Journal of Computers Vol. 31 No. 4, 2020, pp. 234-245
doi:10.3966/199115992020083104018

A Novel Color Image Encryption Algorithm Based on Logistic-Sine System and Hyper-Chaotic Lorenz System

Dong Li*

FuZhou Vocational Technical College, FuZhou 344000, China
lidong9310@126.com

Received 24 February 2019; Revised 20 July 2019; Accepted 26 August 2019

Abstract. A novel color image encryption algorithm based on Logistic-Sine System and hyper-chaotic Lorenz system is proposed. The architecture of permutation and diffusion is adopted. The plain image is firstly decomposed into R, G and B components. Considering the similar structure and strong correlations between the R, G, B components in color image, rows of G and B components are inserted into R component and the insert position is generated by Logistic-Sine System sequence. The proposed permutation strategy can reduce the high correlations between the R, G, B components and encrypt three components simultaneously. Furthermore, hyper-chaotic Lorenz system is employed to diffuse the shuffled image. Experimental results and security analyses prove that the proposed scheme can achieve good encryption effect and be robust against common attacks.

Keywords: color image encryption, diffusion, permutation

1 Introduction

With the rapid development of multimedia and Internet, the real time transmission of information plays a vital role in network communications, a mounting number of information is suffering from thefts and hostile attacks, so the security of information becomes more and more important. Digital image is one of the most common information formats, because of the inherent features of images, including bulk data capacity, high redundancy and strong correlation in adjacent pixels, making image encryption a research hotspot. Most conventional encryptions such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and International Data Encryption Algorithm (IDEA) are inefficient and not suitable for image encryption. In recent years, numbers of image encryption schemes such as fractional wavelet transform, quantum computation, DNA and Chaos have been proposed. Chaotic system possesses some special characteristics, including initial conditions sensitivity, unpredictability, pseudo-randomness, state ergodicity and so forth, which promote the chaos-based image encryption algorithm as a mainstream direction in cryptography.

The typical image encryption structure is permutation-diffusion, which is applied in most of the chaos-based image cryptosystems [1-2]. In the permutation phase, the pixel positions are relocated to reduce the high correlations between adjacent pixels within the plain image. While the pixel gray values are modified randomly to make the statistical property more uniform during the diffusion process. In recent years, some modified permutation–diffusion architectures have been proposed [3-6]. Zhang et al. [7] proposed an image encryption based on three-dimensional bit matrix permutation. In the new double random position permutation scheme, not only the bit location but also the weight of each bit can be simultaneously modified. Unfortunately, the flaws of Ref. [7] have been exposed and a chosen plaintext attack has been proposed to break the scheme by Wu et al. [8].

The chaotic systems used in image encryption are mainly classified into two major categories: one-dimensional systems (1D) and multi-dimensional (MD) systems. The 1D chaotic systems are easy to implement and take lower computation-cost because of the simple structure. But they are limited by some

[*] Corresponding Author

disadvantages such as narrow range of chaotic behaviors, small key space and weak security level. To overcome the shortcoming of the 1D chaotic systems, many researches have been proposed to produce new 1D chaotic system with better chaotic performance and improved properties. Zhou et al. [9] integrated two existing one-dimension chaotic maps to generate Logistic-Tent, Logistic-Sine and Tent-Sine systems, which have excellent chaotic properties, including a wide range of parameter settings, high values of Lyapunov exponents and the uniform distributed variant density function. Then, a novel image encryption algorithm was introduced to verify its applications in multimedia security. Dhall et al. [10] demonstrated cryptanalysis of Ref. [9], the 1D chaotic system was claimed to possess high strength because of the better chaotic properties of employed chaotic system and the use of random pixel insertion. But they identified several weaknesses in the encryption scheme and presented some improvements. In 2018, Pak et al. [11] introduced new improved 1D Logistic map and Sine map made by the output sequences of two same existing 1D chaotic maps. Pak and Huang [12] proposed a color image encryption scheme based on a linear– nonlinear–liner structure by using a 1D chaotic system model with good chaotic performances and large chaotic ranges. But Chen et al. [13] evaluated the security of the proposed scheme and found it can be derived under chosen-plaintext attack. The MD chaotic systems have complex structures and multiple parameters. They generate chaotic sequences with more complex dynamic characteristics and relatively larger key space [14-17].

A color image is composed of red (R), green (G) and blue (B) components, each component determine the intensity of this color image. In fact, R, G, B components have similar structure and any two of them have strong correlations. But three components are considered and calculated independently in most of the previous typical color image encryption algorithms, which are more time-consuming and more vulnerable to attack result from neglecting the correlations among components of color image [18].

Motivated by the above discussion, a new chaos-based color image encryption scheme is proposed. The main novelty of this paper can be summarized as follows: (1) a novel color image encryption using the new 1D Logistic-Sine system is proposed; (2) puts rows of G and B into R randomly, which encrypt the three components simultaneously without neglecting the correlations between R, G, B; (3) to further improve the security of the encryption scheme, the value of the color plain image will calculate the initial value of the Logistic-Sine system. Simulations have been carried out and compared with other color image schemes, which indicate the security and efficiency of proposed scheme

The rest of this paper is organized as follows. A brief description of the chaotic system is given in section 2. The proposed algorithm is concretely described in section 3. Simulation results and security analyses are presented in section 4. The last section draws a conclusion.

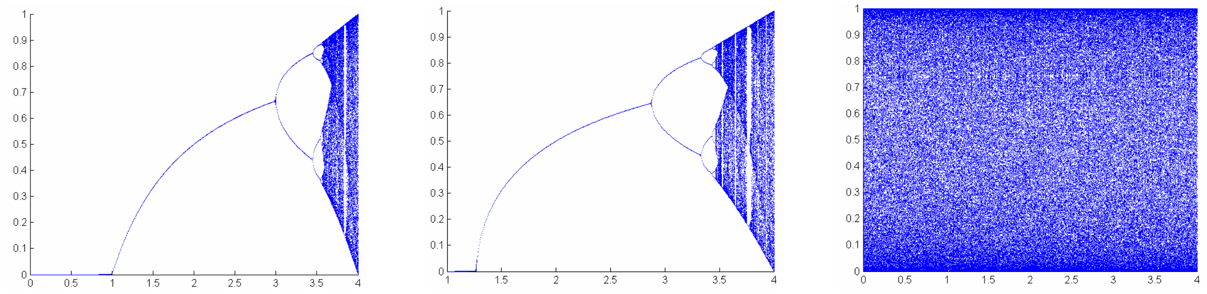
2 Preliminary Work

2.1 Logistic-Sine System

The Logistic-Sine system (denoted as LSS) defined as Eq. (1) is a nonlinear combination of the Logistic map and the Sine map.

$$\mu_{n+1} = (r\mu_n(1-\mu_n) + (4-r)\sin(\pi\mu_n)/4)\bmod 1\ . \tag{1}$$

where $\mathrm{mod}(x,y)$ returns the remainder after dividing x by y, parameter $r \in (0,4]$. The bifurcation diagrams of the Logistic map, the Sine map and the LSS are illustrated in Fig. 1. The chaotic behaviors of the LSS exist in the whole range of parameter settings and its chaotic sequences have a uniform-distribution within $[0,1]$. The LSS has larger chaotic ranges than the Logistic map and the Sine map, which means that LSS is more chaotic.



(a) Logistic map (b) Sine map (c) LSS

Fig. 1. The Bifurcation diagrams of the

2.2 Hyper-chaotic Lorenz System

The hyper-chaotic Lorenz system could be described by the following equations:

$$\begin{cases} \dot{x} = a(y-x)+w \\ \dot{y} = cx - y - xz \\ \dot{z} = xy - bz \\ \dot{w} = -yz + dw \end{cases} . \tag{2}$$

where x, y, z, w are state variables, a, b, c, d are control parameters. If $a=10$, $b=3/8$, $c=28$, $-1.52<d\le -0.06$, the system is in the hyper-chaotic state. When $d=-1$, the system exhibits hyper-chaotic behavior and has two positive Lyapunov exponents. Compared with the general chaotic systems, the dynamic behavior of the hyper-chaotic Lorenz system is more difficult to predict. Therefore it is a more valuable choice for image encryption.

3 Color Image Encryption and Decryption Algorithm

The proposed encryption algorithm is composed of confusion procedure and diffusion procedure. After we obtain the shuffled image with LSS, the hyper-chaotic Lorenz system is employed in the diffusion process. The encryption steps can be described as follows:

Step 1. Read the data of the plain color image I with the size of $m\times n$. Convert the color image into three two-dimensional matrixes $R_{m\times n}$, $G_{m\times n}$, $B_{m\times n}$. The value η is given by

$$\eta = \frac{\text{mod}\left(\text{average}, 256\right)}{256} . \tag{3}$$

where average is the average pixel value of I obtained by

$$\text{average} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}}{m\times n} . \tag{4}$$

where (i,j) is the position of image pixel and a_{ij} is the pixel value of plain image.

Step 2. Arrange $R_{m\times n}$ into one-dimensional matrix $R'_{1\times mn}$; then, merge $G_{m\times n}$, $B_{m\times n}$ into one matrix GB with $2m$ rows and n columns.

Step 3. The initial value u_1 of LSS is updated by

$$u_1 = \text{mod}(u_0 + \eta, 1) . \tag{5}$$

Step 4. Set the parameter r and iterate the LSS for N_1 times to obtain the sequence $\{\mu_i \mid i = 1,2,\ldots,2m\}$ by Eq. (1). The new chaotic sequence k_i is obtained by

$$k_i\text{=round}\left(\text{mod}\left(10^8 \times \left(\mu_i \times 10^{15} - \text{fix}\left(\mu_i \times 10^{15}\right)\right), L\right)\right) . \tag{6}$$

where L is the real-time length of matrix R' in Step 5, round(x) returns the value of x to the nearest integer, fix(y) rounds the value of y to the nearest integer towards zero.

Step 5. Insert each row of GB into the first k_i units of R', then shift the new matrix to the left, make sure the element $GB(i,1)$ to be the first element of matrix $R'_{1\times(mn+i\times n)}$,where, $i = 1,2,\ldots,2m$.

Step 6. Partition the transformed matrix R' into three recombined matrixes $R''_{1\times mn}$, $G''_{1\times mn}$, $B''_{1\times mn}$ from left to right.

Step 7. Substitute initial values x , y , z , w and parameters a , b , c , d in Eq. (2). Iterate the sequences for N_2 times to generate sequences $\{(x_i, y_i, z_i) \mid i = 1,2,\ldots,mn\}$. Three sequences are selected, hence there are four possible combinations. In this paper, we select the combination (x_i, y_i, z_i) .

Step 8. The sequences generated by hyper-chaotic Lorenz system are updated into integers ranging from 0 to 255 using Eq. (7):

$$\begin{cases} x_i = \text{mod}(\text{round}(x_i * 10^{15}), 256) \\ y_i = \text{mod}(\text{round}(y_i * 10^{15}), 256) \\ z_i = \text{mod}(\text{round}(z_i * 10^{15}), 256) \\ w_i = \text{mod}(\text{round}(w_i * 10^{15}), 256) \end{cases} . \tag{7}$$

Step 9. Perform XOR operation between three optimized sequences and the pixels of R'', G'', B'' to obtain R''', G''', B'''.

Step 10. Merge the components R''', G''', B''' into the encrypted color image I'.

The decryption process is an inverse process of the encryption.

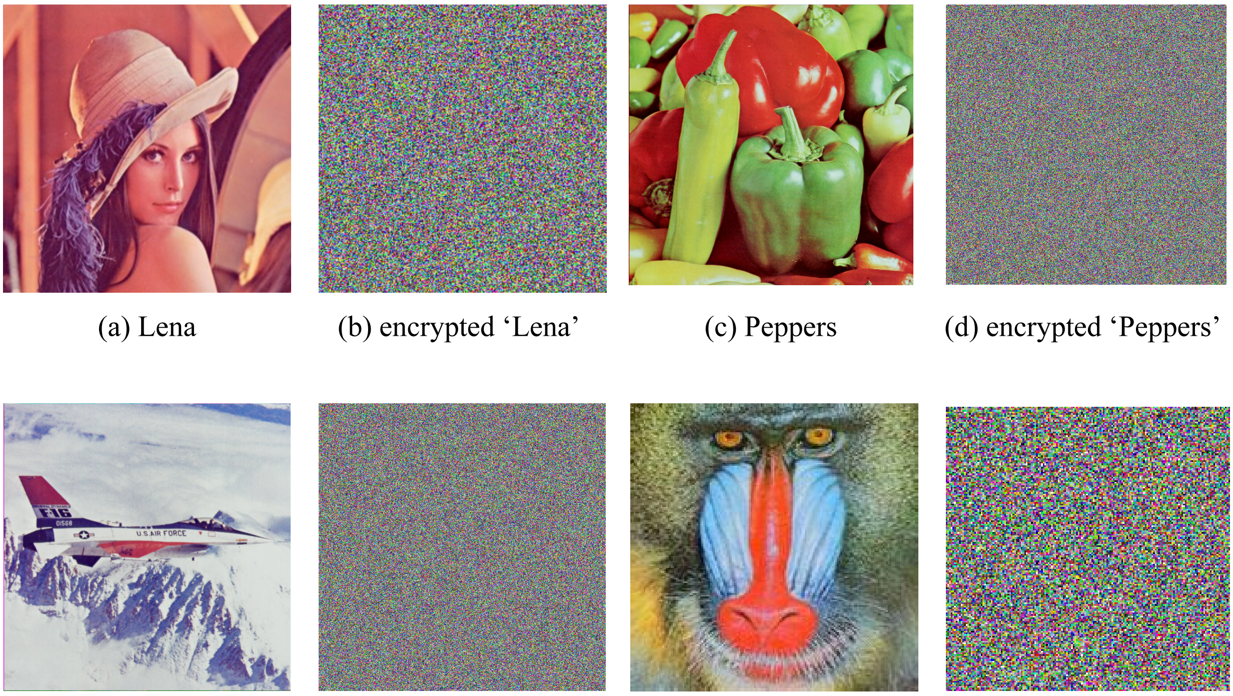
4 Simulation Result and Security Analysis

The standard color image 'Lena' (256×256), 'Peppers' (512×512),'Airplane' (512×512) and 'Baboon' (170×170) are selected as test images. The parameters are taken as $r = 3.28$, $a = 10$, $b = 8/3$, $c = 28$, $d = -0.79$, and the initial values are fixed as $\mu_0 = 0.6$, $x_1 = 0.77$, $y_1 = 1.99$, $z_1 = 0.32$, $w_1 = 0.99$. The encryption results are illustrated in Fig. 1. All the encrypted images are noise-like images, which are significantly different from the plain images. Furthermore, the proposed algorithm can be efficiently applied to color images of various sizes.

4.1 Key Space and Sensitivity Analysis

Key space is the total possible number of different keys which can be used in the encryption process. Any image encryption algorithm should have a sufficient large key space to resist the brute-force attack. In the proposed scheme, the initial conditions of LSS and hyper-chaotic Lorenz system can be used as keys, the total key space can reach to 10^{70} , which is large enough to resist the brute-force attack.

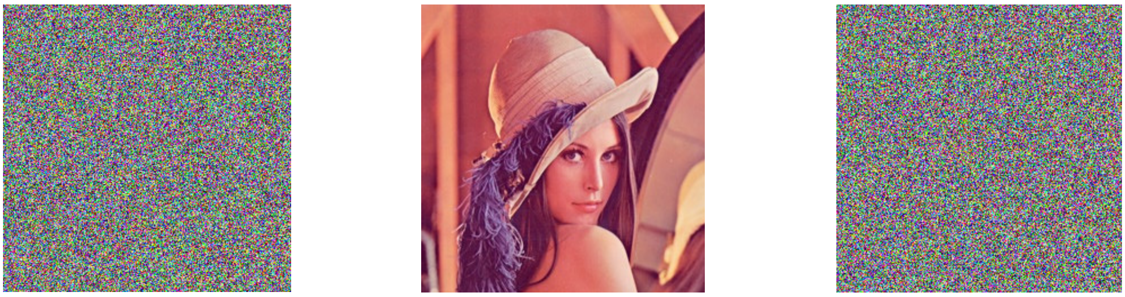
A good algorithm should also be sensitive to all keys in the cryptosystem. The decrypted image should be different from the original image even if one of the decryption keys has a slight difference. $x_1 = 0.77000000000001$ is employed to decrypt the encrypted image 'Lena' with other keys unchanged. The results are illustrated in Fig. 3, even if a slightly different key is used, the decrypted image is different from the plain one. The tests of sensitivity on other keys can be implemented in a similar way, which means that the algorithm is sensitive to secrete key.



(a) Lena (b) encrypted ‘Lena’ (c) Peppers (d) encrypted ‘Peppers’

(e) Airplane (f) encrypted ‘Airplane’ (g) Baboon (h) encrypted ‘Baboon’

Fig. 2. Encryption results



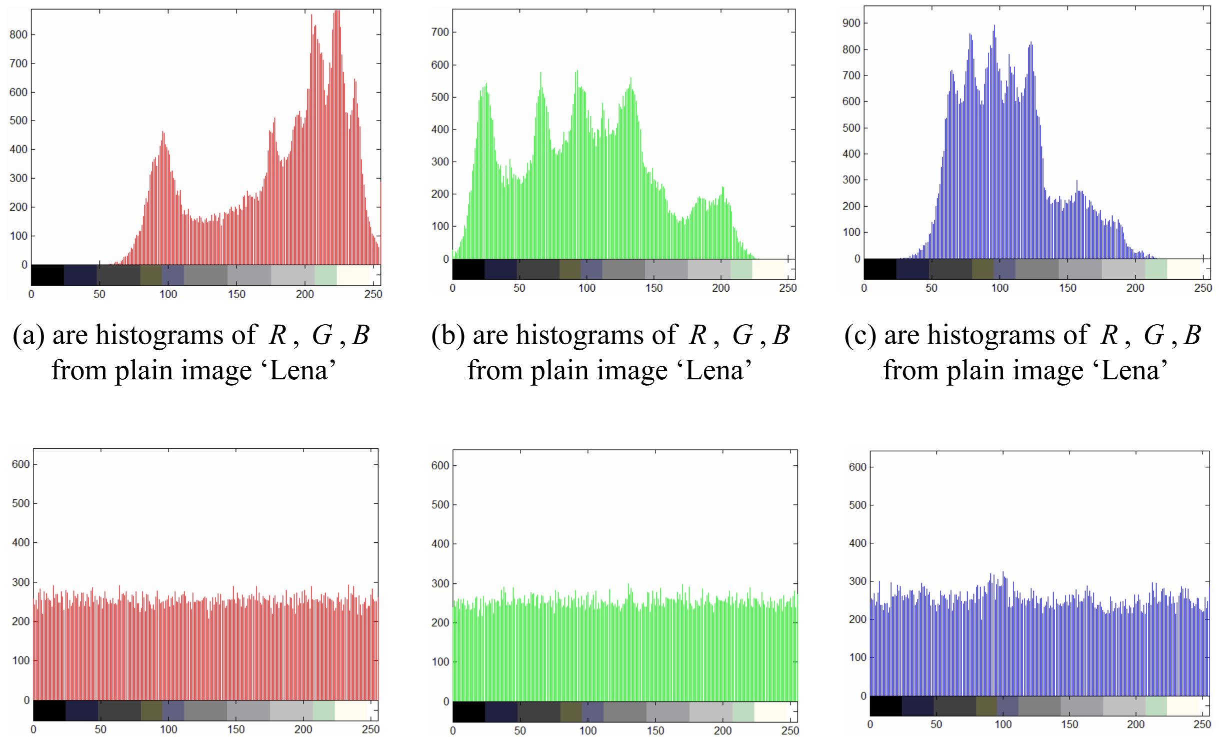
(a) encrypted ‘Lena’ (b) decrypted image of (c) decrypted image

Fig. 3. Sensitivity test of (a) with the same key; (a) with a tiny change (10^{-14}) in key x_1

4.2 Statistical Analysis

4.2.1 Histogram Analysis

The histogram features the distribution of the pixel values characterizing the statistical properties of an image. A good image encryption algorithm should make the histogram of cipher image uniform. The R, G, B histograms of ‘Lena’ and their counterparts of the encrypted ‘Lena’ are shown in Fig. 4. As we can see, the histograms of encrypted image are nearly uniform, and they are more flatter and smoother than those of the plain images.



(a) are histograms of R, G, B from plain image ‘Lena’

(b) are histograms of R, G, B from plain image ‘Lena’

(c) are histograms of R, G, B from plain image ‘Lena’

(d) are histograms of R, G, B from encrypted image ‘Lena’

(e) are histograms of R, G, B from encrypted image ‘Lena’

(f) are histograms of R, G, B from encrypted image ‘Lena’

Fig. 4. Histograms of original image and encrypted one

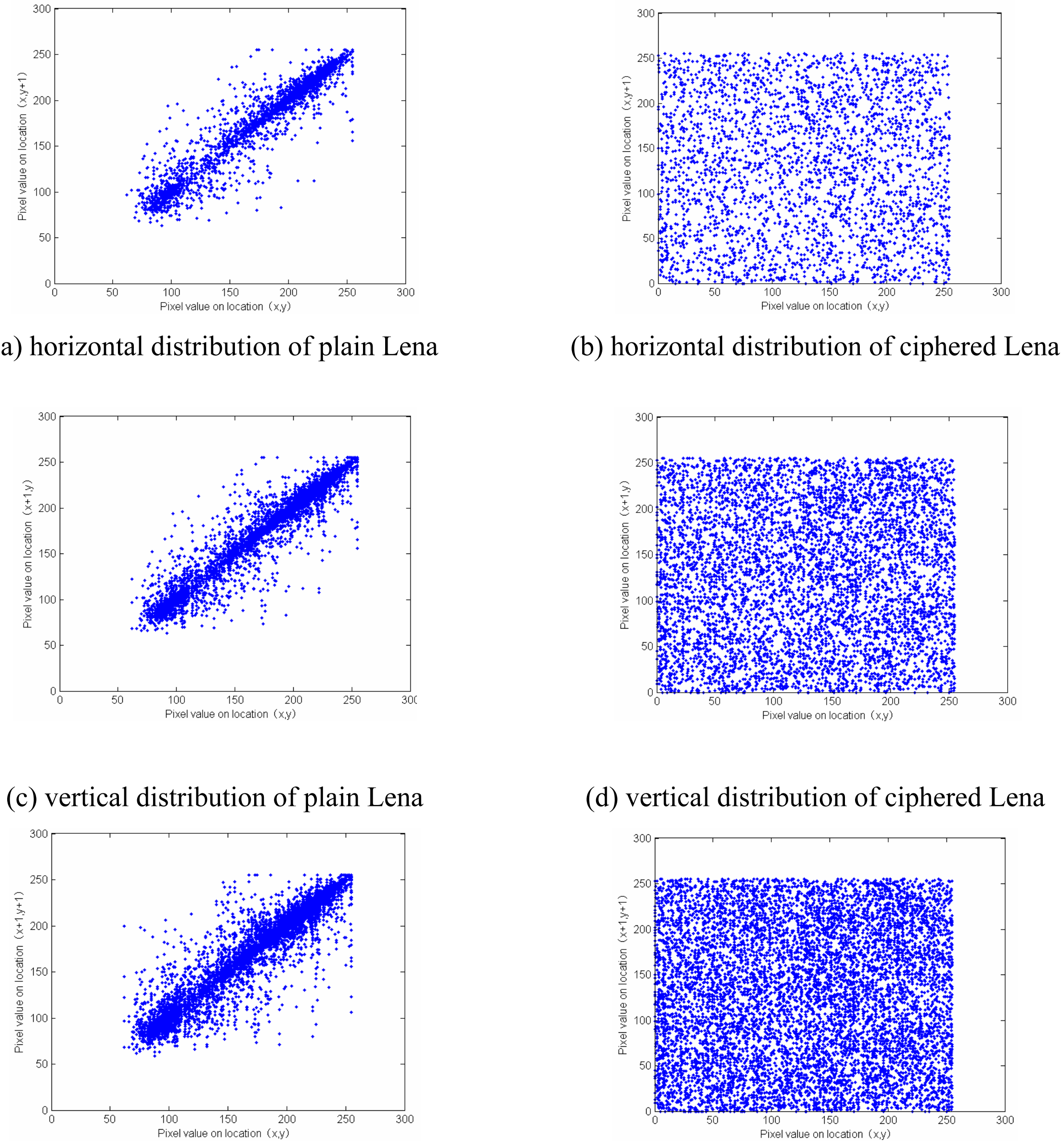
4.2.2 Correlation Coefficient Analysis

There are high correlations between the adjacent pixels in horizontal, vertical and diagonal directions. A good image encryption algorithm should reduce the correlations to avoid statistical attack. 3000 pairs of adjacent pixels from the plain image ‘Lena’ and the corresponding encrypted ‘Lena’ are randomly selected. The correlation coefficient of two adjacent pixels can be calculated as:

$$\begin{cases} R_{xy} = \dfrac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}} \\ E(x) = \dfrac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \dfrac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \\ \operatorname{cov}(x,y) = \dfrac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \end{cases} . \tag{8}$$

where x and y represent the gray values of two adjacent pixels, $\operatorname{cov}(x,y)$ is covariance and $D(x)$, $D(y)$ are variances. The poorer the correlation is, the more safety the method performs.

Fig. 5 represents the correlation of adjacent pixels in the plain image ‘Lena’ and its ciphered image. It is clear that the diagrams before encryption are centralized in all directions, while the correlations of the encrypted image are stochastic.



(a) horizontal distribution of plain Lena

(b) horizontal distribution of ciphered Lena

(c) vertical distribution of plain Lena

(d) vertical distribution of ciphered Lena

(e) diagonal distribution of plain Lena

(f) diagonal distribution of ciphered Lena

Fig. 5. Correlations between the plain image and the ciphered image

Table 1 lists the correlation coefficients of adjacent pixels of the plain image and the encrypted image. The result indicates that the correlations of two adjacent pixels in the plain image are close to 1 while those in the encrypted image come near to 0, which means that the encrypted image presents negligible correlation.

Table 1. Correlation coefficients of adjacent pixels

Correlation	Horizontal	Vertical	Diagonal
Lena	0.9765	0.9460	0.9246
Encrypted Lena	0.0011	−0.0012	−0.0017
Peppers	0.9681	0.9568	0.9599
Encrypted Peppers	−0.0011	−0.0012	0.0014
Airplane	0.9507	0.9794	0.9398
Encrypted Airplane	−0.0014	−0.0017	−0.0012
Baboon	0.9169	0.9231	0.8857
Encrypted Baboon	0.0017	0.0016	0.0012

For color image, there exists strong relationship between three components. Table 2 and Table 3 give the identical position correlations and adjacent position correlations between either two components of plain images and encrypted images, respectively. The results show that the correlation coefficients values are much smaller than those of the plain image. Moreover, the correlation coefficient in this paper is lower than that of Ref. [19-23], the comparison results show that the encryption effect is satisfactory. Thus the proposed algorithm can greatly decrease the high correlations among three components effectively and resist the statistical attacks.

Table 2. Identical position correlations between R, G, B components

Components	R, G	R, B	G, B
Lena	0.8900	0.7007	0.9228
Encrypted Lena	0.0015	−0.0018	−0.0013
Encrypted Lena [19]	−0.0038	−0.0510	0.0123
Encrypted Lena [20]	−0.0012	−0.0027	0.0008
Encrypted Lena [21]	0.0001	−0.0019	0.0029
Encrypted Lena [22]	−0.004	0.0032	−0.0063
Encrypted Lena [23]	-0.006	-0.0035	0.0076

Table 3. Adjacent position correlations between R, G, B components

Components	R, G	R, B	G, B
Lena	0.8411	0.6342	0.8371
Encrypted Lena	0.0012	0.0012	−0.0012
Encrypted Lena [19]	−0.0127	−0.0077	−0.0463
Encrypted Lena [20]	−0.0034	−0.0022	0.0199
Encrypted Lena [21]	−0.0038	0.0018	0.0053
Encrypted Lena [22]	−0.0009	0.0042	0.0031
Encrypted Lena [23]	−0.0093	0.0072	2.4163e-04

4.3 Information Entropy Analysis

The information entropy is the most outstanding feature of randomness. The entropy $H(m)$ of a message source m is defined by：

$$H(m)=\sum_{i=0}^{L} p(m_i)\log_2 \frac{1}{p(m_i)} . \qquad \textbf{(9)}$$

where m_i is the ith gray value for an L level gray image, $p(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. For a gray image of 8 bits, the ideal value of the information entropy is 8 bits. So the closer to 8 bits the information entropy is, the more random the image is. It could be seen from Table 4 that the entropies of the encrypted images are close to theoretical value 8. Moreover, as can be seen in Table 5, compared with Ref. [19-22], the information entropy of the proposed algorithm is closer to 8 bits, which reveals that the presented scheme is more secure against the entropy attack.

Table 4. Information entropy of encrypted image

image	Plain image			Encrypted image		
	R layer	G layer	B layer	R layer	G layer	B layer
Lena	7.2763	7.5834	7.0160	7.9974	7.9975	7.9973
Peppers	7.3388	7.5184	7.0584	7.9990	7.9993	7.9972
Airplane	6.7178	6.8055	6.2140	7.9994	7.9993	7.9987
Baboon	7.6420	7.3277	7.6414	7.9943	7.9944	7.9937

Table 5. Comparison of information entropy with other algorithms

Encrypted image	*R* layer	*G* layer	*B* layer
Lena	7.9974	7.9975	7.9973
Lena [19]	7.9965	7.9963	7.9963
Lena [20]	7.9973	7.9971	7.9968
Lena [21]	7.9967	7.9974	7.9973
Lena [22]	7.9973	7.9969	7.9971

4.4 Differential Attack

In order to test the influence of changing a single pixel in the plain image on the encrypted image, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) are computed as:

$$\begin{cases} \text{NPCR} = \dfrac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \\ \text{UACI} = \dfrac{1}{W \times H}\left[\sum_{i,j} \dfrac{\left|C(i,j) - C'(i,j)\right|}{2^L - 1}\right] \times 100\% \end{cases} . \tag{10}$$

where W and H are the width and the height of the encrypted image, L is the grey level, $C(i,j)$ and $C'(i,j)$ represent two encrypted images whose corresponding plain images have difference in only one pixel. $D(i,j)$ represents the difference between $C(i,j)$ and $C'(i,j)$. If $C(i,j) = C'(i,j)$, then $D(i,j) = 0$; otherwise, $D(i,j) = 1$.

The expected NPCR and UACI are calculated by:

$$\begin{cases} \text{NPCR}_{\text{expected}} = (1 - 1/L) \times 100\% \\ \text{UACI}_{\text{expected}} = \dfrac{1}{L^2}\left(\sum_{1}^{L-1} L(L+1)/(L-1)\right) \times 100\% \end{cases} . \tag{11}$$

For an 8-bit gray image, the theoretical values are $\text{NPCR} = 99.6094\%$, $\text{UACI} = 33.4635\%$. One pixel value in the original plain image is altered, then the original image and the modified image are encrypted with the same key. The calculated NPCR and UACI of the two encrypted images are tabulated in Table 6. The result shows that the NPCR and UACI approach to the ideal value, even if a tiny change in plain image can lead to a significant change in the encrypted image. Thus, the algorithm can resist differential attack.

Table 6. NPCR and UACI results (%)

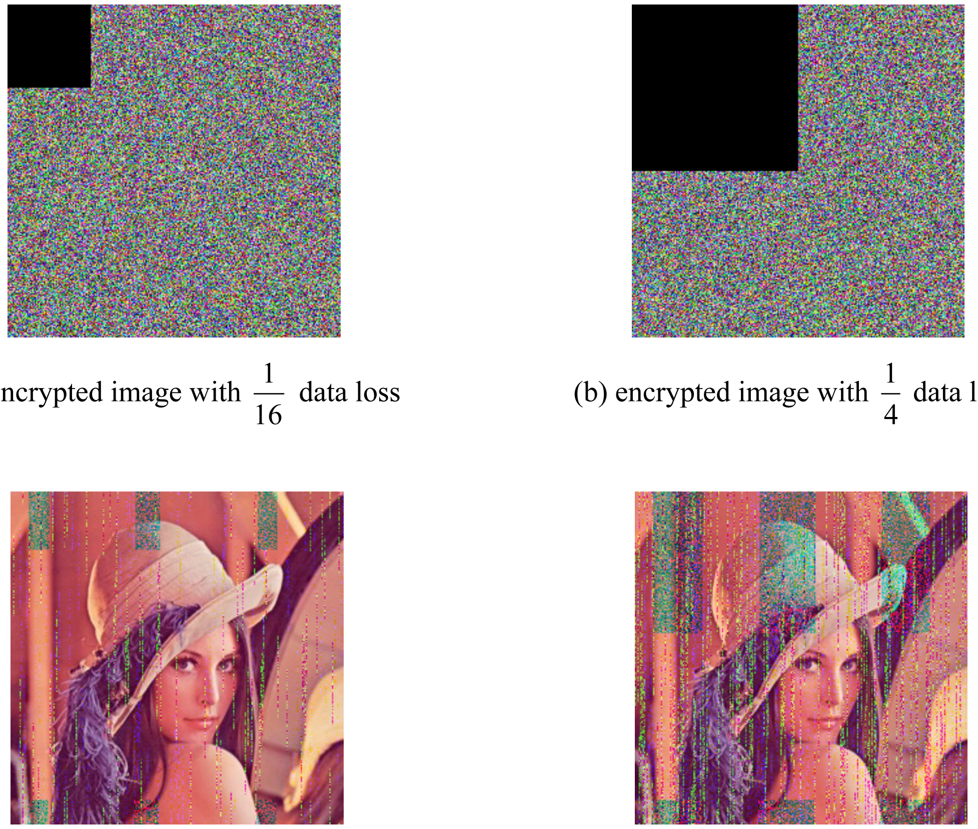
Image	NPCR			UACI		
	R layer	*G* layer	*B* layer	*R* layer	*G* layer	*B* layer
Lena	99.1318	99.4919	99.5224	33.0132	32.2300	33.1051

4.5 Robustness Analysis

The encrypted image may be attacked by the image processing operations and the geometrical distortions during transmission or storage. A good image encryption is supposed to robust against the cropping attack and the noise attack.

4.5.1 Cropping Attack

Cropping attack happens while the data of the encrypted image loss. A region of the encrypted image is replaced by the black pixels in this experiment. Fig. 6 (a) to Fig. 6(b) show the cropped encrypted images with different sizes, while Fig. 6(c) to Fig. 6(d) are the corresponding decrypted images. The decrypted image contains the main information of the original image.



(a) encrypted image with $\frac{1}{16}$ data loss

(b) encrypted image with $\frac{1}{4}$ data loss;

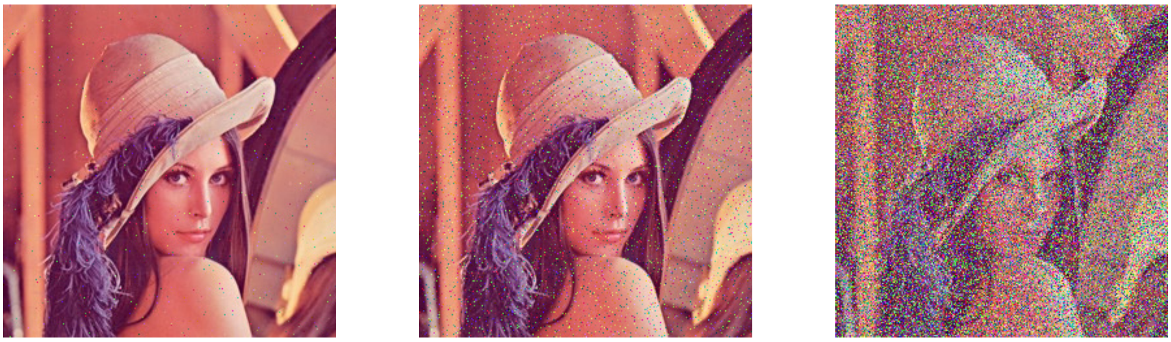
(c) decrypted image of (a)

(d) decrypted image of (b)

Fig. 6. Cropping attack

4.5.2 Noise Attack

To verify the ability against noise attack, the ‘salt & pepper’ noises with different variances d is added to the encrypted image. As can be seen in Fig. 7, the decrypted images are recognizable even if the encrypted images are affected by noises whose density is 0.005, 0.05 and 0.5, respectively.



(a) $d = 0.005$

(b) $d = 0.05$

(c) $d = 0.5$

Fig. 7. The decrypted images with ‘salt& pepper’ noise

5 Conclusion

A novel color image encryption algorithm based on chaos is proposed. LSS is exploited in the confusion process, whose initial condition depends on the pixel values of plain image. During the permutation, rows of G and B are inserted into R, three components are shuffled simultaneously rather than individually, which make the encryption algorithm more rapidly. Moreover, the hyper-chaotic Lorenz system is employed in diffusion process to enhance the encryption effect. The experiment results demonstrate that the proposed algorithm can not only achieve good encryption effect, but also disrupt the high correlations between the R, G, B components effectively. However, color image encryption scheme is only simulated in MATLAB. Thus, research on making the encryption scheme easier to implement in the hardware is the trend of the future.

Acknowledgements

The research is supported by Science and Technology Research Item of Jiangxi Provincial Department of Education (grant No. 171362).

References

[1] M.-X. Wang, X.-Y. Wang, Y.-Q. Zhang, Z.-G. Gao, A novel chaotic encryption scheme based on image segmentation and multiple diffusion models, Optics & Laser Technology 108(2018) 558-573.

[2] M. Essaid, I. Akharraz, A. Saaidi, A. Mouhib, A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map, Procedia Computer Science 127(2018) 539-548.

[3] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, A fast image encryption scheme with a novel pixel swapping-based confusion approach, Nonlinear Dynamics 77(4)(2014) 1191-1207.

[4] X. Zhang, Z. Zhao, Chaos-based image encryption with total shuffling and bidirectional diffusion, Nonlinear Dynamics 75(1-2)(2014) 319-330.

[5] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, Y.-S. Zhang, An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach, Communications in Nonlinear Science & Numerical Simulation 23(1-3)(2015) 294-310.

[6] X.-P. Zhang, R. Guo, H.-W. Chen, Z.-M. Zhao, J.-Y. Wang, Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes, Chinese Physics B 8(2018) 174-182.

[7] W. Zhang, H. Yu, Y.-L. Zhao, Z.-L. Zhu, Image encryption based on three-dimensional bit matrix permutation, Signal Processing 118(2016) 36-50

[8] J.-H. Wu, X.-F. Liao, B. Yang, Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation, Signal Processing 142(2018) 292-300.

[9] Y.-C. Zhou, L. Bao, C.L.P. Chen, A new 1D chaotic system for image encryption, Signal Processing 97(2014) 172-182.

[10] S. Dhall, S. K. Pal, K. Sharma, Cryptanalysis of image encryption scheme based on a new 1D chaotic system, Signal Processing 146(2018) 22-32.

[11] C. Pak, K. An, P.K. Jang, J. Kim, S. Kim. A novel bit-level color image encryption using improved 1D chaotic map, Multimedia Tools and Applications 78(9)(2018) 12027-12042.

[12] C. Pak, L.-L. Huang, A new color image encryption using combination of the 1D chaotic map, Signal Process 138(2017) 129-137.

[13] J.-X. Chen, F.-F. Han, W. Qian, Y.-D. Yao, Z.-L. Zhu, Cryptanalysis and improvement in an image encryption scheme using combination of the 1D chaotic map, Nonlinear Dynamics 93(8)(2018) 1-15.

[14] X.-L. Chai, Z.-H. Gan, Y. Lu, M.-H. Zhang, Y.-R. Chen, A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system, Chin. Phys. B 25(10)(2016)76-88

[15] D. Li, Y. Liu, L.-H. Gong, Color image encryption algorithm based on Chua's circuit and Chen's hyper-chaotic system, Journal of Information and Computational Science 12(3)(2015) 1021-1028.

[16] H.-W. Xue, J. Du, S.-L. Li, W.-J. Ma, Region of interest encryption for color images based on a hyperchaotic system with three positive Lyapunov exponets, Optics & Laser Technology 106(2018) 506-516.

[17] Y. Zhang, A chaotic system based image encryption scheme with identical encryption and decryption algorithm, Chinese Journal of Electronics 26(5)(2017) 1022-1031.

[18] G.-M. Zhou, D.-X. Zhang, Y.-J. Liu, Y. Yuan, Q. Liu, A novel image encryption algorithm based on chaos and Line map, Neurocomputing 169(2015) 150-157.

[19] X.-Y. Wang, L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos, Signal Processing 92(4)(2012) 1101-1108.

[20] Y.-S. Zhang, D. Xiao. Self-adaptive permutation and combined global diffusion for chaotic color image encryption, AEU - International Journal of Electronics and Communications 68(4)(2014) 361-368.

[21] L.-M. Zhang, K.-H. Sun, W.-H. Liu, S.-B. He, A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations, Chin. Phys. B 26(10)(2017) 100504-1-100504-9.

[22] X.-L Chai, X.-L. Fu, Z.-H Gan, Y. Lu, Y.-R. Chen, A color image cryptosystem based on dynamic DNA encryption and chaos, Signal Processing 155(2019) 44-62.

[23] P. Li, J. Xu, J. Mou, F.-F. Yang. Fractional-order 4D hyperchaotic memristive system and application in color image encryption, Journal on Image and Video Processing 1(2019) 1-11.