A new color image encryption using combination of the 1D chaotic map

Chanil Pak, Lilian Huang

PII: S0165-1684(17)30093-2
DOI: 10.1016/j.sigpro.2017.03.011
Reference: SIGPRO 6423

To appear in: *Signal Processing*

Received date: 12 June 2016
Revised date: 28 February 2017
Accepted date: 8 March 2017

Please cite this article as: Chanil Pak, Lilian Huang, A new color image encryption using combination of the 1D chaotic map, *Signal Processing* (2017), doi: 10.1016/j.sigpro.2017.03.011

Highlights

- One method of making a simple and effective chaotic system by using a difference of the outputs sequences of two same existing one-dimension (1D) chaotic maps was introduced.
- A novel encryption system of linear-nonlinear-linear structure based on total shuffling was proposed and its accuracy was demonstrated by experiments.

A new color image encryption using combination of the 1D chaotic map

Chanil Pak[b,c], **Lilian Huang**[a]

[a] *College of Information and Communication, Harbin Engineering University, Harbin, Heilongjiang, 150001, China*

[b] *College of Mechanical and Electrical Engineering, Harbin Engineering University, Harbin, Heilongjiang, 150001, China*

[c] *Information Center, Kim Chaek University of Technology, Pyongyang 950003, DPR.Korea*

Abstract

This paper introduces a method of making a simple and effective chaotic system by using a difference of the output sequences of two same existing one-dimension (1D) chaotic maps. Simulations and performance evaluations show that the proposed system is able to produce a one-dimension (1D) chaotic system with better chaotic performances and larger chaotic ranges compared with the previous chaotic maps. To investigate its applications in image encryption, a novel encryption system of linear-nonlinear-linear structure based on total shuffling is proposed. The experiment demonstrated the accuracy of the encryption algorithm. Experiments and security analysis prove that the algorithm has an excellent performance in image encryption and various attacks.

Keywords : Chaos; Chaotic system, Image Encryption

1. Introduction

Nowadays information security is a vital problem in information communication. With the advancements of information technology, lots of digital contents are being stored and transmitted in various forms. As a result, the protection of digital contents data against irregular phenomena, such as illegal copying, and guarantee of their secure utility has become an important issue. In particular, compared to text data, some intrinsic features of image data, such as big size, high redundancy of data and strong correlation among neighbouring pixels are different with ordinary information. Furthermore, image data requires the strong real-time property in communication, therefore, an encryption method with fast speed and high security is needed. But the traditional block encryption being widely used now is found to be inefficient for real-time communication[1]. Hence a lot of image encryption methods using chaotic maps with high sensitivity to their initial conditions and system parameter values and simple structures are proposed. There are several algorithms used in image encryption, such as fractional wavelet transform[2, 3], p-Fibonacci transform[4], gray code[5], vector quantization[6] and chaos[10-29], have been proposed and among them the image encryption based on the chaotic map is being widely used. In some researches, S-box using the chaotic sequence is used in encryption[30-32].

This encryption system can be divided into two parts: 1) one part of generating the security key; 2) the other part of encryption by using the key. Chaotic maps used in generating the security key can be divided into two categories: one-dimension (1D) and multi-dimension (MD). At present, the MD chaotic maps are being widely applied to image encryption systems. But, owing to their complex structures and multiple parameters, the difficulty of their hardware/software implementations and the computation complexity are increased. On the contrary, 1D chaotic maps have an advantage that their structures are simple, they are easy to implement and have lower computation-cost.

But, they also have some problems: (1) the range of chaotic behaviours is limited; (2) the data

∗E-mail addresses: lilian_huang@163.com, pakchanil@hrbeu.edu.cn

distribution of output chaotic sequences is non-uniform[7-9]. It's very important to produce a new chaotic system with better chaotic performance.

Recently, various 1D chaotic map schemes with improved properties have been proposed and they can be divided into some categories: 1) generating new chaotic sequences by modifying the existing 1D chaotic map[10]; 2) generating new chaotic sequences by using the sum of output chaotic sequences of two 1D chaotic maps[11,12]; 3) generating new chaotic sequences by converting two 1D chaotic maps into 2D chaotic map[13,14]; 4) generating new chaotic sequences by using the output sequences of one 1D chaotic map as initial values of other 1D chaotic map[15]; 5) controlling the output sequences of several 1D chaotic maps by using parametric switching[16,17].

In encryption systems using the output sequences of chaotic map, the encryption part consists of a pair of linear(permutation)-nonlinear(diffusion) conversion and some encryption systems repeat this process to raise the strength of encryption. But the repetition of this linear-nonlinear process requires a large period of computation time and therefore gives an influence on the performance of the whole encryption system.

On the basis of analysis of the above mentioned problems, a 1D chaotic system model is proposed and evaluated by using Logistic, Sine and Chebyshev map in this paper. The simulation and analysis of range expansion possibility of system parameters used as the secret key, bifurcation property of chaotic map and Lyapunov exponent and information entropy evaluating chaotic performance demonstrate the accuracy of chaotic system. And on the basis of consideration of existing encryption system structures, an encryption system of linear-nonlinear-linear conversion structure based on chaotic map is proposed. Simulation and experiment will evaluate key space and key sensitivity, correlation and resistance to attack.

The paper is organized as follows. Section 2 briefly reviews the performance of the existing Logistic, Sine and Chebyshev maps. Section 3 makes a new chaotic map by using the above mentioned three 1D chaotic maps and demonstrate its accuracy. Section 4 proposes an encryption algorithm of linear-nonlinear-linear structure based on total shuffling. Section 5 shows the results of simulation and analysis. Section 6 shows conclusion.

2. Background

The 1D chaotic maps have simple structures, so that they are being widely used in image encryption. In this section, three 1D chaotic maps: Logistic, Sine and Chevyshev maps used for our new chaotic system will be briefly discussed.

2.1. Logistic map

The logistic map which is a simple dynamic nonlinear equation with complex chaotic behaviour is one of the famous 1D chaotic maps. It can de expressed in the following equation.

$$x_{n+1} = F_L(u, x_n) = u \times x_n \times (1 - x_n) \tag{1}$$

where u is a control parameter with range of $u \in (0, 4]$ and x_0 is the initial value of chaotic map, x_n is the output chaotic sequence.

To show its chaotic behaviour, its bifurcation diagram and Lyapunov Exponent are presented in Figs.1(a) and Figs.2(a). There are two problems in the Logistic map. First, its chaotic range is limited. As shown in Fig.1(a), its chaotic range is limited only within $[3.57, 4]$ and the control parameter u beyond the range cannot have chaotic behaviours. This can be verified in the diagram of Lyapunov Exponent in

Fig.2(a). The Lyapunov Exponent is a value for the quantitative evaluation of the chaotic performance. When the Lyapunov Exponent has a positive value, the chaotic map has a chaotic property and the larger the value is, the better the chaotic performance. As shown in Fig.2(a), the Lyapunov Exponents of the Logistic map are smaller than zero when parameter $u < 3.57$. It means that they have no chaotic behaviours. Secondly, the data distribution of the output chaotic sequences is non-uniform. As shown in Fig.1(a), the data range of the chaotic sequences is within $[0, 1]$, showing the non-uniform distribution in the range of $[0, 1]$. In the encryption system, the generated chaotic sequences are used in the process of permutation and diffusion of pixels or bits of the original image. Therefore, the non-uniform output chaotic sequences have some influences not only on the distribution of encrypted image data, but also on the performance of the encryption system. As the encrypted image should have close correlation with the security key, it is important to use a good key generation algorithm. These problems narrow down the applications of Logistic map.

2.2. Sine map

The Sine map is one of 1D chaotic maps and has a similar chaotic behaviour with the Logistic map. The definition can be described by the following equation.

$$x_{n+1} = F_S(r, x_n) = r \times sin(\pi \times x_n) \tag{2}$$

where parameter $r \in (0, 1]$ and x_n is the output chaotic sequence.

Its bifurcation diagram and Lyapunov Exponent diagram are shown in Fig.1(b) and Fig.2(b). It may be observed from these figures that the sine map has a similar property with the Logistic map.

2.3. Chebyshev map

The Chebyshev map is also one of 1D chaotic maps and can be described by the following equation.

$$x_{n+1} = F_C(a, x_n) = cos(a \times arccosx_n) \tag{3}$$

where parameter $a \in N$.

Its bifurcation diagram and Lyapunov Exponent diagram are shown in Fig.1(c) and Fig.2(c). As may be observed, when parameter $a > 1$, it has a chaotic behaviour and the value range of the output chaotic sequences is $[-1, 1]$. Although it has a chaotic behaviour in the range, the distribution of the output sequences is non-uniform in the range of $a \in [1, 2]$.

3. A new chaotic system

In this section, a new chaotic system will be proposed to solve the problems mentioned in section 2. To verify its accuracy, three 1D chaotic maps mentioned above are used.

3.1. System structure

The new chaotic system map is defined by the following equation.

$$x_{n+1} = F(u, x_n, k) = F_{chaos}(u, x_n) \times G(k) - floor(F_{chaos}(u, x_n) \times G(k)) \tag{4}$$

$$where \quad G(k) = 2^k, 8 \leq k \leq 20$$

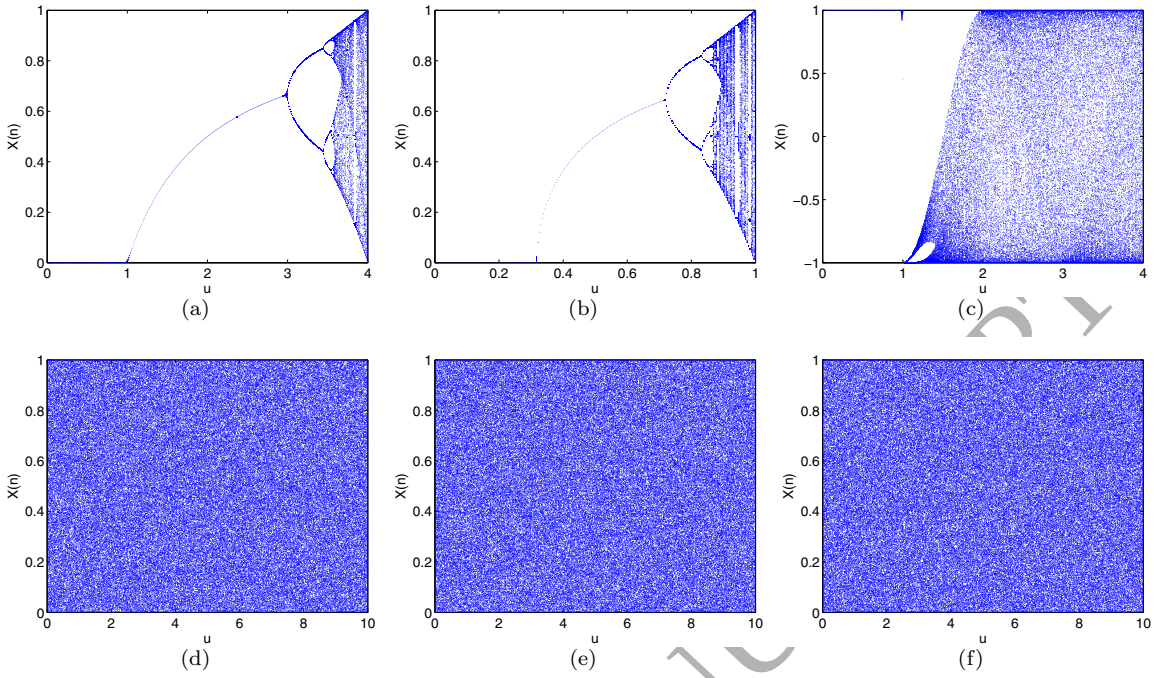


Fig.1. The bifurcation diagrams of the (a) Logistic map; (b) Sine map; (c) Chebyshev map; (d) LLS; (e) SSS; (f) CCS.

where $F_{chaos}(u, x_n)$ is one of 1D chaotic maps mentioned above and $F(u, x_n, k)$ is a newly made chaotic map. u is a control parameter which has no limited range. In other words, $F(u, x_n, k)$ still has a chaotic property in the expanded range of $u \in (0, 10]$ lager than chaotic range of the existing 1D chaotic maps. This is the result of 'floor' operation to ensure that the output chaotic sequences are in the range of $(0, 1]$. x_n is the sequence of the chaotic map, n is the iteration number, and $G(k)$ is an adjustable function with parameter k. When k is in the range of $[8, 20]$, the new chaotic system has a good chaotic performance and the larger the value of k in it, the better its chaotic performance. The value range of k was confirmed in the experiment.

In the paper, the parameter u is set to be in the range of $(0, 10]$ and k is set to 14. The new proposed chaotic system has a simple structure and is easy to implement by software and hardware. Lots of new chaotic sequences can be made by using the proposed chaotic system.

3.2. Verification of the new chaotic system

To verify the performance of the proposed chaotic system, three existing 1D chaotic maps discussed above have been used.

3.2.1. Logistic-Logistic map

The system of Logistic map combined by equation(4) is called Logistic-Logistic system(LLS). The combination equation is as follows.

$$x_{n+1} = u \times x_n \times (1 - x_n) \times 2^{14} - floor(u \times x_n \times (1 - x_n) \times 2^{14}) \tag{5}$$

where the parameter $u \in (0, 10]$ and x_0 is the initial value of the sequence.

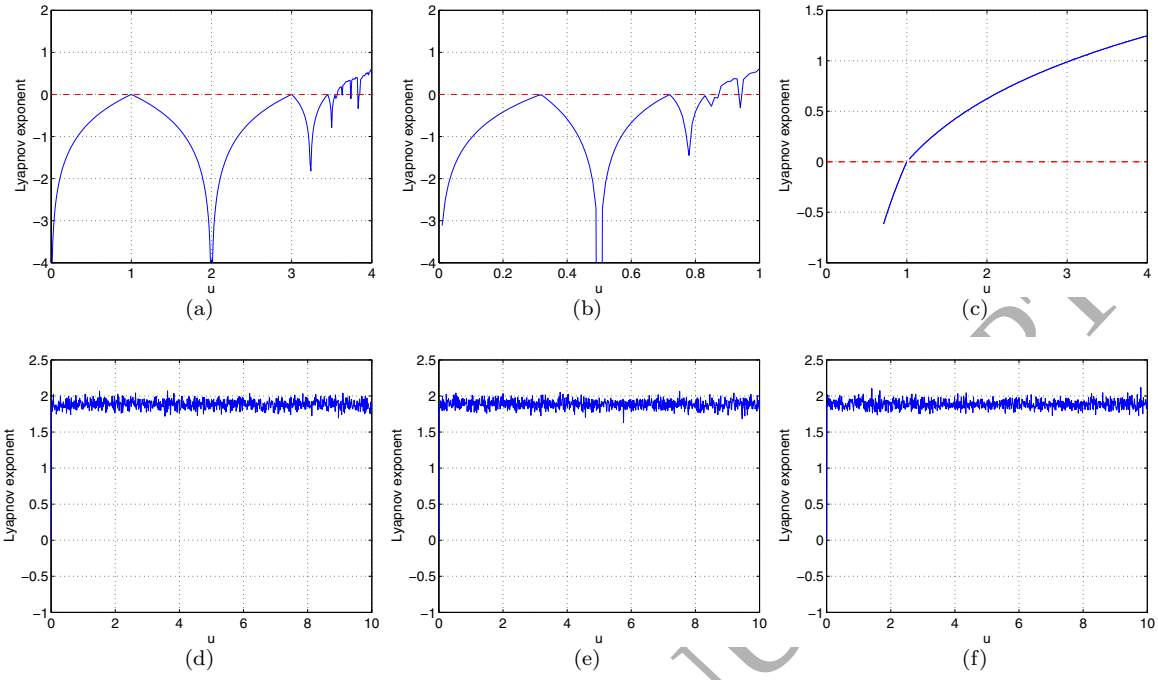


Fig.2. The Lyapunov exponent diagram of the (a) Logistic map; (b) Sine map; (c) Chebyshev map; (d) LLS; (e) SSS; (f) CCS.

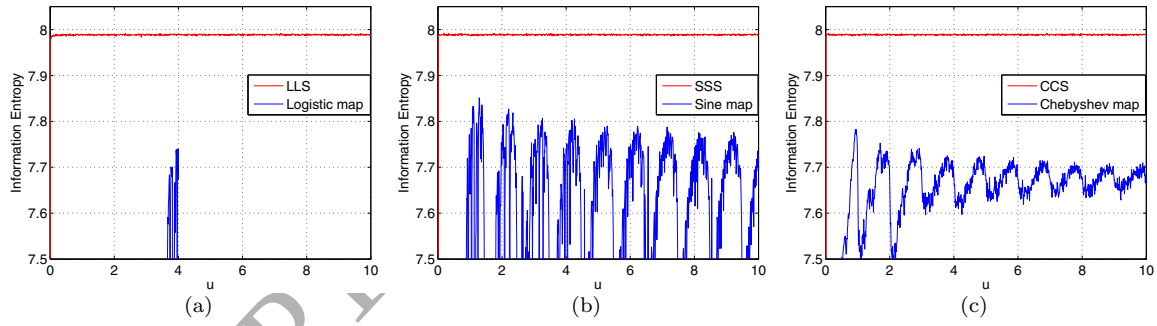


Fig.3. The Information entropy diagram of the (a) Logistic map and LLS; (b) Sine map and SSS; (c) Chebyshev map and CCS.

The Lyapunov exponent and bifurcation diagram of LLS are shown in Fig.1(d) and Fig.2(d). As shown in Fig.1(d) and Fig.2(d), its chaotic range is $(0, 10]$, and is much larger than that of the Logistic map and has good chaotic performance.

3.2.2. Sine-Sine map

The system of the Sine map combined by equation(4) is called Sine-Sine system(SSS). It is defined in the following equation.

$$x_{n+1} = u \times sin(\pi \times x_n) \times 2^{14} - floor(u \times sin(\pi \times x_n) \times 2^{14}) \tag{6}$$

where the parameter $u \in (0, 10]$ and x_0 is the initial value of the sequence.

The Lyapunov exponent and bifurcation diagram of SSS are shown in Fig.1(e) and Fig.2(e). Like LLS, its chaotic range and performance is much better than the previous Sine map's.

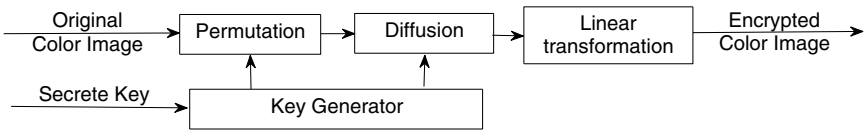


Fig.4. The block diagram of the proposed cryptosystem

3.2.3. Chebyshev-Chebyshev map

To generate a chaotic sequence with good chaotic performance, we slightly modified the control parameter and combined the Chebyshev map by using equation(4). The system is called Chebyshev-Chebyshev system(CCS). The combination equation is as follows.

$$x_{n+1} = cos((u+1) \times arccos(x_n)) \times 2^{14} - floor(cos((u+1) \times arccos(x_n)) \times 2^{14}) \tag{7}$$

where the control parameter $u \in (0, 10]$ and x_0 is the initial value of the sequence.

The Lyapunov exponent and bifurcation diagram of CCS are shown in Fig.1(f) and Fig.2(f). Like LLS, its chaotic range and performance is much better than the previous Chebyshev map's.

3.2.4. Information Entropy of the new chaotic system

The information entropy (IE) is designed to evaluate the uncertainty in a random variable and its ideal value is 8. The evaluation equation is as follows.

$$H(R) = -\sum_{i=0}^{F-1} P(R=i) \times log_2 P(R=i) \tag{8}$$

where F is the gray level, $F = 256$ and P is a discrete probability density function.

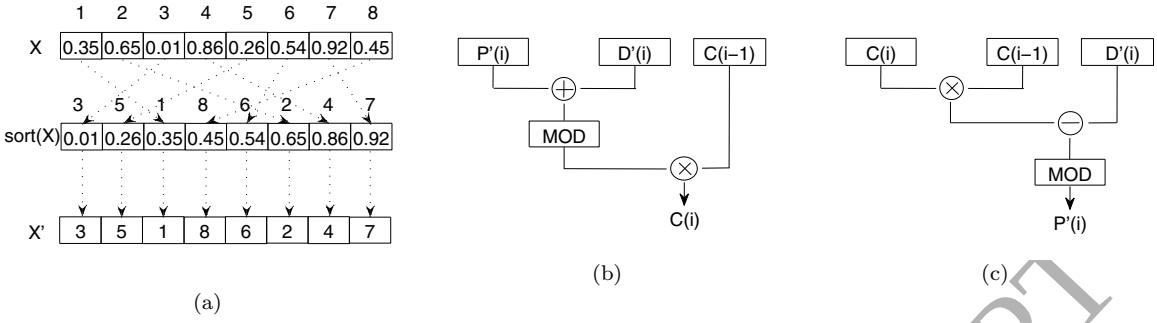
The information entropy has a maximum when all signal values have random distributions. In this experiment, we made a comparison analysis between the information entropy of the output sequences of the existing 1D chaotic maps and that of the output chaotic sequences of the proposed chaotic system. The diagrams of the information entropy of the above mentioned chaotic systems are shown in Fig.3. As observed, the information entropy of the output sequences of the proposed chaotic system has a value close to 8 in the range of $(0, 10]$. This means that its distribution has a higher randomness compared to that of the existing 1D chaotic output sequences.

4. Image encryption algorithm

In this section, a new image encryption algorithm is proposed and its application in information security is verified. The encryption algorithm uses five parameters of (x_0, u, k, N_0, lp) as the security key. The diagrams of the proposed cryptosystem are shown in Fig.4.

4.1. Encryption process

Step 1: The color image with the size of $M \times N$ is divided into 3 images with R, G and B channels respectively, and then the 3 images are linked to make a grayscale image with the size of $M \times 3N$. In the case of the Grayscale image with the size of $M \times N$, it will be used without conversion.



(a) (b) (c)

Fig.5. The diagram of a) the generating of permutation position matrix: b) Diffusion process in encryption: c) Diffusion process in decryption.

Step 2: The grayscale image obtained above is converted into the 1D image pixel matrix $P = \{p_1, p_2, ...p_{M\times 3N}\}$ with the size of $M \times 3N$.

Step 3: The chaotic sequence X used in the encryption system is obtained in the above-mentioned new chaotic system.

where x_0, u and k are initial values of the chaotic system and are used as the security keys.

Iterate the new chaotic system $(M \times 3N + N_0)$ times and discard the former N_0 elements to make a new sequence with $M \times 3N$ elements. Where N_0 is a constant used as the security key.

Step 4: Obtain the permutation position matrix $X' = \{x'_1, x'_2...x'_{M\times 3N}\}$ by sorting the chaotic sequence X in ascending order. The process is shown in Fig.5[a].

Step 5: Obtain the permuted image pixel matrix $P' = \{p'_1, p'_2, ...p'_{M\times 3N}\}$ by using the permutation position matrix X' and the image pixel matrix P. Permutation equation can expressed by the following.

$$P'(i) = P(X'(i)); \tag{9}$$

Step 6: Obtain the diffusion matrix $D' = \{d'_1, d'_2, ...d'_{M\times 3N}\}$ by the following equation.

$$D'(i) = mod(floor(X(i) \times 10^{14}), 256); \tag{10}$$

Step 7: Obtain the encrypted image pixel matrix $C = \{c_1, c_2, ...c_{M\times 3N}\}$ from the diffusion matrix D' and the permuted image matrix P' by the following diffusion equation.

$$C(i) = mod(P'(i) \oplus D'(i), 256) \otimes C(i-1); \tag{11}$$

where $\oplus$ is the arithmetic plus operator, $\otimes$ bit-level XOR operator, and $C(i-1)$ the previous encrypted pixel. The process is shown in Fig.5[b].

Step 8: Obtain a new encrypted image pixel matrix $C' = \{c'_1, c'_2, ...c'_{M\times 3N}\}$ by rotating the above obtained encrypted matrix C to the left by the amount of lp. Where lp is used as a security key and $lp \in [1, M \times 3N]$.

The new image pixel matrix C' is obtained in the following equation.

$$\begin{cases} C'(i - lp) = C(i); & i - lp \geq 1 \\ C'((i - lp) + M \times 3N) = C(i); & i - lp < 1 \end{cases} \tag{12}$$

The step 8 not only avoids the repetition of linear(permutation)-nonlinear(diffusion) conversion to shorten the encryption time, but also increases the strength of encryption.

Step 9: Convert the C' into the R, G and B color image with the size of $M \times N$.

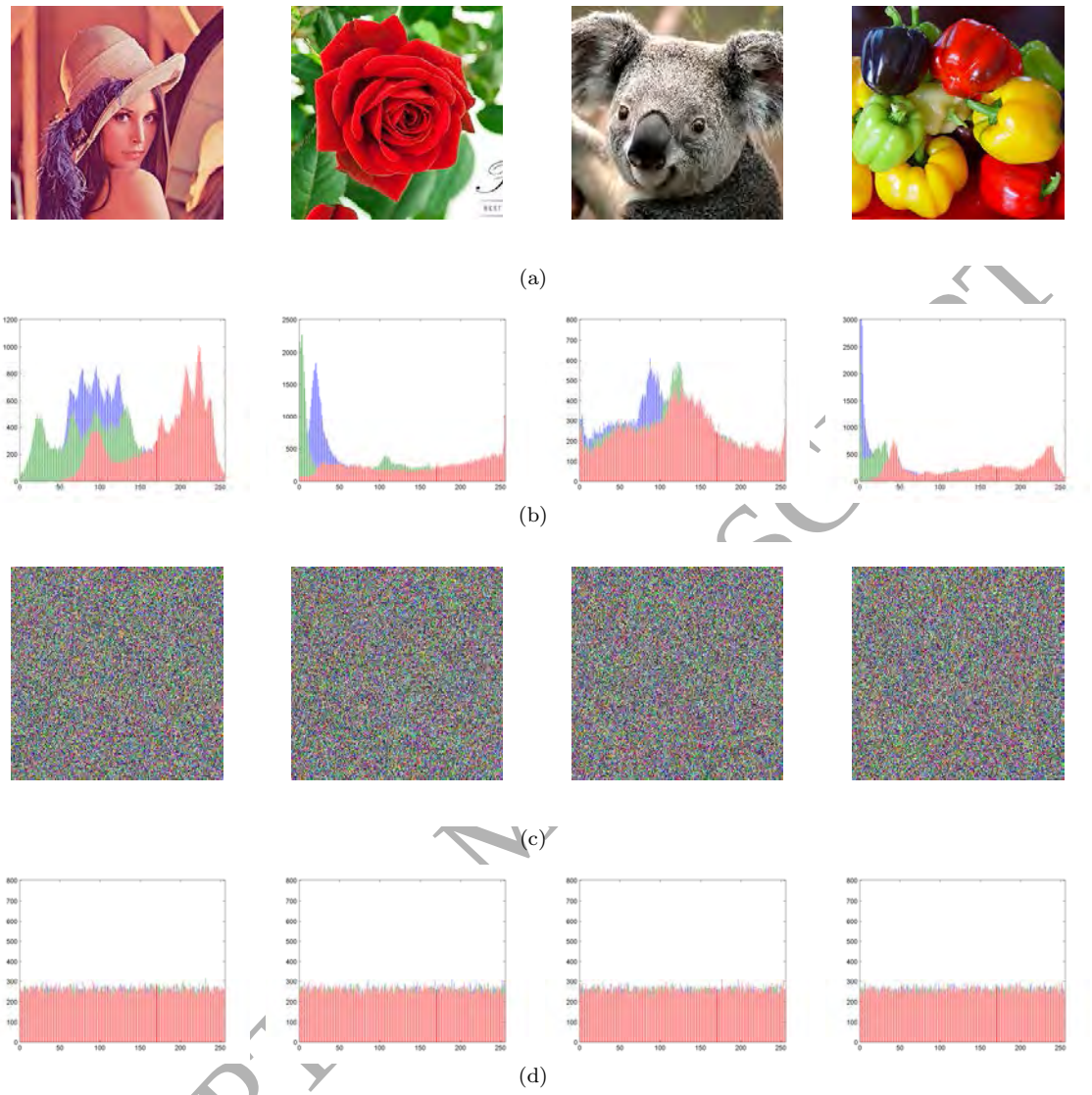


Fig.6. Encryption result of some images. (a) the original images; (b) the histogram of the original images; (c) the encrypted images; (d) the histogram of the encrypted images.

The obtained color image is a noise-like encrypted image.

4.2. Decryption process

The decryption is the inverse process of encryption. The permutation and diffusion equations used in decryption are as follows.

$$P(X'(i)) = P'(i); \tag{13}$$

$$P'(i) = mod(C(i) \otimes C(i-1) \ominus D'(i), 256); \tag{14}$$

where $\ominus$ is the arithmetic minus operator. The process of the equation(14) is shown in Fig.5[c].

The encryption and decryption algorithms are simple, but they are enough to increase the strength of encryption. They can be applied not only to color image, but also to grayscale image.

5. Experimental results and discussion

To evaluate the performance of the encryption algorithm, we made a simulation experiment with Matlab 2013a. The above proposed SSS and color images with the size of 256×256 are used. The initial value of SSS $x_0 = 0.456$, the control parameter $u = 5.4321$, $k = 14$ and $N_0 = 1000$. The results of encryption and decryption are shown in Fig.6. This shows that all encrypted images are noise-like ones and can be efficiently applied to images of various forms such as grayscale images, color images and binary images.

5.1 Security key space

For better security performance, the encryption algorithm should be very sensitive to any change of its security key and have a larger space than 2^{100}, enough to withstand the brute force attack. Our encryption algorithm has 5 security keys: $u,\ x_0,\ k,\ N_0,\ lp.$ where $u \in (0, 10],\ x_0 \in (0, 1],\ k \in [8, 20],\ lp \in [1, M \times 3N]$. Here we compute the u and x_0 in the accuracy of 10^{-16}, set the size of image to 256×256, set $N_0 = 10^3$ and consider the k, so we can get the total key space as $10^{16} \times 10^{16} \times (256 \times 256 \times 3) \times 10^3 \times 12 \approx 2^{138}$.

This means that our algorithm can withstand the brute force attack.

5.2. Statistical analysis

5.2.1. Histogram analysis

Image histogram reflects the distribution of pixel values of an image. To resist statistic attacks, the image histogram should be flat. Fig. 6[b, d] show the histograms of the some images and the histograms of their encrypted images. As shown in Fig. 6[b, d], the histogram of the encrypted image has a good uniform distribution, so that it is enough to resist statistic attacks.

5.2.2. Correlation of two adjacent pixels

Image data generally has some intrinsic features, such as high redundancy of data and strong correlation among neighbouring pixels, and it can be used by attackers for attacking information. In the experiment we randomly selected 1000 pairs of adjacent pixels from the original images and the encrypted images and analyzed the correlations at horizontal, vertical and diagonal directions. The correlation coefficient is calculated by the equation(15) below.

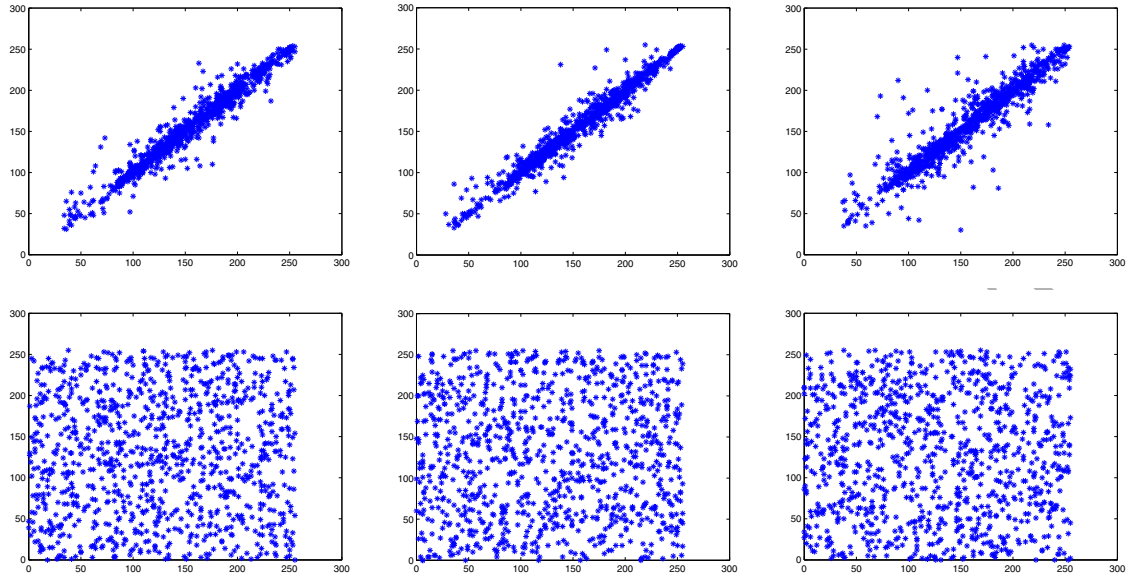
$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{15}$$

$$where \quad cov(x, y) = \frac{1}{N} \sum_{i=0}^{N} (x_i - E(x))(y_i - E(y))$$

$$D(x) = \frac{1}{N} \sum_{i=0}^{N} (x_i - E(x))^2, \quad E(x) = \frac{1}{N} \sum_{i=0}^{N} x_i$$

where x and y are color values of two adjacent pixels in the images.

The correlation diagram among adjacent pixels at horizontal, vertical and diagonal directions of R channel in Lena image is shown in Fig.7 and the correlation coefficients according to the directions of



(a) (b) (c)

Fig.7. Correlation analysis of image Lena in R channel. (a) horizontal correlation of original and encrypted images; (b) vertical correlation of original and encrypted images; (c) diagonal correlation of original and encrypted images.

some images in Table 1. As seen in Table 1, the correlation coefficient of the original images comes near to 1, but the correlation coefficient of the encrypted images comes near to 0.

This means that the encrypted image has no correlation property with original image.

Table 1 Correlation coefficient of the some encrypted images in R channel

	Original image			Encrypted image		
Image	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
lena.bmp	0.9239	0.9567	0.8888	-0.0038	-0.0026	0.0017
koala.bmp	0.9078	0.9051	0.8687	-0.0054	0.0013	0.0031
flower.bmp	0.9563	0.9542	0.9238	0.0007	-0.0046	-0.0063
greens.bmp	0.9758	0.979	0.9622	-0.0025	0.0064	0.0010
back.bmp	0.9178	0.9087	0.8661	-0.0054	-0.0068	0.0023
ctable.bmp	0.9960	0.9806	0.9768	0.0059	-0.0014	0.0002
dog.bmp	0.9774	0.9694	0.9493	-0.0045	-0.0002	-0.0073

5.2.3. Sensitivity analysis

A good encryption system should be very sensitive to tiny differences in key and plain images. The sensitivity can be quantitatively evaluated by NPCR(number of pixels change rate) and UACI(unified average changing intensity) and is expressed in the following equation.

$$NPCR = \frac{1}{W \times H} \sum_{i=0}^{H} \sum_{j=0}^{W} D(i,j) \times 100(\%) \tag{16}$$

$$where \quad D(i,j) = \begin{cases} 0 & \text{if } c_1(i,j) = c_2(i,j) \\ 1 & \text{if } c_1(i,j) \neq c_2(i,j) \end{cases}$$

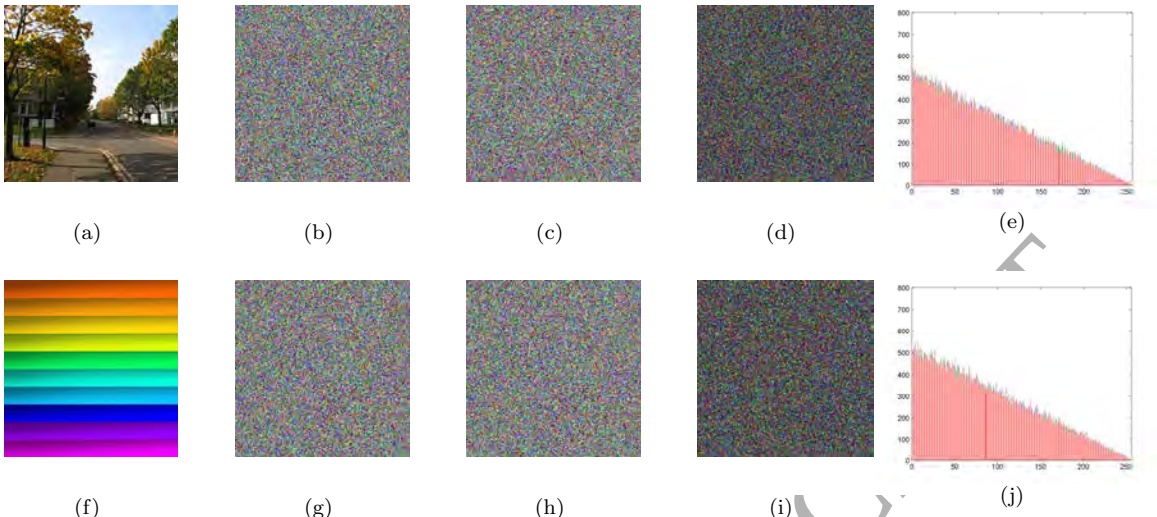


Fig.8. Encryption results with closed initial values and their difference. (a, f) The original images; (b) the encrypted image(c_1) with $x_0 = 0.456$; (c) the encrypted image(c_2) with $x_0 = 0.4560000000000001$; (d, e) the pixel-to-pixel difference ($|c_1 - c_2|$) and its histogram; (g) the encrypted image(c_1') with $lp = 1000$; (h) the encrypted image(c_2') with $lp = 1001$; (i, j) the pixel-to-pixel difference ($|c_1' - c_2'|$) and its histogram.

$$UACI = \frac{1}{W \times H} \sum_{i=0}^{H} \sum_{j=0}^{W} \frac{|c_1(i,j) - c_2(i,j)|}{255} \tag{17}$$

where c_1 and c_2 are encrypted images corresponding to two security keys.

Table 2 shows NPCR and UACI of 7 images. The results of encryption and decryption of two security keys with tiny differences are shown in Fig.8. As seen in Table 2 and Fig.8, the proposed chaotic system is very sensitive to tiny differences of the initial condition, that is, the security key.

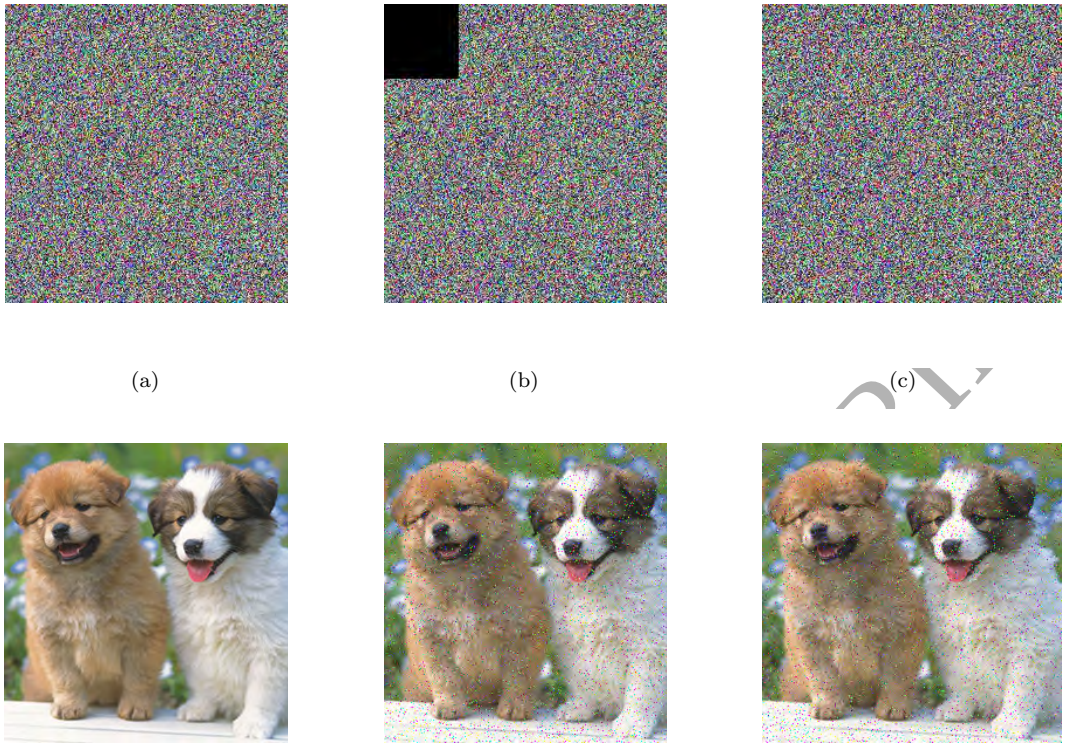
Table 2 The mean NPCR and UACI of the some encrypted images

	NPCR(%)			UACI(%)		
Image	R	G	B	R	G	B
lena.bmp	99.6552	99.6277	99.588	33.4846	33.4132	33.3441
koala.bmp	99.5834	99.6262	99.5926	33.5202	33.4907	33.4115
flower.bmp	99.6277	99.6063	99.5575	33.3951	33.5272	33.4008
greens.bmp	99.614	99.6017	99.6231	33.4233	33.5183	33.4065
back.bmp	99.6323	99.5483	99.6017	33.2367	33.4043	33.4295
ctable.bmp	99.6124	99.6323	99.5941	33.4798	33.5387	33.5354
dog.bmp	99.6353	99.6063	99.5926	33.4502	33.3814	33.5937

5.2.4. Data loss and Noise Attack

Digital images can be easily influenced by noise and data loss during transmission through the network and storage in physical media. An image encryption algorithm should have an ability of resisting these abnormal phenomena.

To test the ability of resisting the attack, we did some experiments on a data loss and a noise attack. An original image is first encrypted by our proposed algorithm. The encrypted image is attacked by a data cut of size 64×64(Fig.9(b)) and with 3% *'salt&pepper'* noise(Fig.9(c)), respectively. The decryption process is then applied to these three encrypted images. As can be seen in Fig.9(e) and Fig.9(f), the



(a) (b) (c)

(d) (e) (f)

Fig.9. Data loss and noise attack. (a) the encrypted original image; (b) the encrypted image with 64×64 data loss; (c) the encrypted image added with 3% *'salt&pepper'* noise; (d) the decrypted image of (a); (e) the decrypted image of (b); (f) the decrypted image of (d).

decrypted images contain most of original visual information, even if there are limited data loss and noise.

The restoring ability of an image is evaluated by PSNR(Peak Signal to Noise Ratio) and is expressed in the following equation.

$$PSNR = 10 \times lg \frac{255^2}{MSE} \ (dB) \tag{18}$$

$$where \quad MSE = \frac{1}{W \times H} \sum_{i=0}^{H} \sum_{j=0}^{W} (OI(i,j) - DI(i,j))^2$$

where $M \times N$ is the size of image, $OI(i,j)$ a pixel of the original image and $DI(i,j)$ a pixel of the decrypted image.

The larger the value of PSNR, the smaller the breakdown coefficient of the image gets, and when the value of PSNR is above 35dB, it is very difficult to distinguish the real image and the decrypted image. Table 3 shows the PSNR coefficients in some images. As can be seen in the experimental results, the proposed encryption algorithm has excellent performance in noise and attacks.

6. Conclusion

Table 3 The PSNR of the some encrypted images

	lena.bmp	koala.bmp	flower.bmp	greens.bmp	back.bmp	ctable.bmp	dog.bmp
Data loss	47.4199	46.4290	43.1885	43.0299	44.3702	43.6736	47.5974
Noise attack	48.1770	47.2217	43.0872	43.7381	45.3850	43.0456	48.2478

In this paper, firstly, we proposed a method of making a simple and effective chaotic system by using a difference of the output sequences of two same existing one-dimension (1D) chaotic maps. Simulations and performance evaluations showed that the proposed system is able to produce a one-dimension (1D) chaotic system with better chaotic performances and larger chaotic ranges compared with the previous chaotic maps. Secondly, we proposed a novel encryption system of linear-nonlinear-linear structure based on total shuffling to confirm its applications in image encryption. Experiments and security analysis proved that the algorithm has an excellent performance in image encryption and various attacks.

Acknowledgment

This research is funded by National Natural Science Foundation of China (No. 61203004, 61306142) and Natural Science Foundation of Heilongjiang Province (Grant No. F201220).

References

[1] S. Li, G. Chen, A. Cheung, B. Bhargava, KT. Lo, On the Design of Perceptual MPEG-Video Encryption Algorithms, IEEE Transactions on Circuits & Systems for Video Technology, 17(2) (2005) 214-223.

[2] G. Bhatnagar, QMJ. Wu, B. Raman, A New Fractional Random Wavelet Transform for Fingerprint Security, IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum.42(1) (2012) 262-275.

[3] G. Bhatnagar, QMJ. Wu, B. Raman, Discrete fractional wavelet transform and its application to multiple encryption, Information Sciences. 223(2) (2013) 297-316.

[4] Y. Zhou, K. Panetta, S. Agaian, CLP. Chen, Image encryption using P-Fibonacci transform and decomposition, Optics Communications. 285(5) (2012) 594-608.

[5] Y. Zhou, K. Panetta, S. Agaian, CL. Chen, (n, k, p)-Gray Code for Image Systems, IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum. 43(2) (2012) 515-529.

[6] TH. Chen, CS. Wu, Compression-unimpaired batch-image encryption combining vector quantization and index compression, Inf. Sci. 180(9) (2010) 16901701.

[7] Y. Sangeetha, S. Meenakshi, CS. Sundaram, A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process, Multimedia Tools and Applications. 71(3) (2014) 1469-1497

[8] A. Kassem, HAH. Hassan, Y. Harkouss, R. Assaf, Efficient neural chaotic generator for image encryption, Digital Signal Processing. 25(2) (2014) 266-274.

[9] D. Arroyo, J. Diaz, FB. Rodriguez, Cryptanalysis of a one round chaos-based Substitution Permutation Network, Signal Processing. 67(2) (2013) 1358-1364.

[10] AAA. El-Latif, X. Niu, A hybrid chaotic system and cyclic elliptic curve for image encryption, AEU. 67(2) (2013) 136-143.

[11] Y. Zhou, L. Bao, CLP. Chen, A new 1D chaotic system for image encryption, Signal Processing. 97(7) (2014) 172-182.

[12] W. Wen, Y. Zhang, Z. Fang, JX. Chen, Infrared target-based selective encryption by chaotic maps, Optics Communications, 341 (2015) 131-139.

[13] Z. Hua, Y. Zhou, CM. Pun, CLP. Chen, 2D Sine Logistic modulation map for image encryption, Information Sciences. 297 (2014) 80-94.

[14] CY. Song, YL. Qiao, XZ. Zhang, An image encryption scheme based on new spatiotemporal chaos, Optik. 124(124) (2013) 3329-3334.

[15] C. Lv-Chen, L. Yu-Ling, Q. Sen-Hui, L. Jun-Xiu, A perturbation method to the tent map based on Lyapunov exponent and its application, Chinese Physics B. 24(10) (2015) 78-85.

[16] Y. Zhou, L. Bao, CLP. Chen, Image encryption using a new parametric switching chaotic system, Signal Processing. 93(11) (2013) 3039-3052.

[17] RR. Kumar, MB. Kumar, A NEW CHAOTIC IMAGE ENCRYPTION USING PARAMETRIC SWITCHING BASED PERMUTATION AND DIFFUSION. Ictact Journal on Image & Video Processing. 4(4) (2014).

[18] C. Fu, BB. Lin, YS. Miao, X. Liu, JJ. Chen, A novel chaos-based bit-level permutation scheme for digital image encryption, Optics Communications. 284(23) (2011) 5415-5423.

[19] Z. Eslami, A. Bakhshandeh, An improvement over an image encryption method based on total shuffling, Optics Communications, 286(1) (2013) 51-55.

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

[21] FG. Jeng, WL. Huang, TH. Chen, Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes, Signal Processing Image Communication. 34 (2015) 45-51.

[22] FG. Jeng, WL. Huang, TH. Chen, Cryptanalysis of an improvement over an image encryption method based on total shuffling, Optics Communications. 350 (2015) 77-82.

[23] R. Liu, New Algorithm for Color Image Encryption Using Improved 1D Logistic Chaotic Map, Open Cybernetics & Systemics Journal. 9(1) (2015) 210-216.

[24] L. Xu, Z. Li, J. Li, W. Hua, A novel bit-level image encryption algorithm based on chaotic maps, Optics & Lasers in Engineering. 78(21) (2016) 17-25.

[25] B. Stoyanov, K. Kordov, Novel image encryption scheme based on Chebyshev polynomial and Duffing map, Scientific World Journal, 2014 (2014) 283639-283639.

[26] B. Stoyanov, K. Kordov, Image Encryption Using Chebyshev Map and Rotation Equation, Entropy, 17(4) (2015) 2117-2139.

[27] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications, 284(1617) (2011) 3895-3903.

[28] G. Sun, M. Wang, L. Huang, L Shen, Generating Multi-Scroll Chaotic Attractors via Switched Fractional Systems, Circuits Systems & Signal Processing, 30(6) (2011) 1183-1195.

[29] GuangHhui. Sun, Mao. Wang, The Fractional Order Modified Chaotic n-SCROLL Chua Circuit and Fractional Control, International Journal of Modern Physics B, 26(14) (2012) 1099-1113.

[30] M. Khan, T. Shah, An efficient chaotic image encryption scheme, Neural Computing and Applications, 26(5) (2015) 1137-1148.

[31] M. Khan, T. Shah, SI. Batool, Construction of S-box based on chaotic Boolean functions and its application in image encryption, Neural Computing and Applications, 27(3) (2016) 677-685.

[32] A. Belazi, M. Khan, AAA. El-Latif, S. Belghith, Efficient cryptosystem approaches: S-boxes and permutationsubstitution-based encryption, Nonlinear Dynamics, (2016) 1-25.

[33] MT. RosensteinJJ. CollinsCJD. Luca, A practical method for calculating largest Lyapunov exponents from small data sets, Physica D Nonlinear Phenomena, 65(s 12) (1993) 117-134.

[34] A. Wolf, JB. Swift, HL. Swinney, JA. Vastano, Determining Lyapunov exponents from a time series, Physica D Nonlinear Phenomena, 16(3) (1985) 285-317.

[35] MR. Titchener, WB. Ebeling, Deterministic Chaos and Information Theory, Data Compression Conference, (2001) 0520-0520.

[36] C.E. Shannon, A mathematical theory of communication, McGraw-Hill, 27(3) (1974) 379-423.

[37] KT. Alligood, TD. Sauer, JA. Yorke, CHAOS : An Introduction to Dynamical Systems, Springer, 50(11) (2008) 67-68.