Send Orders for Reprints to reprints@benthamscience.ae

 The Open Cybernetics & Systemics Journal, 2015, *9,* 210-216

New Algorithm for Color Image Encryption Using Improved 1D Logistic Chaotic Map

Liu Rui*

College of Electronic Engineering, Xi' an University of Posts and Telecommunications, Xi' an, Shaanxi, 710121, P.R. China

Abstract: This paper introduces a simple and effective improved one-dimension (1D) Logistic chaotic map. Simulations and performance evaluations show that the improved 1D Logistic chaotic map is able to get larger chaotic range and better chaotic behaviors compared with its prototype map. To investigate its applications in multimedia security, I propose an efficient encryption algorithm for color image. Firstly, used an improved 1D Logistic chaotic map to confuse the addresses of a color image pixels. Secondly, decomposed the resultant image into 24-bits planes to get a bit-matrix containing a mixture of the red, green and blue elements. Finally, utilized global diffusion to permute the bit-matrix which makes the three elements influence each other effectively without neglecting the relativity between R, G and B. Computer simulations indicate that the proposed algorithm has some good properties such as easy to implement, large key space, and excellent encryption effect with just one round of iteration. Hence, it has application in secure communication to enhance the security of transmitting color image.

Keywords: Bit plane decomposition, color image encryption, global diffusion, logistic map.

1. INTRODUCTION

Based on the rapid development of network and multimedia technology, a large number of digital images are being transmitted and stored over the Internet or wireless networks. However, in such interconnected environments, it is becoming a challenge to keep information safe. Digital images security becomes increasingly important in many areas, *e.g.*, video surveillance and confidential transmission, telemedicine, military and medical communications.

Traditional cryptosystems such as DES and AES are found to be inefficient for image encryption because of some intrinsic features of the image, such as big size, high redundancy of data and strong correlation among neighboring pixels. To adapt those unique characteristics of image data and to improve efficiency and security of image encryption, numerous special image encryption algorithms were proposed, such as gray code [1], wave transmission [2], vector quantization [3], fractional wavelet transform [4], p-Fibonacci transform [5], and chaos [6-10]. Among those algorithms, the chaos-based algorithms have attracted the interest of many researchers from science and engineering realms due to some good properties of the chaotic, such as unpredictable data and strong sensitivity to initial conditions and system parameters. Therefore, many chaotic image encryption algorithms have been developed by directly utilizing existing chaotic systems/maps to their encryption processes. Make use of one-dimensional (1D) or multi-dimensional (MD) chaotic systems, many various image encryption schemes have been proposed in the past few years [11, 12], which considers the trade-offs between the security and computational complexity. The 1D chaotic systems have been widely used for their high efficiency and simple implementation, however, their weaknesses such as limited range of chaotic behaviors and non-uniform data distribution of output chaotic sequences, are disturbing [13]. MD chaotic systems, on the other hand, have more complex dynamical characteristics and multiple parameters. Nevertheless, multiple parameters increase the difficulty of their hardware/software implementations and computation complexity [14]. Hence, developing new 1D chaotic systems with better chaotic performance is needed.

Most of the proposed algorithms as to color images utilize the same method to encrypt each component, which are not distinguished from that as to gray images. So, it means that the same encryption steps needs to be repeated three times in these schemes and the correlations between R, G and B components are neglected.

According to the above discussion, this paper introduces a new chaotic map with a simple structure. It improves existing 1D Logistic chaotic map and has excellent chaotic properties, including a wide range of parameter settings and the uniform-distributed variant density function. These can be verified by simulation and analysis of the proposed chaotic map. To demonstrate its applications, I then introduce a novel color image encryption algorithm which combined global diffusion based on improved 1D Logistic chaotic map makes the three elements influence each other effectively without neglecting the correlations between R, G and B. Results of the analyses confirm that the proposed algorithm has some good properties such as easy to implement, large key

1874-110X/15

space, and excellent encryption effect with just one round of iteration. Hence, it can enhance the cryptosystem resistance against some typical attacks, and can be used in the secure transmission of color images.

2. LOGISTIC MAP

In mathematics, a chaotic map is a evolution function that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time parameter. Discrete maps usually take the form of iterated functions.

The Logistic map is a recurrence relation of degree 2, among 1D chaotic maps, it is widely used in many occasions. Its chaotic behavior can come from very simple nonlinear dynamical equation. Mathematically, the Logistic map is expressed as:

$$X_{n+1} = L(\mu, X_n) = \mu X_n (1 - X_n) \tag{1}$$

where X_n is a number between zero and one, and control parameter μ with range of (0, 4].

For evaluating chaotic properties of the Logistic map, Figs. (**1a**) and (**2a**) show the bifurcation diagram and Lyapunov Exponent, respectively. From Fig. (**1a**), we can see that the outputs of the system are more disordered when the value of μ is just near the four, so it is in chaotic state with range of [3.57, 4]. However, there has the blank window with in this range which proclaims not all parameters of the range can make the Logistic map to have chaotic behaviors. For the Lyapunov Exponent, a positive value is usually taken as an indication that the system is chaotic. As shown in Fig. (**2a**), the Lyapunov Exponents of the Logistic map are negative numbers when parameter μ<3.57. In addition to, the data range of the chaotic sequences is smaller than [0, 1], showing the non-uniform distribution in the range of [0, 1]. These narrow down the applications of the Logistic map.

Hence, an improved 1D Logistic map is introduced to alleviate these weaknesses.

2.1. Improved Logistic Map

The improved 1D Logistic map is defined as follows:

$$X_{n+1} = A_{LG}(\mu, X_n, k) = L(\mu, X_n) \times G(k) - floor\left(L(\mu, X_n) \times G(k)\right) \tag{2}$$

$$\begin{cases} L(\mu, X_n) = \mu X_n (1 - X_n) \\ G(k) = 2^k, \quad k \in Z^+, k \geq 8 \end{cases} \tag{3}$$

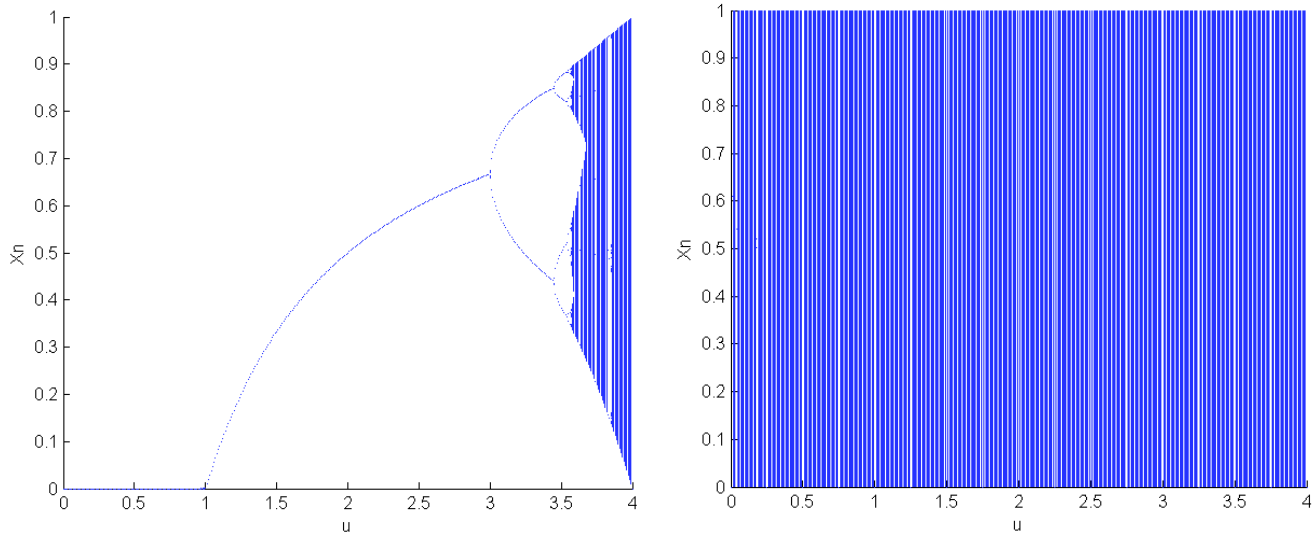
where μ and X_n are defined as above, G(k) is an adjustable function with parameter k. The larger the value of k, the chaotic characteristics of the improved system will be better (*e.g.*, k= 8 in the paper), floor is the rounding operation, and n is the iteration number. Here, the 'floor' operation is to ensure its output data within range of [0, 1]. An analysis of Equation (2) and Equation (3) shows the improved Logistic map hardware and software implementations are simple.

2.2. Comparison Logistic Map and Improved Logistic Map

To show the excellent performance of the improved Logistic map, three different aspects will be analyzed here include bifurcation diagram, Lyapunov exponent and histogram of the map.

The bifurcation diagram and Lyapunov Exponent of the improved Logistic map are shown in Figs. (**1b**) and (**2b**), respectively. As shown in Fig. (**1**), Logistic map has the limited data ranges within [0, 1], but the output sequences of its improved map spread out in the entire data range between 0 and 1.

The improved Logistic map has more complex chaotic properties than its prototype. When Logistic map is out of the chaotic range, the improved Logistic map can still have excellent chaotic behaviors. This can be demonstrated by the results shown in Fig. (**2**). The Lyapunov Exponents of improved Logistic map is greater than 0 almost in the entire



(a) **(b)**

Fig. (1). Bifurcation diagrams of the: (**a**) 1D Logistic chaotic map, (**b**) improved 1D Logistic chaotic map.

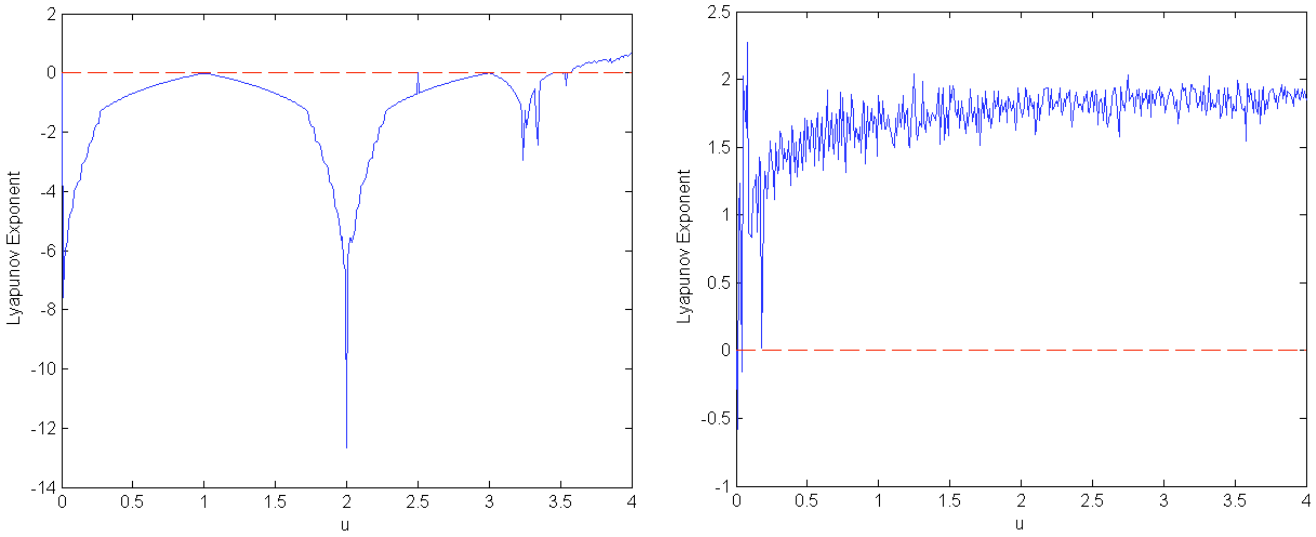


Fig. (2). Lyapunov Exponent of the: (**a**) 1D Logistic chaotic map, (**b**) improved 1D Logistic chaotic map.

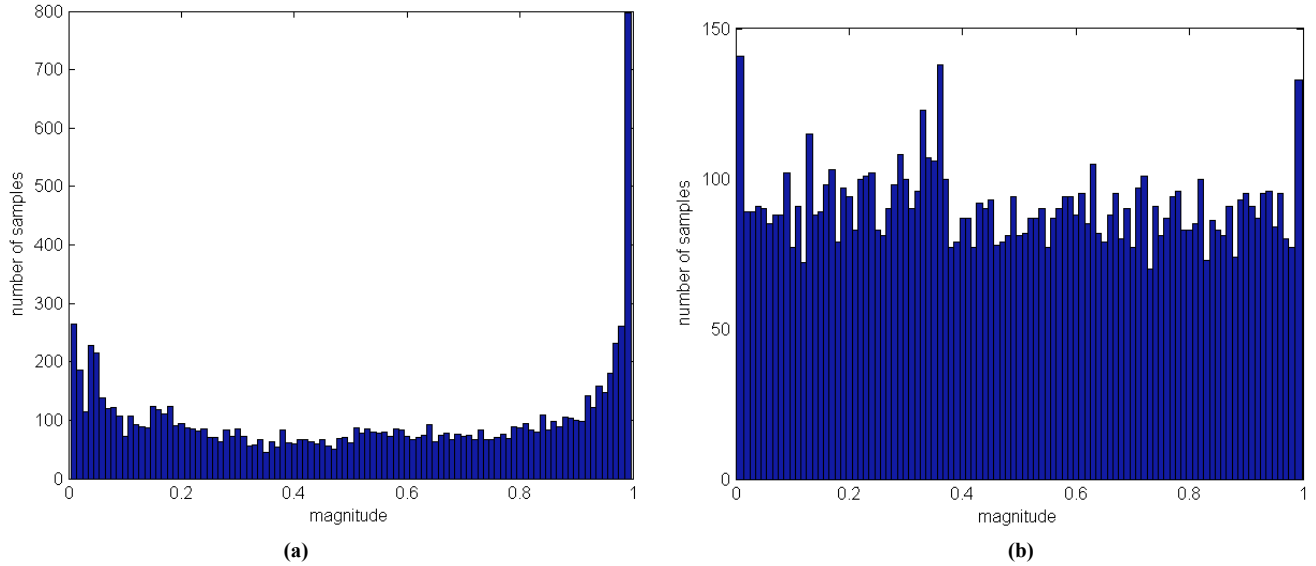


Fig. (3). Histogram of the: (**a**) 1D Logistic chaotic map, (**b**) improved 1D Logistic chaotic map.

range of the parameter settings $\mu \in (0, 4]$. However, the Logistic map has positive values of Lyapunov Exponents only within limited ranges.

A histogram is a graphical representation of the distribution of data, which can give a rough sense of the density of the data, and often for density estimation. To construct a histogram of chaotic map, I have divide the entire range of [0, 1] into 100 equal intervals, and then count how many output values of chaotic map fall into each interval. The histograms of 1D Logistic map and improved 1D Logistic map are shown in Fig. (**3**). Note that, The distribution of improved Logistic map density function is more uniform than its prototype.

Hence, the chaotic performance and the key size of the improved 1D Logistic map are all better than its prototype. These properties ensure it well suit able for different applications such as in formation security.

3. THE PROPOSED ENCRYPTION ALGORITHM

To verify the applications of the improved 1D Logistic map in information security, I propose an efficient encryption algorithm for color image in this section.

A block diagram of the proposed algorithm is shown in Fig. (**4**). It has a one-round-encryption structure, and can transform original color images randomly into different noise-like encrypted images with excellent confusion and diffusion properties.

3.1. Image Encryption

For M×N 24-bits RGB color image F, I carry out the encryption algorithm, which consists of two main steps pixels permutation and pixels value diffusion. Detailed procedure of the proposed encryption algorithm is described as follows:

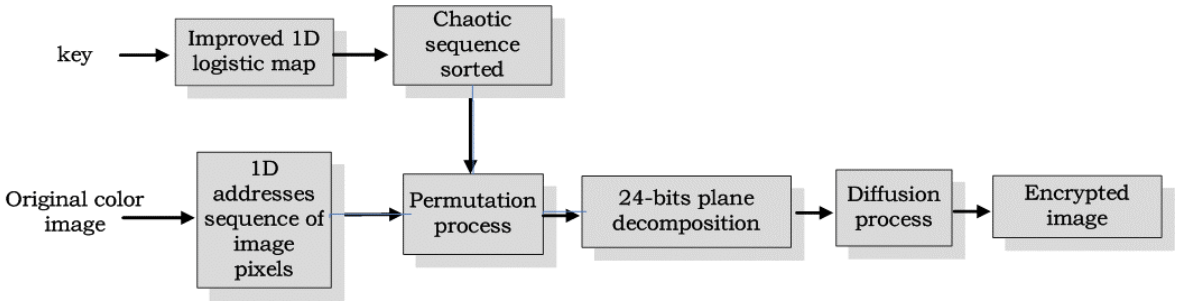


Fig. (4). The new color image encryption algorithm.

Step 1: Pseudorandom sequence X_n is generated by Equation (2)-(3). X_0, μ and k are the preset parameters as secret keys, where n=1,2,…, M×N.

Step 2: Sort X_n in ascending order, and obtain the new sequence X'_n. Use a sequence M_n, which has the same size as X_n, to record the address codes. In other words, M_n denotes the new subscript of X_n in the new sequence X'_n.

Step 3: Suppose the matrix of the red component of image F is F_R of size M×N. Similarly, the green component of image F is F_G and the blue component of image F is F_B. Then transfer the F_R to P_R of size 1×MN. Similarly, we can get P_G and P_B.

Step 4: According to the address codes M_n, I shuffle the positions of elements in the P_R to generate new sequence P'_R. Similarly, we can get P'_G and P'_B. At this point, pixels permutation is accomplished.

Step 5: Transform each pixel of P'_R into a 8-bit array, so the sequence is transformed into a binary matrix I_R of size 8×MN. Similarly, we can get I_G and I_B. Then, convert I_R, I_G and I_B into a large binary matrix S of size24×MN by Equation (4), which denote S(x, y), 1≤x≤24 and 1≤y≤MN. It includes the red, green and blue components of image F simultaneously.

$$S(x,y)=\begin{cases} I_R, for \quad 1\le x\le 8, \quad 1\le y\le MN \\ I_G, for \quad 9\le x\le 16, \quad 1\le y\le MN \\ I_B, for \quad 17\le x\le 24, \quad 1\le y\le MN \end{cases} \tag{4}$$

Step 6: Use global diffusion to sequentially modify the elements in the binary matrix S(x, y) to obtain a new binary matrix E(x, y) of size24×MN. The key principle of global diffusion was showed in Equation (5)-(6):

$$g=(x+y+offset) \bmod MN \tag{5}$$

$$E(25-x,y)=S(x,M(g)) \tag{6}$$

In the Equation (5), offset is a preset parameter as secret key, 1≤offset≤MN. In the Equation (6), M and S are defined as above.

It could make the three components of color image influence each other effectively without neglecting the relativities between R, G and B, so could get better diffusion results.

Step 7. Using Equation (7), to split the binary matrix E(x, y) into three binary matrix I'_R of size 8×MN, I'_G of size 8×MN and I'_B of size 8×MN.

$$\begin{cases} I'_R(x,y)=E(x,y), & 1\le x\le 8, \quad 1\le y\le MN \\ I'_G(x,y)=E(x+8,y), & 1\le x\le 8, \quad 1\le y\le MN \\ I'_B(x,y)=E(x+16,y), & 1\le x\le 8, \quad 1\le y\le MN \end{cases} \tag{7}$$

Step 7: Transform binary matrix I'_R into sequence T_R of size 1×MN, obviously, $0\le T_R\le 255$. Similarly, we can get T_G and T_B. Then transform three sequences T_R, T_G and T_B into three matrices C_R, C_G and C_B, which size are all M×N.

Step 8: Combine three matrices C_R, C_G and C_B to get a encrypted color image C with the size of M×N.

In short, the proposed scheme has at least three following advantages. In other words, the scheme is able to:

(1) Extract good chaotic sequences from an improved 1D Logistic map, which has excellent dynamical properties and easy to implement with both hardware and software.

(2) Encrypt images with excellent characteristics of confusion and diffusion with just one round of iteration.

(3) Enhance the cryptosystem resistance against some typical attacks.

3.2. Image Decryption

The decryption scheme is identical to the encryption procedure. The difference is that pixels permutation and pixels value diffusion are carried on with a reversed order in the decryption scheme.

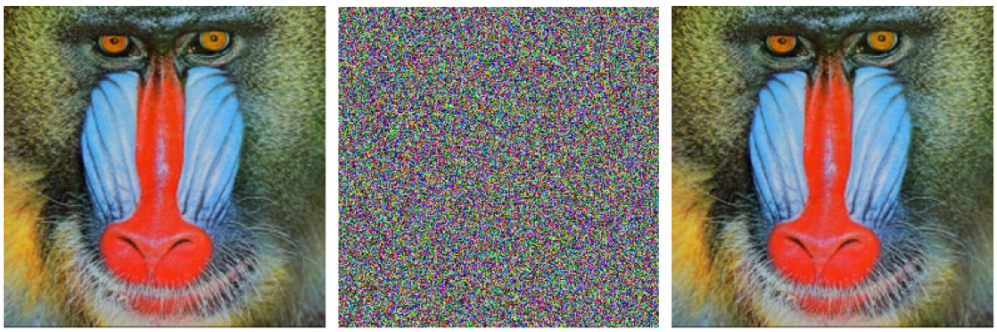
4. EXPERIMENTAL RESULTS AND ANALYSES

4.1. Experimental Results

To assess the availability of the encryption scheme, we conduct some simulations using MATLAB. The image for testing is a 24-bits RGB color image of size 256×256. The initial values X_0=0.25, the controlling parameters are μ=1.95164, k=8 and offset =3. Then result of encryption and decryption is showed as Fig. (**5**).

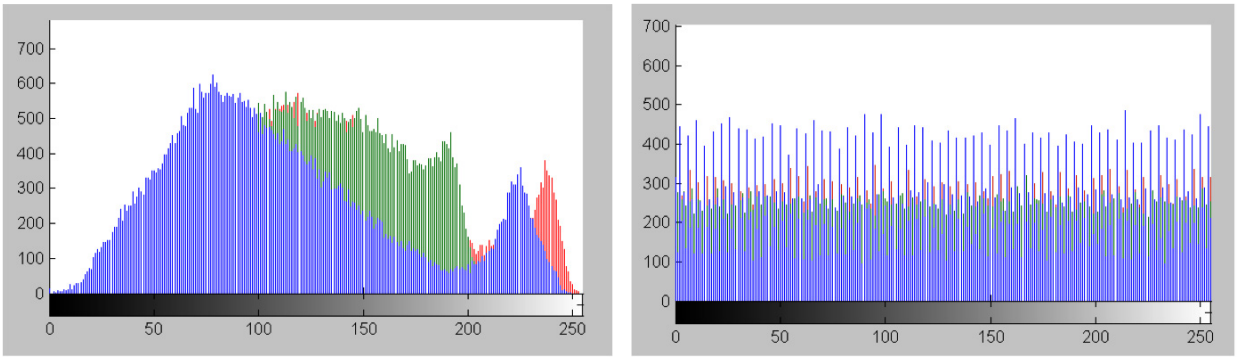
4.2. Histogram Analysis

Image histogram reflects the distribution of pixel values of an image. To resist statistic attacks we need a flat enough histogram for an encrypted image. Fig. (**6**) shows the histograms of the plain image and the encrypted image, which include the red, green and blue channels simultaneously. We can see that, the proposed scheme can get a histogram of the encrypted image with uniform distribution. This result indicates that it does not offer any clue to make use of statistical attack on the encryption image.



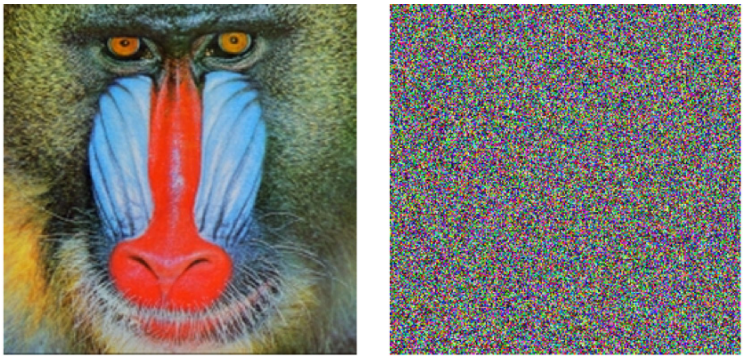
(a) (b) (c)

Fig. (5). Plain, encryption and decryption images: (**a**) plain color image, (**b**) encryption image, (**c**) decryption image.



(a) (b)

Fig. (6). Histogram analysis: (**a**) histogram of the plain image, (**b**) histogram of the encrypted image.



(a) (b)

Fig. (7). Key sensitivity: (**a**) decrypted image with correct key={1.95164, 0.25, 8, 3}, (**b**) decrypted image with wrong key={1.9516400000000001, 0.25, 8, 3}.

4.3. Key Space and Sensitivity Analysis

To offer a highly secure encryption algorithm, the key space should be large enough to let any brute force attack invalid. My encryption algorithm has four secret key, which they are μ, X_0, k and offset, where $\mu \in (0, 4]$ and $X_0 \in (0,1)$. the sensitivity variation is $\mu=10^{-16}$ and $X_0=10^{-16}$. So, the secret key space is almost 10^{40}.

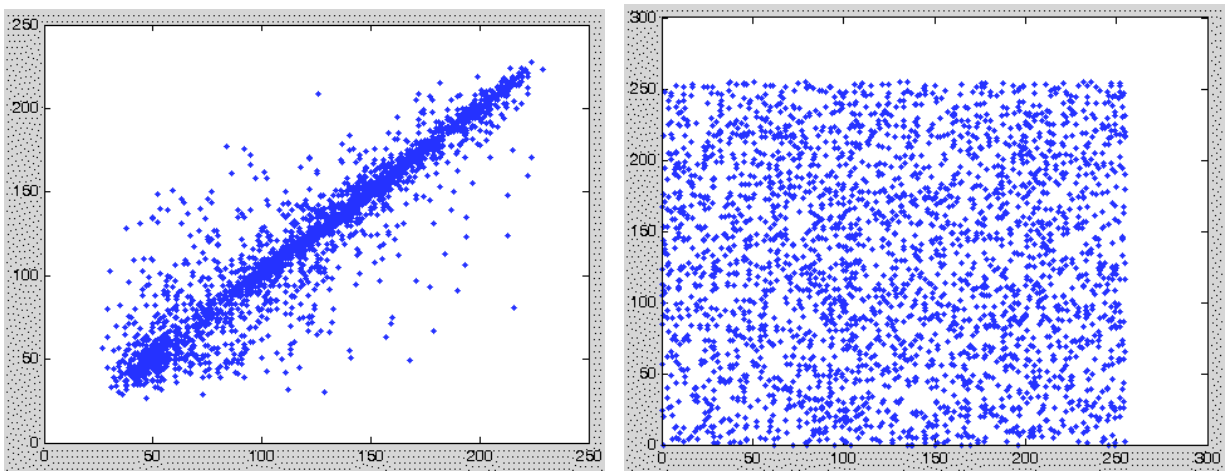
For the improved 1D Logistic chaotic map, the sensitivity to initial conditions is high. So the proposed scheme is very sensitive to slight differences in secret keys. Fig. (**7**) shows the decrypted image with the wrong key, which illustrates a slight fluctuation will lead to a wrong decryption.

4.4. Correlation of Two Adjacent Pixels

Correlation coefficient is employed to measure the correlations between two adjacent pixels in a certain direction in the image. The closer correlation coefficient come near to 1, the more correlations will strengthen. So, we can use it as a means for encryption performance estimation. The correlation coefficient is given in Equation (8) [15].

$$r_{xy} = \frac{\left|Cov(x,y)\right|}{\sqrt{D(x)} \cdot \sqrt{D(y)}}$$

$$\begin{cases} E(x) = \dfrac{1}{K}\sum_{i=1}^{K} x_i \\ D(x) = \dfrac{1}{K}\sum_{i=1}^{K}\left(x_i - E(x)\right)^2 \\ Cov(x,y) = \dfrac{1}{K}\sum_{i=1}^{K}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \end{cases} \tag{8}$$

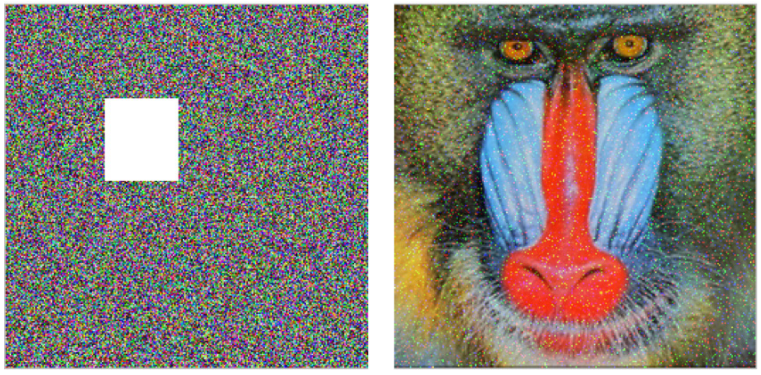


(a) **(b)**

Fig. (8). Correlation of two neighbor pixels: (**a**) distribution of horizontally neighbor pixels in the red channel of the plain image, (**b**) distribution of horizontally neighbor pixels in the red channel of the encrypted image.

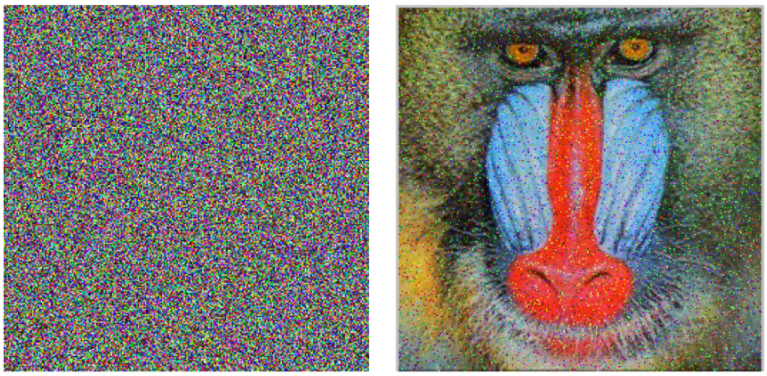
Table 1. Correlation coefficients of adjacent pixels.

Directions	Correlation Coefficients of Adjacent Pixels					
	Plain Image			*Encrypted Image*		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*
Horizontal direction	0.9678	0.9587	0.9724	0.0019	0.0027	0.0033
Vertical direction	0.9596	0.9168	0.9403	0.0022	0.0041	0.0021
Diagonal direction	0.9304	0.9378	0.9518	0.0043	0.0017	0.0036



(a) **(b)**

Fig. (9). Cutting attacks and reconstructed image: (**a**) the encrypted image with a 52×58 data loss, (**b**) reconstructed image of (**a**).



(a) **(b)**

Fig. (10). Noise attack and reconstructed image: (**a**) the encrypted image with 2% Gaussian noise, (**b**) reconstructed image of (**a**).

where x and y are gray-scale pixel values of the plain and encrypted images. 3000 pairs of neighbor pixels (in vertical, horizontal, and diagonal direction) from red, green and blue channel of the plain and encrypted images were randomly chose and the correlation coefficients are counted in three directions, separately. The result of the red channel of plain and its encrypted image in horizontal direction is plotted in Fig. (**8**). The numerical results are shown in Table **1**. These results suggest that the proposed scheme has the low correlation between neighbor pixels in all three directions.

4.5. Data Loss Attack and Noise Attack

In data transfer phase, images will undergo the data loss and noise now and then. To verify the encryption algorithm can whether or not resist the data loss and noise attacks. I do some tests on the encrypted image, such as cutting attack and noise attack, the experimental results are shown in Figs. (**9**) and (**10**).

From Figs. (**9**) and (**10**), we can see that the encrypted image is attacked by a data cut of size 52×58 and with 2% 'Gaussian' noise, respectively. The reconstructed images retain most of visual information of original color image, even if there are some spots in the decrypted image. These indicate the proposed algorithm has good performance to resist to the data loss and noise attacks.

CONCLUSION

In this paper, I have proposed an improved 1D Logistic chaotic map. Simulations and performance evaluations show that the improved Logistic chaotic map has some good properties including excellent chaotic behaviors, large chaotic range and uniform distributed density function. To examine practicability of the proposed chaotic map in information security, a novel color image encryption technique is introduced. The simulation results confirm that the proposed scheme can obtain excellent encryption effect with just one round of iteration and low time complexity, in addition it can resist against some well-known attacks. So it can be used in the secure transmission of color images.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work was supported by Scientific Research Program Funded by Shaanxi Provincial Education Department (Program No. 14JK1653), and the Natural Science Foundation of Shaanxi Province of China (No.2014JM8331, No. 2014JQ5183).

REFERENCES

[1] A.A. Abd El-Latif, L. Li, N. Wang, Q. Han, X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces", *Signal Process.*, vol. 93, pp. 2986-3000, Nov. 2013.

[2] X. Liao, S. Lai, Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission", *Signal Process*, vol. 90, pp. 2714-2722, 2010.

[3] T. H. Chen, C. S. Wu, "Compression-unimpaired batch-image encryption combining vector quantization and index compression", *Inf. Sci*, vol. 180, pp. 1690-1701, 2010.

[4] G. Bhatnagar, Q. M. J. Wu, B. Raman, "A new fractional random wavelet transform for fingerprint security", *IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum.,* vol. 42, pp. 262-275, Jan. 2012.

[5] Y. Zhou, K. Panetta, S. Agaian, C. L. P. Chen, "Image encryption using P-Fibonacci transform and decomposition", *Opt. Commun,* vol. 285, pp. 594-608, 2012.

[6] S. M. Seyedzadeh, S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", *Signal Process.*, vol. 92, pp. 1202-1215, 2012.

[7] Y. Zhou, L. Bao, C. L. Philip Chen, "A new 1D chaotic system for image encryption", *Signal Process.*, vol. 97, pp. 172-182, 2014.

[8] I. S. Sam, P. Devaraj, R. S. Bhuvaneswaran, "An intertwining chaotic maps based image encryption scheme", *Nonlinear Dyn*, vol. 69, pp. *1995-2007*, 2012.

[9] Y. Zhang, Di Xiao, "Self-adaptive permutation and combined global diffusion for chaotic color image encryption", *Int. J. Electron. Commun. (AEÜ)*, vol. 68, pp. 361-368, 2014.

[10] Y. Zhang, D. Xiao, Y. Shu, J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations", *Signal Process.,: Image Commun*., vol. 28, pp. 292-300, Mar. 2013.

[11] A. Kanso, M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map", *Commun. Nonlinear Sci. Numer. Simul*,, vol. 17, pp. 2943-2959, Jul. 2012.

[12] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps", *Chaos, Soliton. Fract.*, vol. 35, pp. 408-419, 2008.

[13] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process", *Multimed. Tools Appl*., vol. 71, pp. 1469-1497, 2014.

[14] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map", *Pattern Recognit. Lett*. vol. 31, pp. 347-354, 2010.

[15] S. Zhenwei, R. Honge, and Z. Jian, *A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformatio*n, ICYCS 08, Zhangjiajie, pp. 2942-2947, 2008.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014