Hindawi
Security and Communication Networks
Volume 2019, Article ID 8132547, 8 pages
https://doi.org/10.1155/2019/8132547

Research Article

A Hyperchaotic Color Image Encryption Algorithm and Security Analysis

Chenghai Li,[1] Fangzheng Zhao,[2] Chen Liu,[1] Lei Lei,[1] and Jie Zhang[2]

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

Correspondence should be addressed to Fangzheng Zhao; zhaofz1020@163.com

Received 21 December 2018; Accepted 13 May 2019; Published 27 June 2019

Academic Editor: Stelvio Cimato

The current common color image encryption algorithms applying "scrambling-diffusion" have some problems, such as the small key space, the cumbersome encryption process, and the security vulnerability. Aiming at these problems, this paper proposes a new color image encryption algorithm based on the hyperchaotic system and applying "transforming-scrambling-diffusion" model. Before scrambling, in accordance with the plaintext itself attributes, the number of iterations was calculated, all the pixel values of color image were transformed into gray code iteratively, and then the chaotic sequence was generated from the four-dimensional hyperchaotic system. Pixel matrix after gray code transformation was converted to one-dimensional matrix. The chaotic sequence was sorted and the one-dimensional matrix was changed positions correspondingly to complete the whole domain scrambling. And then, bit-operation was executed for image diffusion. The ciphertext can be obtained by matrix transformation. The key sensitivity, histogram, information entropy, correlation, and other evaluation indexes were calculated and analyzed through the simulation experiment. Compared with other algorithms, it can be proved that the encryption algorithm has the strong antiattack ability.

1. Introduction

With the rapid development of multimedia information industry, the security requirements of information are gradually improved [1]. In multimedia security, image encryption is playing a more and more essential role and has become one of hot issues in military, medical, meteorological, and other fields [2]. Due to the strong initial value and parameter sensitivity, chaotic systems which show good randomness have been widely used in image encryption [3]. Karan Nair, Janhavi Kulkarni et al. proposed an image encryption using logistic and rectangular chaotic maps [4]. However, the process of the algorithm was quite simple which resulted in the ciphertext distribution not being uniform which made it difficult to resist statistical attacks. Abbas A. M. proposed an image encryption algorithm, based on independent component analysis and Arnold's Cat Map [5], which was easy to be realized and provide an effective and safe way for image encryption. However, only square images could be encrypted in this algorithm; the range of application was remarkably restrained. Ran Wei et al. proposed an image encryption algorithm combining DNA encoding and various chaotic maps [6]. The simulation experiments showed that the sensitivity of plaintext and keys and the scramble effect could be greatly enhanced. But the process was complex and the requirements to hardware were comparatively high. Besides, compared with low-dimensional chaos, high-dimensional chaos has stronger dynamic characteristics and randomness. Nazira Shaikh, Santosh Chapaneri et al. proposed a single round color image encryption scheme based hyperchaotic system [7], and Chai Xiuli et al. proposed a color image encryption algorithm based on Chen's hyperchaotic system [8]; both algorithms achieved good encryption results. This paper proposes a new color image encryption algorithm based on four-dimensional hyperchaotic system and improved encryption process. This algorithm was different from the traditional "scrambling-diffusion" encryption mode. Before scrambling, the pixel values were firstly converted into gray codes. On that basis, a new "transformation-scrambling-diffusion" mode was formed that can expand the key space and improve

the security of encryption. During the scrambling process, the global pixel positions were scrambled according to the chaotic sequence generated by the hyperchaotic system. The scrambling procedure can reduce the correlation of adjacent elements and each color component. The scrambled sequences and chaotic sequences were bitwise manipulated to complete image diffusion. After the whole encryption process was iterated, the ciphertext image would be obtained by matrix transformation. With this algorithm, the security and cryptography characteristics of the encrypted color image were improved.

2. Hyperchaotic System

The equation of state of the 4-dimensional autonomous hyperchaotic system used in this paper is [9]

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

where x, y,z, and u are the state variables of system (1) and a, b, c, and m are the real value parameters. The dynamic characteristics of the chaotic system depend on the change of parameters above all. When a = 33.4, b = 33.6, c = 2.3, and m = 9.1, chaotic attractors exist in system (1), as shown in Figure 1.

Compared with low-dimensional chaotic systems, high-dimensional hyperchaotic systems have more complex phase space and dynamic characteristics. At this time, system (1) has no less than two positive Lyapunov exponentials; thus it has hyperchaotic characteristics [10]. The randomness of the system is greatly increased [11] which means it has a better performance in color image encryption.

3. Image Encryption and Decryption Algorithm

The common image encryption algorithms mostly apply the model of "scrambling-diffusion" [12, 13]. Before scrambling, this algorithm firstly converts the pixel value of the image into gray code to expand the key space and improve the security.

3.1. Gray Code Conversion. Gray code is a typical binary communication coding format [14]. Its encoding rule is that there is only one-bit difference between two adjacent codes. The method of converting the natural binary code of bit j into a typical gray code is as follows:

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

Among them, $G(i)$ is typical gray code and $B(i)$ is natural binary code of the ith; $\bigoplus$ means exclusive or (XOR) operation. The method to convert a typical n-bit gray code into a natural binary code is as follows:

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

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

$$r_0 = \mathrm{mod}((L + W), 7) + 1 \tag{4}$$

where L and W represent the length and width in pixels.

3.2. 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 is used to iterate the chaotic system (1), and the four chaotic real value sequences of x,y,z, and u were obtained.

(2) Four chaos real value sequences are converted into a one-dimensional matrix. To reduce the impact of the initial value on the system, the previous n_0 results are given up and a one-dimensional chaos sequence C_i could be generated ($i = 1, 2, \ldots, N \times M \times 3$),

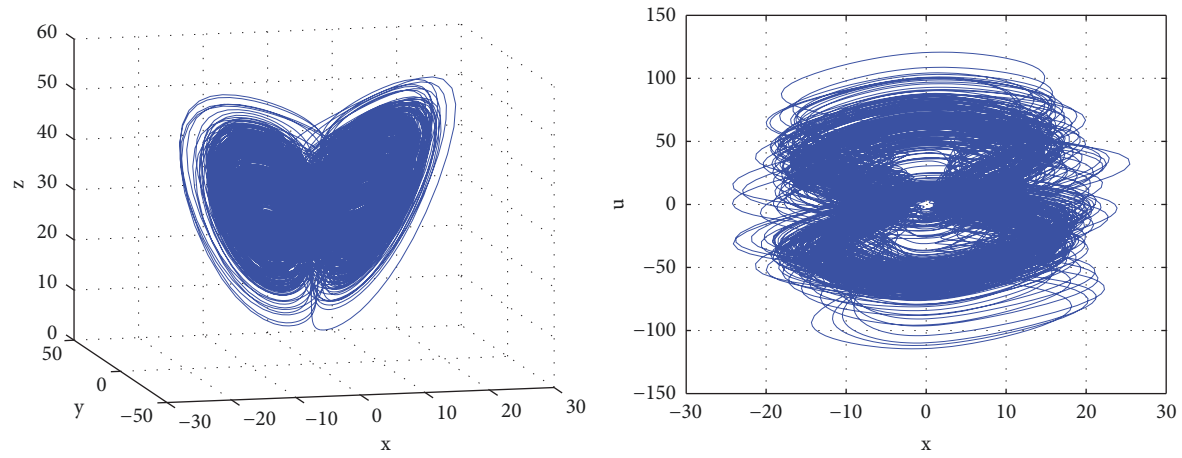
$$n_0 = \left[\left(\overline{R} + \overline{G} + \overline{B}\right) \times r_0\right] \tag{5}$$

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

(3) 3D matrix which has been converted to gray code is converted to a one-dimensional matrix P_i; then, the one-dimensional chaotic matrix C_i in step (2) is sorted and P_i changes positions synchronously. This step completes the whole-field pixel scrambling.

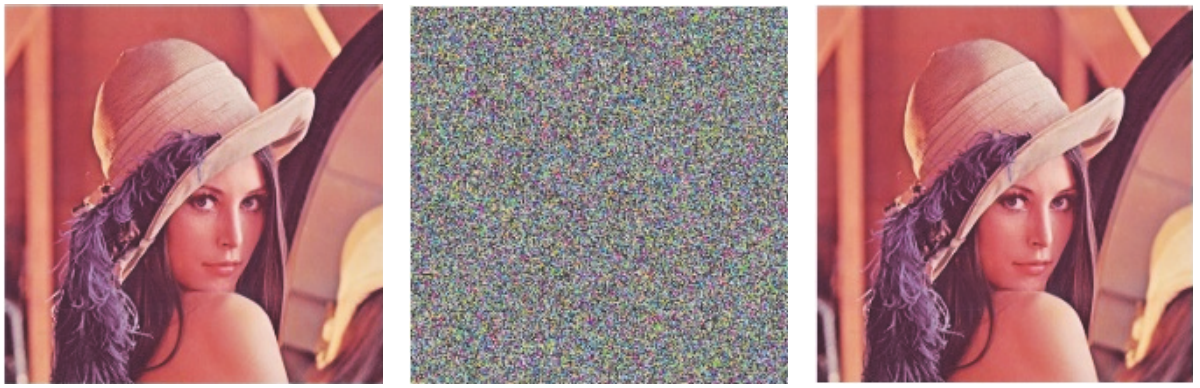
For color images, there is a strong correlation between adjacent pixels and each color component. The whole-field pixel scrambling method not only disrupts the correlation between adjacent pixels, but also changes the correlation among R, G, and B color components to achieve a better scrambling effect.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

3.3. Value Diffusion. In order to improve the security of image encryption, especially to equalize the histogram and hide the statistical information of plaintext, this algorithm uses the sequence generated by hyperchaotic system to diffuse the pixel value of image. The hyperchaotic sequence



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

Figure 1: Chaotic attractors of system (1).



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

Figure 2: Plaintext, ciphertext, and decrypted image.

transforming into one dimension is discretized as follows to obtain the key flow D_i:

$$D_i = \mathrm{mod}\left(round\left(abs\left(C_i\right)\right), 256\right) \quad (6)$$

The matrix generated by the XOR operation of scrambled image sequence with the key flow D_i is converted as the final output sequence.

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

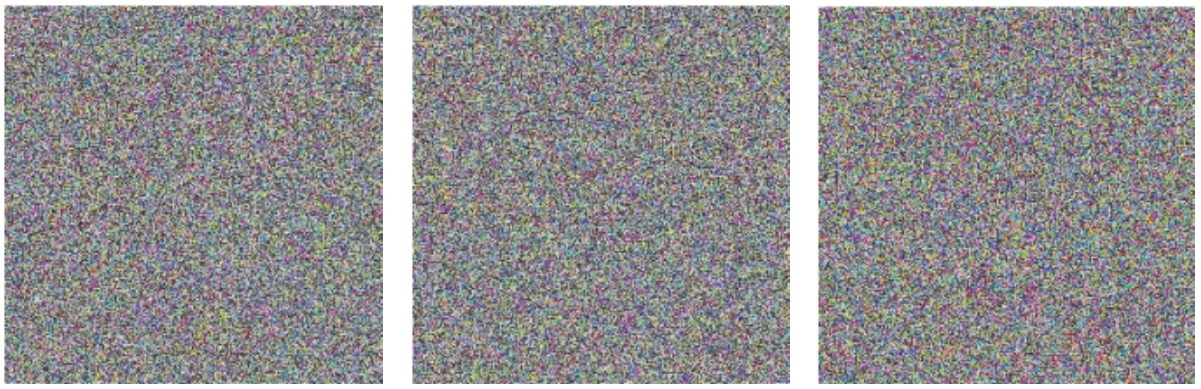
4. Simulation Experiment

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 = 33.4, b = 33.6, c = 2.3, and m = 9.1, and the initial values were $x_0 = 6.2$, $y_0 = 7.5$, $z_0 = 19.7$, and $u_0 = 16.3$. The total number of iterations in the image encryption process is $t = 5$. According to (4) and (5), the first round of encryption, and the times of gray code conversion of iterations is $r_0 = 2$ and the selection of chaotic sequence starts from $n_0 = 768$. 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 the same as the encryption key. The encryption and decryption results of the image are shown in Figure 2. The ciphertext image is disordered and the decrypted image is exactly the same as the plaintext image.

5. Analysis of Simulation Results

5.1. Key Sensitivity. To detect the key sensitivity of the algorithm, only one key was 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 $u_0 = 16.3000001$, $t = 6$, and $n_0 = 769$; the decrypted images are shown in Figure 3.

Although only one key was changed imperceptibly during every round, the ciphertext could not be decrypted precisely,



(a) $u_0 = 16.3000001$ (b) $t = 6$ (c) $n_0 = 769$

Figure 3: 3 Error decrypted images.

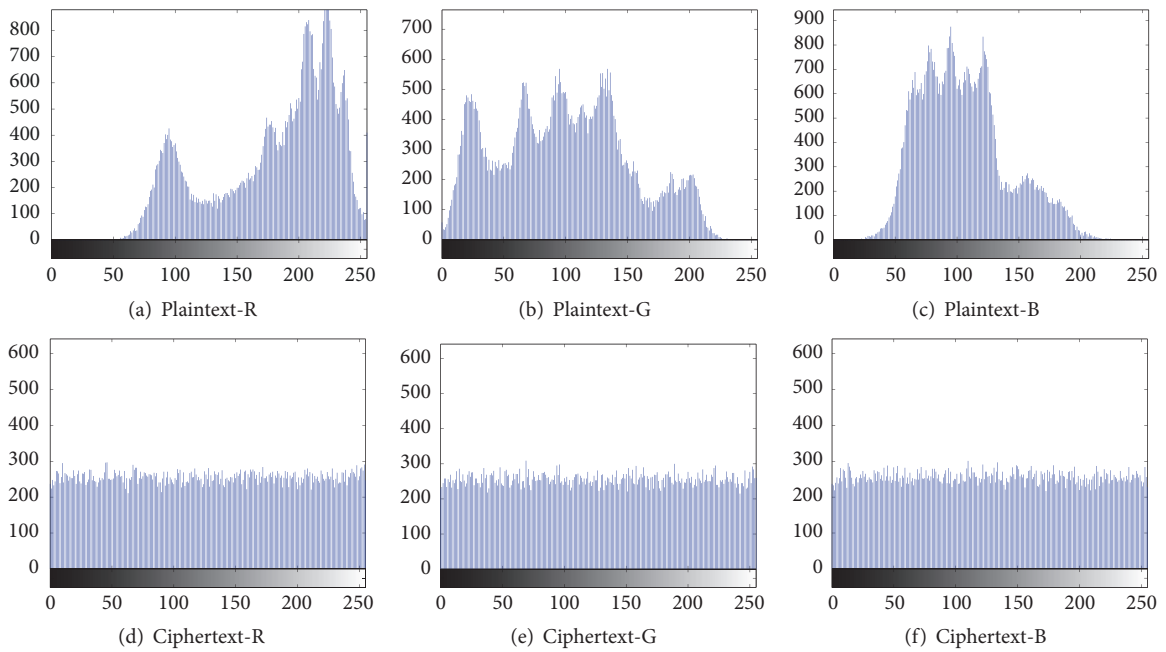


Figure 4: Histogram of plaintext and ciphertext.

therefore, this algorithm can be proved to have a strong key sensitivity.

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 [15]. One of the aims of image encryption is to increase the difficulty of extracting image histogram features by histogram equalization or generalization [16]. The histograms of the images before and after encryption are shown in Figure 4.

The histogram of color components tends to be uniform distribution, which is completely different from the plaintext distribution. Figure 4 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. The correlation coefficients in horizontal, vertical, and diagonal directions are calculated according to the following equations:

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

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

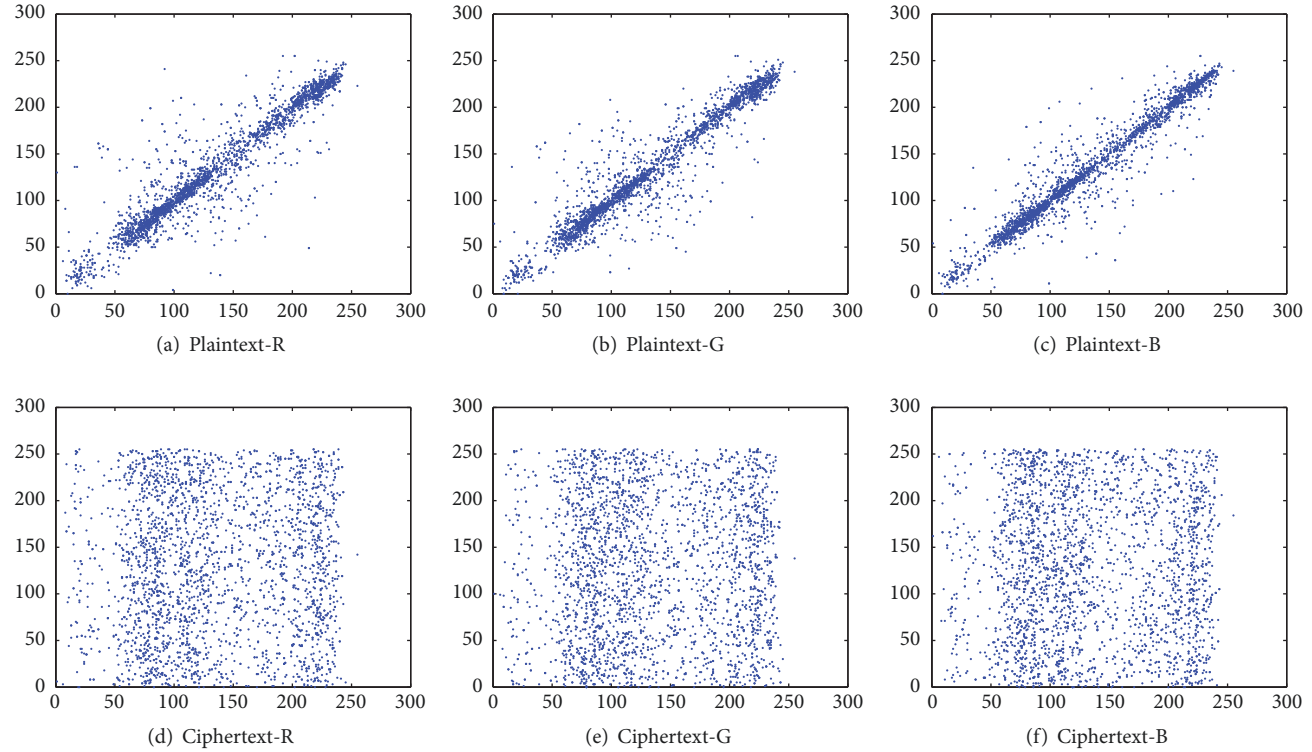


Figure 5: Correlation of pixel components in the diagonal direction of plaintext and ciphertext.

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

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

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

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 Figure 5.

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 Figures 5(a)–5(c). The scrambling and diffusion operation are aimed at reducing this correlation, which is shown as nearly uniform distribution in the region [0, 255], as shown in Figures 5(d)–5(f).

In fact, pixel values at the same relative position of different color components in color images are often highly correlated. Therefore, in the process of color image encryption, attention should be paid to reducing the correlation between pixel values at the same relative position of different components.

Some random points are randomly selected in plaintext and ciphertext. The pixel values of the three-color components R, G, and B represent the X, Y, and Z axis coordinates, the adjacent elements in the diagonal direction are plotted as the relationship diagram of the adjacent elements. The scatter diagram is shown in Figure 6, where the red points are the selected random points and the blue points are the pixels in the diagonal direction of the random points. For color plaintext images, the pixel values of components at the same relative position are highly correlated; as shown in Figure 6(a), the scattered points are distributed centrally around the line $x = y = z$, and the overlap degree between red and blue points is high; in Figure 6(b), the scattered points selected from ciphertext are randomly distributed in space and the overlap degree is low. As can be seen from Figure 6, plaintext images show obvious characteristics of centralized distribution, while ciphertext images show strong randomness.

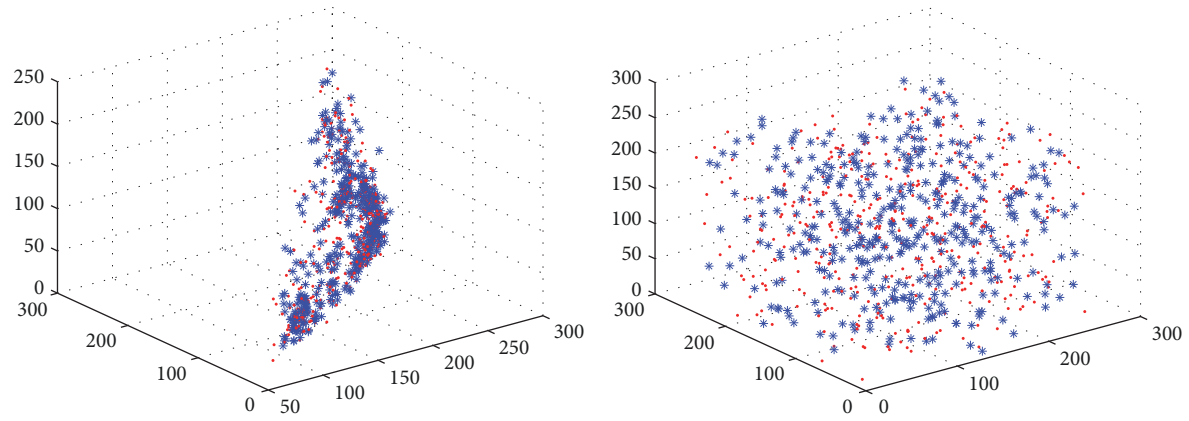
Table 1 and Figures 5 and 6 show that this encryption algorithm has good diffusion characteristics.

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 [21]. Therefore, the image encryption and decryption algorithm should adapt to clipping and noise to a certain extent. Figure 7 shows the images decrypted after a 1/4 clipping, adding 0.20 pepper noise, 0.1 Gaussian noise, Poisson noise, and speckle noise.

According to Figure 7, ciphertexts have been recovered well and plaintext information can be basically restored. Figure 7 indicates that this algorithm has good robustness.

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 [17]	-0.0102	0.0076	-0.0153
Ciphertext [18]	0.0129	0.0065	0.0013
Ciphertext [19]	0.0034	0.0050	0.0056
Ciphertext [20]	0.0173	-0.0112	-0.0125



(a) Plaintext-diagonal (b) Ciphertext-diagonal

Figure 6: RGB components are represented by the distribution of adjacent elements diagonally.

6. Antiattack Analysis

6.1. Antiexhaustive Attack. This algorithm is based on gray code and hyperchaos system of 4D. Parameters, initial value, the number of iterations, and image size are the encryption key. When the precision is set to 10^{14}, key space would be more than 10^{86}. According to the current calculation conditions, when the key space is larger than 2^{128}, ciphertext images can effectively resist violent attacks. The key space of this algorithm far exceeds this standard [22]. Thereunder, the key space of this encryption algorithm can effectively resist exhaustive attack.

6.2. Antientropy Attack. Image information entropy is used to represent the aggregation feature of image pixel value distribution [23]. 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 equation 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:

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

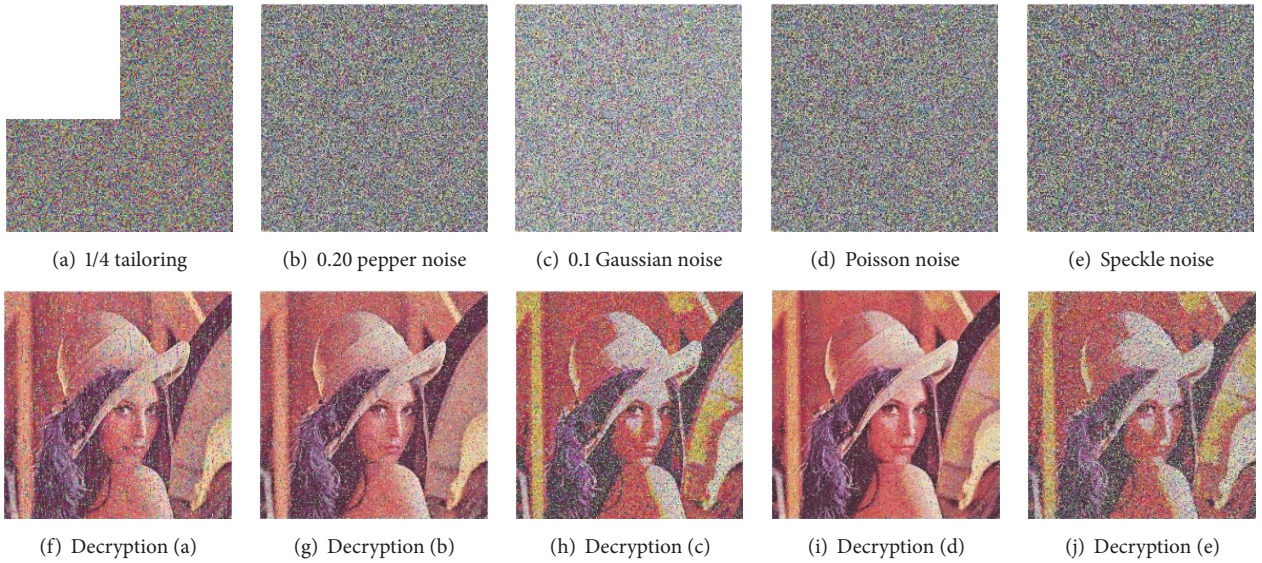
$k \in \{R, G, B\}$ and H_k represents the information entropy of each color component of RGB.

Table 2: Comparison of information entropy.

Image	Information Entropy
plaintext	7.4481
ciphertext	7.9991
ciphertext [4]	7.8556
ciphertext [17]	7.8534
ciphertext [20]	7.9994
ciphertext [24]	7.9551

According to Table 2, by comparing the information entropy of plaintext, ciphertext of this algorithm, and ciphertext image of [4, 17, 20, 24], it can be concluded that the information entropy value of the encrypted image of this algorithm is closer to the ideal value 8 which means that the encrypted image is closer to the random signal source and this algorithm has the ability to resist entropy attack.

6.3. Antiplaintext Attack. Since the starting sequence number of gray code and chaotic sequence is related to the attribute of plaintext image itself [25], the key obtained by selecting different plaintext is often different; "One Picture One Key" can basically be realized. The key deduced from the specific plaintext cannot correctly decrypt the other ciphertext [8]. Therefore, it can be concluded that this algorithm has good antiselective plaintext attack ability.



(a) 1/4 tailoring (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)

Figure 7: Decrypted images of 1/4 clipping and noises.

6.4. Antidifferential Attack. NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) [26] can be used to measure the sensitivity of encryption algorithm to plaintext, which is an essential indicator to measure the algorithm's resistance to differential attack. NPCR and UACI represent the proportion and degree of change of pixel values at corresponding positions. The more significant the proportion and degree of change is, the stronger the ability of algorithm's resistance to differential attack is. The calculation equation is as follows:

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

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

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

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

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

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

Table 3: Comparison of NPCR and UACI.

Image	NPCR/%	UACI/%
Ciphertext	99.63	33.52
Ciphertext [4]	99.63	33.54
Ciphertext [17]	86.55	33.47
Ciphertext [18]	99.63	33.51
Ciphertext [20]	99.60	30.34

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

The calculated results are shown in Table 3.

When the NPCR and UACI of the ciphertext 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 [4, 17, 18, 20], this algorithm is more sensitive to plaintext than the references listed in Table 3. Therefore, this algorithm can meet the security requirements and has good resistance to differential attack.

Data Availability

The data used to support the findings of this study are included within the article.

Additional Points

In this paper, a new color image encryption algorithm based on 4D hyperchaotic system and "transformation-scrambling-diffusion" is proposed. 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 and the algorithm shows better statistical characteristics. The process of encryption and decryption 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 antiplaintext attack ability. The simulation results show that this algorithm has good security and strong antidamage ability. As a result, this algorithm has a very high application value in the field of image encryption.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This project is funded by the National Natural Science Foundation of China (NSFC), with the Fund no. 61806219.

References

[1] V. B. Durdi, P. T. Kulkarni, and K. L. Sudha, "Selective encryption framework for secure multimedia transmission over wireless multimedia sensor networks," in *Proceedings of the International Conference on Data Engineering and Communication Technology*, 2017.

[2] S. Dhall, S. K. Pal, and K. Sharma, "New lightweight conditional encryption schemes for multimedia," in *Proceedings of the Third International Conference on Soft Computing for Problem Solving*, vol. 258 of *Advances in Intelligent Systems and Computing*, pp. 365–377, Springer India, New Delhi, India, 2014.

[3] Y. Song, S. Jia, and J. Qu, "A secure image encryption algorithm based on multiple one-dimensional chaotic systems," in *Proceedings of the IEEE International Conference on Computer & Communications*, 2017.

[4] Y. H. Zhang and B. Zhang, "Algorithm of image encrypting based on Logistic chaotic system," *Application Research of Computers*, vol. 32, no. 6, pp. 1770–1773, 2015.

[5] A. M. Abbas, "Image encryption based on independent component analysis and arnold's cat map," *Egyptian Informatics Journal*, vol. 17, no. 1, pp. 139–146, 2016.

[6] W. Ran, P. C. WEI, and A. Duan, "Image encryption algorithm based on multi-chaotic mapping and DNA coding," *Computer Engineering and Design*, vol. 7, 2018.

[7] N. Shaikh, S. Chapaneri, and D. Jayaswal, "Hyper chaotic color image cryptosystem," in *Proceedings of the IEEE International Conference on Advances in Computer Applications*, IEEE, 2017.

[8] X. L. Chai and Z. H. Gan, "New bit-level self-adaptive color image encryption algorithm based on hyperchaotic system," *Computer Science*, vol. 43, no. 4, pp. 134–139, 2016.

[9] L. Zhang and J. S. Tang, "Hopf bifurcation analysis and anticontrol of bifurcation of a four-dimensional hyperchaotic system," *Chinese Journal of Computational Mechanics*, vol. 2, 2018.

[10] H. Koçak and K. Palmer, "Lyapunov exponents and stability in interval maps," *Sema Journal*, vol. 51, no. 1, pp. 79–82, 2010.

[11] C. Wang, C. Fan, and Q. Ding, "Constructing discrete chaotic systems with positive lyapunov exponents," *International Journal of Bifurcation and Chaos*, vol. 28, no. 07, Article ID 1850084, 2018.

[12] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Optics and Lasers in Engineering*, vol. 91, pp. 41–52, 2017.

[13] M. H. Beheri, M. Amin, X. Song et al., "Quantum image encryption based on scrambling-diffusion (SD) approach," in *Proceedings of the International Conference on Frontiers of Signal Processing*, 2017.

[14] M. Zanin and A. N. Pisarchik, "Gray code permutation algorithm for high-dimensional data encryption," *Information Sciences*, vol. 270, no. 2, pp. 288–297, 2014.

[15] R. M. Thanki and A. M. Kothari, "Image enhancement in the spatial domain," *Digital Image Processing Using SCILAB*, 2019.

[16] M. Dwipayana, F. Arnia, and Z. Musliyana, "Histogram equalization smoothing for determining threshold accuracy on ancient document image binarization," *Journal of Physics Conference Series*, vol. 1019, 2018.

[17] Q. C. Chen, Z. J. Zhang, A. Q. Zhang et al., "New color image encryption algorithm based on hyper-chaos," *Computer & Digital Engineering*, vol. 6, 2018.

[18] X. Y. Wang, N. Wei, and D. D. Zhang, "A novel image encryption algorithm based on chaotic system and improved Gravity Model," *Optics Communications*, vol. 338, pp. 209–217, 2015.

[19] H. B. Lu and L. J. Wang, "Color image encryption algorithm of chaotic based on the hopfield network," *Journal of Jilin University (Information Science Edition)*, vol. 32, no. 2, pp. 131–137, 2014.

[20] O. Reyad, M. A. Mofaddel, W. M. Abd-Elhafiez, and M. Fathy, "A novel image encryption scheme based on different block sizes for grayscale and color images," in *Proceedings of the 12th International Conference on Computer Engineering and Systems, ICCES 2017*, pp. 455–461, Egypt, December 2017.

[21] X. Deng and Z. Liu, "An improved image denoising method applied in resisting mixed noise based on MCA and median filter," in *Proceedings of the 11th International Conference on Computational Intelligence and Security, CIS 2015*, China, 2016.

[22] W. Stallings, "Cryptography and network security: principles and practice," *International Journal of Engineering & Computer Science*, vol. 01, no. 01, pp. 121–136, 2011.

[23] D. Y. Tsai, Y. Lee, and E. Matsuyama, "Information entropy measure for evaluation of image quality," *Journal of Digital Imaging*, vol. 21, no. 3, pp. 338–347, 2008.

[24] J. Q. Li, F. M. Bai, and X. Q. Di, "Color image encryption algorithm based on hopfield chaotic neural networks," *Journal of Changchun University of Science and Technology (Natural Science Edition)*, vol. 35, no. 4, pp. 117–121, 2012.

[25] Y. Liu, Y.-A. Zheng, and L.-L. Mo, "Image encryption scheme based on hyperchaos system," *Journal of Central South University*, vol. 40, no. 1, pp. 121–126, 2009.

[26] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *IEEE Journal on Selected Areas in Communications*, pp. 31–38, April 2011.