting different plaintext is often different, and "One Picture One Key" can basically realize that the key pushed by the specific plaintext cannot correctly decrypt the other ciphertext [7]. Therefore, it can be concluded that this algorithm has good anti-selective plaintext attack ability.

6.4. Anti-differential Attack

NPCR(Number of Pixels Change Rate) and UACI(Unified Average Changing Intensity) can be used to measure the sensitivity of encryption algorithm to plaintext, which is an important indicator to measure the algorithm's resistance to differential attack. NPCR and UACI respectively represent the proportion and degree of change of pixel values at corresponding positions. The greater the proportion and degree of change is, the stronger the ability of algorithm's resistance to differential attack is. The calculation formula is as follows:

$$NPCR = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{S_{ij}}{M\times N}\times 100\% \tag{13}$$

$$S_{ij} = \begin{cases} 1 & X(i,j) \neq X'(i,j) \\ 0 & X(i,j) = X'(i,j) \end{cases} \tag{14}$$

$$UACI = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|X(i,j)-X'(i,j)|}{M\times N\times 255}\times 100\% \tag{15}$$

where $M \times N$为 is the size of the image, $X(i,j)$ and $X^{'}(i,j)$ respectively represent the pixel values of the corresponding positions of plaintext and ciphertext. Define the calculation method of NPCR and UACI for color image according to the gray images', as follows:

$$NPCR_3 = \sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{k=1}^{3}\frac{S'_{ijk}}{M\times N\times 3}\times 100\% \tag{16}$$

$$S'_{ijk} = \begin{cases} 1 & X(i,j,k) \neq X'(i,j,k) \\ 0 & X(i,j,k) = X'(i,j,k) \end{cases} \tag{17}$$

$$UACI_3 = \sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{k=1}^{3}\frac{S'_{ijk}}{M\times N\times 255\times 3}\times 100\% \tag{18}$$

The calculated results are shown in Table 3:

Table 3. Comparison of NPCR & UACI

Image	NPCR/%	UACI/%
Ciphertext	99.63	33.52
Ciphertext [3]	99.63	33.54
Ciphertext [11]	86.55	33.47
Ciphertext [12]	99.63	33.51

When the NPCR and UACI of the image are greater than 99.6% and 33.46% respectively, it indicates that the algorithm has good security. As shown in Table 3, by comparing the NPCR and UACI values of references [3], [11] and [12], this algorithm, more sensitive to plaintext than the references listed in Table 3, can meet

the security requirements, and has good resistance to differential attack.

7. Conclusion

In this paper, a new color image encryption algorithm based on "transformation-scrambling-diffusion" is proposed for a four-dimensional hyperchaotic system. It is different from the traditional encryption algorithm based on "scrambling-diffusion". According to the chaotic sequence generated by the four-dimensional chaotic system, the scrambling and diffusion are completed, which makes the algorithm show better statistical characteristics, and the algorithm process is simple and easy to implement. In the design of this algorithm, some encryption keys are dependent on plaintext, which increases the sensitivity of the algorithm to plaintext and improves the anti-plaintext attack ability. The simulation results show that this algorithm has good security and strong anti-damage ability, and has a very high application value in the field of image encryption.

References

[1] Shang, B. (2018). Discussion on Chinese computer network security. *Wireless Internet Technology, 2018(8).*

[2] Whitman, M. E., & Mattord, H. J. (2011). Principles of information security. *Information Security Management & Policy, 12(3),* 429-437.

[3] Zhang, Y. H., & Zhang, B. (2015). Algorithm of image encrypting based on logistic chaotic system. *Application Research of Computers, 32(6),* 1770-1773.

[4] Gao, F., & Fan, Q. Y. (2015). Image encryption research based on Arnold transformation. *Journal of Fuyang Teachers College(Natural Science), 2015(2),* 92-96.

[5] Ran, W., Wei, P. C., & Duan, A. (2018). Image encryption algorithm based on multi-chaotic mapping and DNA coding. *Computer Engineering and Design, 2018(7).*

[6] Zhao, F., & Wu, C. M. (2016). Image encryption algorithm combined self-encoded theory with super-chaotic mapping. *Journal of Computer-Aided Design & Computer Graphics, 28(1),* 119-128.

[7] Chai, X. L., & Gan, Z. H. (2016). New bit-level self-adaptive color image encryption algorithm based on hyperchaotic system. *Computer Science, 43(4),* 134-139.

[8] Zhang, L., & Tang, J. S. (2018). Hopf bifurcation analysis and anti-control of bifurcation of a four-dimensional hyperchaotic system. *Chinese Journal of Computational Mechanics, 2018(2).*

[9] Koçak, H., & Palmer, K. (2010). Lyapunov exponents and stability in interval maps. *Sema Journal, 51(1),* 79-82.

[10] Dwipayana, M., Arnia, F., & Musliyana, Z. (2018). Histogram equalization smoothing for determining threshold accuracy on ancient document image binarization. *Journal of Physics Conference Series,* 1019.

[11] Chen, Q. C., Zhang, Z. J., & Zhang, A. Q. (2018). New color image encryption algorithm based on hyper-chaos. *Computer & Digital Engineering, 2018(6).*

[12] Wang, X. Y., Wei, N., & Zhang, D. D. A novel image encryption algorithm based on chaotic system and improved gravity model.

[13] Lu, H. B., & Wang, L. J. (2014). Color image encryption algorithm of chaotic based on the hopfield network. *Journal of Jilin University(Information Science Edition), 32(2),* 131-137.

[14] Lian, S. (2009). A block cipher based on chaotic neural networks. *Neurocomputing, 72(4),* 1296-1301.

[15] Li, J. Q., Bai, F. M., & Di, X. Q. (2012). Color image encryption algorithm based on hopfield chaotic neural networks. *Journal of Changchun University of Science and Technology(Natural Science Edition), 35(4),* 117-121.

Fangzheng Zhao was born in October, 1994 in Beijing, China. She obtained a bachelor's degree of software engineering in Beihang University in 2017 and is studying as a second grade postgrade in Graduate School of Air Force Engineering University, majoring in CAT (Computer Application Technology). Her main research include network and information security, image encryption, etc.

Chenghai Li is a professor, he was born in October, 1966 in Shandong, China. He obtained a bachelor's degree of computer science and technology in Air Force Missile Academy in 1988, a master's degree of computer application in Xi'an University of Electronic Science and Technology in 1997 and a doctor's degree of military operation research in Air Force Engineering University in 2008.

Chen Liu was born in April, 1997 in Liaoning, China. He is studying in Air and Missile Defense College of Air Force Engineering University, majoring in information security.