Multimedia Tools and Applications (2019) 78:12027–12042
https://doi.org/10.1007/s11042-018-6739-1

A novel bit-level color image encryption using improved 1D chaotic map

Chanil Pak[1] · Kwangil An[1] · Paeksan Jang[2] · Jonggun Kim[3] · Sok Kim[4]

Received: 10 December 2017 / Revised: 17 August 2018 / Accepted: 1 October 2018 /
Published online: 9 October 2018

Abstract

This paper introduces new simple and effective improved one-dimension(1D) Logistic map and Sine map made by the output sequences of two same existing 1D chaotic maps. The comparison analysis of the proposed improved 1D chaotic map and previous 1D chaotic map confirmed the accuracy of the improved chaotic map. To investigate the applications of the improved chaotic system in image encryption, a novel bit-level image encryption system is proposed. Experiments and analysis prove that the improved chaotic map and the algorithm has an excellent performance in image encryption and various attacks.

Keywords Chaos · Chaotic system · Image encryption

1 Introduction

With the development of internet and information communication technique, a large number of image and video data including various information are distributed and stored, so the safe storage and distribution of the data has a vital importance. In particular, compared to text data, some intrinsic features of image data, such as big size, high redundancy of data and strong correlation among neighboring pixels require the strong real-time property in communication. For this reason, the traditional block encryptions (DES, IDEA, AES) being widely used now is found to be inefficient for image encryption [14].

✉ Chanil Pak
pakchanil@126.com; pakchanil@hrbeu.edu.cn

[1] Information Center, Kim Chaek University of Technology, Pyongyang 950003, Democratic People's Republic of Korea

[2] Institute of Nano Physicsal Engineering, Kim Chaek University of Technology, Pyongyang 950003, Democratic People's Republic of Korea

[3] Information Center, Kim Il Sung University, Pyongyang 950003, Democratic People's Republic of Korea

[4] Department of Information Engineering, Chongjin Mine Metal University, Chongjin 999091, Democratic People's Republic of Korea

To prevent the loss of image information, a large number of algorithms, such as fractional wavelet transform [3, 4], p-Fibonacci transform [29], gray code [28], vector quantization [5] and chaos [1, 2, 6–13, 15–27, 30, 31], have been proposed and among them the image encryption based on the chaotic map is being widely used.

The chaotic map is distinguished by the sensitivity to initial conditions and system parameters and the excellent random distribution. In particular, in the image encryption by chaotic map, some property coefficients of encryption result depend on the property of the chaotic map, so it needs the better distribution of chaotic map used in the encryption. Compared to the multi-dimensional chaotic map, the 1D chaotic map has some disadvantages in the chaotic range and distribution, but, because of the advantage of easiness of implementation by hardware and software, the 1D chaotic map is being widely used now. But the 1D chaotic systems have some disadvantages such as limited range of chaotic behaviors and non-uniform data distribution of output chaotic sequences [1, 12, 19]. Many researches are being done to overcome the disadvantages of 1D chaotic map, obtain the chaotic distribution with improved properties and apply it to image encryption [7, 10, 13, 16, 18, 20, 24, 30].

The bit-level image encryption has different advantages in image encryption. The permutations in the bit-level image encryption have an advantage that the position and value of a pixel can be changed simultaneously, but little research on it is being made now. Some bit-level encryption algorithms are being proposed [6, 9, 15, 17, 21, 22, 25–27, 31]. One pixel of image is composed of 8 bits, the amount of information occupied by the 8 bits is different from position to position. The computation shows that the 4 upper-level bits have about 94 percent of a pixel information, for this reason, the method of encryption using the 4 upper-level bits is proposed.

The encryption system 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 number of computation time, so that it gives an influence on the performance of whole encryption system.

On the basis of analysis of above mentioned problems, we propose the improved Logistic map and Sine map and evaluate their performance in this paper. The simulation and analysis of bifurcation property of chaotic map and Lyapunov exponent and information entropy evaluating chaotic performance demonstrate the accuracy of the improved chaotic map. And, on the basis of analysis of existing encryption systems, a bit-level image encryption system of linear-nonlinear-linear conversion structure is proposed. Simulation and experiment evaluate key space and key sensitivity, correlation and resistance to attack.

The paper is organized as follows. Section 2 briefly reviews the performance of existing Logistic map and Sine map. Section 3 makes an improved 1D chaotic map by using above mentioned existing 1D chaotic map and demonstrate its accuracy. Section 4 proposes a bit-level image encryption algorithm of linear-nonlinear-linear structure. Section 5 shows the results of simulation and analysis. Section 6 shows the conclusion.

2 1D chaotic maps

Because of the simplicity of structure, the 1D chaotic maps are being widely used in image encryption. In this section, 1D chaotic maps: Logistic map and Sine map will be briefly discussed.

2.1 Logistic map

The logistic map is one of simple 1D chaotic maps with complex chaotic behavior and it is 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 the range of $(0, 4]$ and x_0 is the initial value of chaotic map, x_n is the output chaotic sequence.

The bifurcation diagram and Lyapunov Exponent diagram are shown in Figs. 1a and 2a. There are two problems in the Logistic map. Two problems are that its chaotic range is limited and the data distribution of output chaotic sequences is non-uniform. As shown in the bifurcation diagram and Lyapunov Exponent diagram, its chaotic range is limited only within $[3.57, 4]$ and the control parameter beyond the range can't have chaotic behaviors. 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 good performance and the larger the value is, it has a better chaotic performance. In other words,

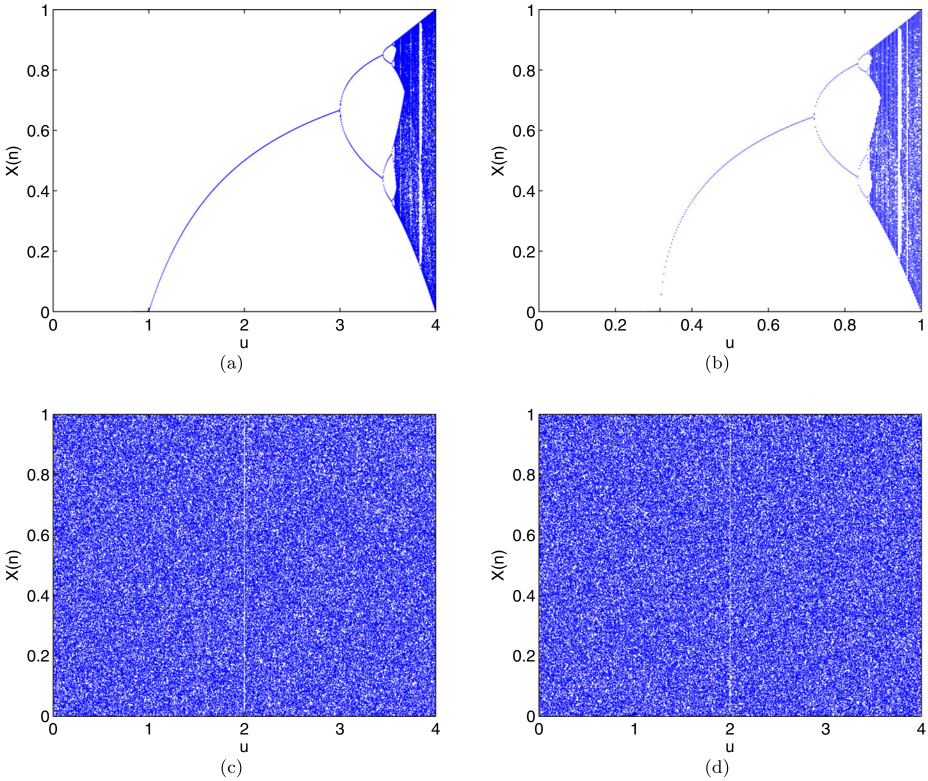


Fig. 1 The bifurcation diagrams of the (**a**) Logistic map; (**b**) Sine map; (**c**) improved Logistic map; (**d**) improved Sine map

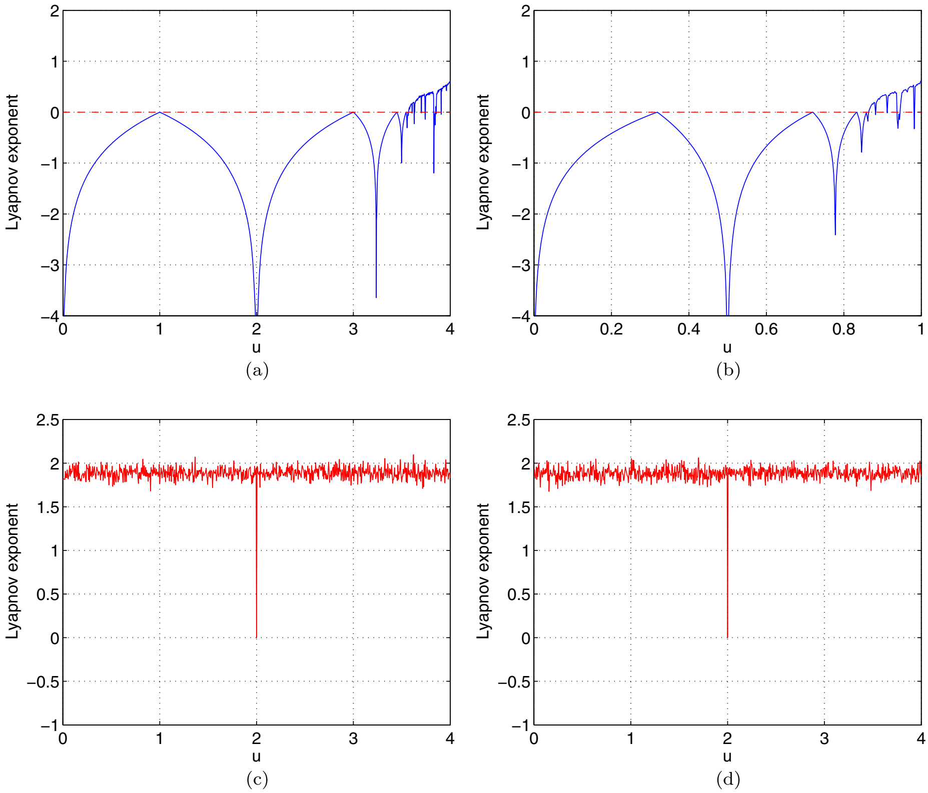


Fig. 2 The Lyapunov exponent diagram of the (**a**) Logistic map; (**b**) Sine map; (**c**) improved Logistic map; (**d**) improved Sine map

when parameter $u < 3.57$, the Lyapunov Exponents of the Logistic map are smaller than zero and it means that they have no chaotic behaviors. On the other hand, the data range of the chaotic sequences is smaller than [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. And, the encrypted image should have close correlation with the security key, so that 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 behavior 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.

As shown in bifurcation diagram and Lyapunov Exponent diagram of Figs. 1b and 2b, it has a similar property with the Logistic map.

3 The improved chaotic system

In this section, an improved 1D chaotic map is proposed to solve the problems mentioned in Section 2. To verify its accuracy, above-mentioned Logistic map and Sine map are used.

3.1 The structure of chaotic map

The new chaotic map is defined by the following equation.

$$x_{n+1} = F(u, x_n, k) = mod((F_{chaos}(u, x_n) - F'_{chaos}(u, x_n)) \times G(k), 1) \tag{3}$$

$$where \quad G(k) = 2^k, 9 \leq k \leq 16$$

where $F_{chaos}(u, x_n)$ is one of the existing 1D chaotic maps mentioned above and $F(u, x_n, k)$ is a newly made chaotic map. $F'_{chaos}(u, x_n)$ is the function where u of the function $F_{chaos}(u, x_n)$ is replaced with $(4 - u)$. u is a control parameter with the range of $[0, 2) \bigcup (2, 4]$.

From equation [4], it can be seen that the proposed system does not have a chaotic property when $u = 2$, and the all values of output sequences become zero.

In other words, $F(u, x_n, k)$ still has a chaotic property in the expanded range of $[0, 2) \bigcup (2, 4]$ lager than the range of the existing 1D chaotic maps. The output chaotic sequences surely are to be in the range of $(0, 1)$ by the 'mod' operation. x_n is the sequence of the chaotic map, n is the iteration number, and $G(k)$ is an adjustable function with parameter k. k has a good chaotic performance in the range of [9, 16]. In Fig. 3, it can be seen that the larger k means the better chaotic performance in the range. The value range of k has been confirmed in the experiment. In the paper, the control parameter k is set to 12. The new proposed chaotic system has a simple structure, so it is easy to implement by software and hardware. Lots of new chaotic sequences can be made by using the proposed chaotic system.

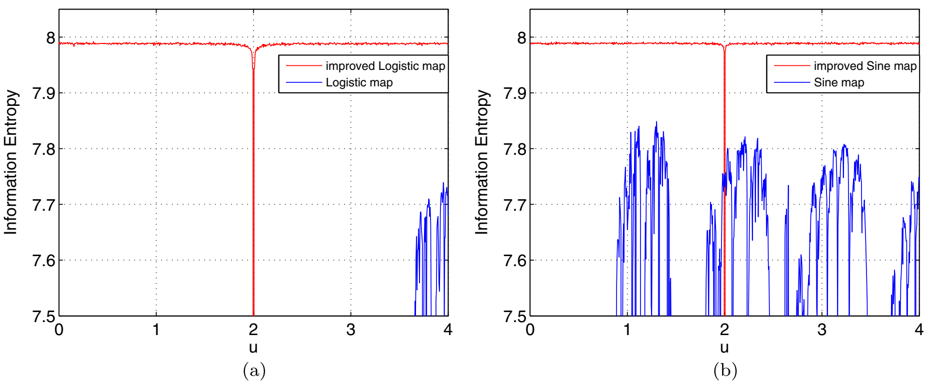


Fig. 3 The Information entropy diagram of the (**a**) Logistic map and improved Logistic map with $k = 12$; (**b**) Sine map and improved Sine map with $k = 12$

3.2 The improved 1D chaotic maps

To verify the performance of the proposed chaotic system, two existing 1D chaotic maps discussed above are used.

3.2.1 The improved logistic map

The Logistic map are combined by using the equation [4]. It can be expressed in the following equation.

$$x_{n+1} = mod((u \times x_n \times (1 - x_n) - (4 - u) \times x_n \times (1 - x_n)) \times 2^{12}, 1) \tag{4}$$

where the parameter $u \in [0, 2) \bigcup (2, 4]$ and x_0 is the initial value of the sequence.

The bifurcation diagrams and Lyapunov exponent of the improved Logistic map are shown in Figs. 1c and 2c. As shown in Figs. 1c and 2c, the chaotic range is $[0, 2) \bigcup (2, 4]$ and it is much larger than that of the existing Logistic map, and it has a good chaotic performance.

3.2.2 The improved sine map

The Sine map are combined by using the equation [4], it can be expressed in the following equation.

$$x_{n+1} = mod((u \times sin(\pi \times x_n) - (4 - u) \times sin(\pi \times x_n)) \times 2^{12}, 1) \tag{5}$$

where the parameter $u \in [0, 2) \bigcup (2, 4]$ and x_0 is the initial value of the sequence.

The bifurcation diagrams and Lyapunov exponent of the improved Sine map are shown in Figs. 1d and 2d. Like the improved Logistic map, its chaotic range and performance is much better than the previous Sine map's.

3.2.3 Information Entropy of the improved chaotic maps

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.

$$H(R) = -\sum_{i=0}^{F-1} P(R = i) \times log_2 P(R = i) \tag{6}$$

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. We made a comparison analysis between the information entropy of output sequences of the existing 1D chaotic maps and that of the output chaotic sequences of the proposed chaotic system. The results are shown in Fig. 3. As shown in Fig. 3, the more the value of k is, the information entropy of the output sequences of the proposed chaotic map has a value closer to 8 in the range of $[0, 2) \bigcup (2, 4]$. This means that its distribution has a higher randomness compared to the existing 1D chaotic output sequences.

4 A new encryption algorithm

In the section, a new bit-level image encryption algorithm is proposed and its application in information security by using the above-mentioned improved Logistic map is verified.

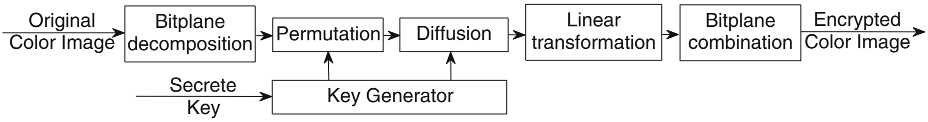


Fig. 4 The block diagram of the proposed cryptosystem

Bitplane decomposition adopts BBD(binary bitplane decomposition) method [26]. The encryption algorithm uses six parameters of (x_0, u, k, N_0, kd, rp) 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 is linked to make a grayscale image with the size of $M \times 3N$. In case of the Grayscale image with the size of $M \times N$, it will be used without conversion.

Step 2: The grayscale image obtained above is converted into the 1D image pixel matrix and then it is converted into 1D image bit matrix $B = \{b_1, b_2, ...b_{M\times 24N}\}$ again.

Step 3: The chaotic sequence X used in the encryption system is obtained in the above-mentioned improved chaotic map. where x_0, u and k are initial values of the chaotic system and are used as the security keys.

Iterate the improved chaotic map $(M \times 24N + N_0)$ times and discard the former N_0 elements to make a new sequence with $M \times 24N$ elements. where N_0 is a constant used as the security key.

Step 4: Obtain the permutation position matrix $X' = \{x'_1, x'_2...x'_{M\times 24N}\}$ by sorting the chaotic sequence X in ascending order.

Step 5: Obtain the permuted image bit matrix $B' = \{b'_1, b'_2, ...b'_{M\times 24N}\}$ by using the permutation position matrix X' and the image bit matrix B. Permutation equation can expressed in the following equation.

$$B'(i) = B(X'(i)); \tag{7}$$

Step 6: Obtain the diffusion matrix $D' = \{d'_1, d'_2, ...d'_{M\times 24N}\}$ by the following equation.

$$D'(i) = mod(floor(X(i) \times kd), 2); \tag{8}$$

where kd is a positive integer and are used as the security keys, the diffusion matrix D' consists of 0 and 1.

Step 7: Obtain the encrypted image bit matrix $C = \{c_1, c_2, ...c_{M\times 24N}\}$ from the diffusion matrix D' and the matrix B' by the following diffusion equation.

$$C(i) = bitxor(B'(i), D'(i)); \tag{9}$$

Step 8: Obtain a new encrypted image bit matrix $C' = \{c'_1, c'_2, ...c'_{M\times 24N}\}$ by rotating the above obtained matrix C to the right by the amount of rp. where rp is used as a security key and $rp \in [1, M \times 24N]$.

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

$$\begin{cases} C'(i + rp) = C(i); & i + rp \le M \times 24N \\ C'((i + rp) - M \times 24N) = C(i); & i + rp > M \times 24N \end{cases} \tag{10}$$

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

Step 9: Convert the C' into the R, G and B color image with the size of $M \times N$. The obtained color image is a noise-like encrypted image.

4.2 Decryption process

The decryption is the inverse process of encryption.

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.

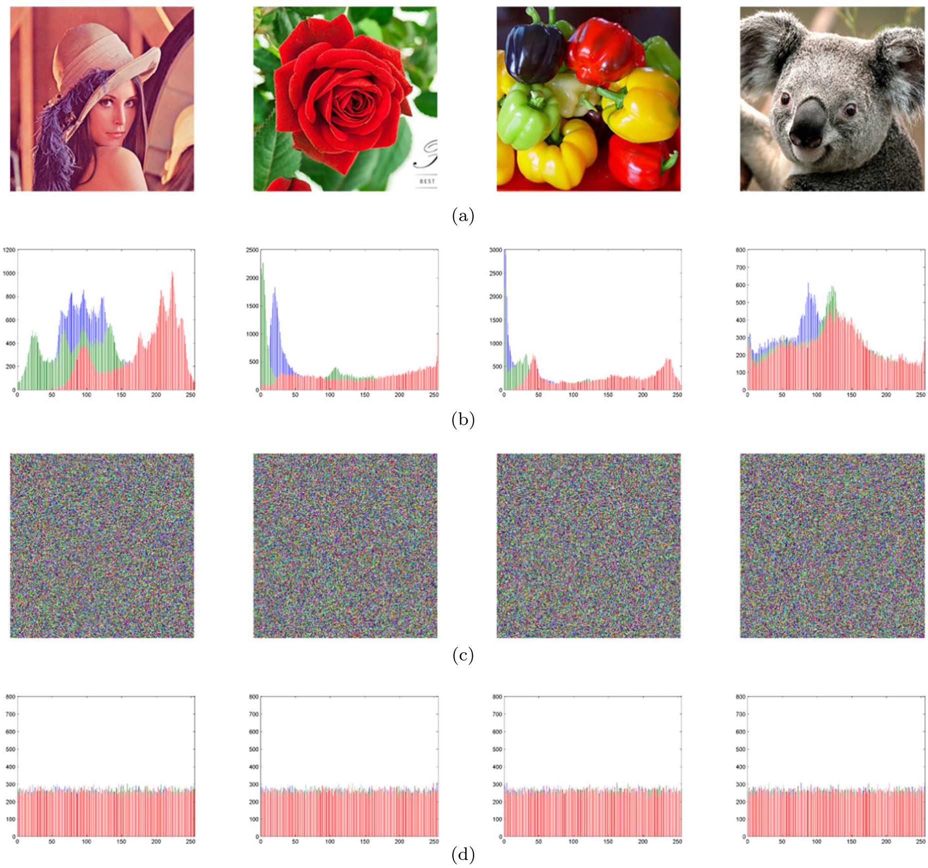


Fig. 5 Encryption result of some images. **a** the original images; **b** the histogram of the original images; **c** the encrypted images; **d** the histogram of the encrypted images

5 Experimental results and discussion

To evaluate the performance of our encryption algorithm, we made a simulation experiment with Matlab 2013a. The above-mentioned improved Logistic map and color images with the size of 256 × 256 are used. The parameters are set as follows. The initial value of the chaotic map $x_0 = 0.34$, the control parameter $u = 2.56$, $k = 12$, $N_0 = 1000$, $kd = 654321$ and $rp = 1000$ and the results of encryption and decryption are shown in Fig. 5. As shown in Fig. 5, 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 the good security performance of an encryption algorithm, it 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. The encryption algorithm has 6 security keys: u, x_0, k, N_0, kd and rp. where $u \in [0, 2) \bigcup (2, 4], x_0 \in (0, 1), k \in [9, 6], rp \in [1, M \times 24N]$ and kd a positive integer. Here we compute the u and x_0 in the accuracy of 10^{-15}, set the size of image to 256×256, set $N_0 = 10^3$, so the total key space is $10^{15} \times 10^{15} \times (256 \times 256 \times 24) \times 10^3 \approx 2^{130}$. When k and kd is considered, the maximum key space is much greater than 2^{130}.

This means that the algorithm can withstand any blute 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. Figure 5b, d shows the histograms of the some images and the histograms of their encrypted images. As shown in Fig. 5b, d, the histogram of the encrypted image has a good uniform distribution, so that it is enough to resist statistic attacks. The distribution scale of the encrypted images are calculated by equation [5] and the results are shown in Table 1.

Table 2 shows the performance comparison with the reference [22]. As shown in Table 2, the information entropy of a image encrypted by the proposed system is equally distributed in channels of R, G and B. As a result, it can be seen that the performance of entropy is superior to that of the system proposed by the preceding literature.

Table 1 Information entropy of the some encrypted images

Image	Original image			Encrypted image		
	R	G	B	R	G	B
lena.bmp	7.314029	7.639443	7.050612	7.997213	7.997199	7.997233
flower.bmp	7.743743	7.130098	6.854102	7.997215	7.997182	7.99711
greens.bmp	7.743528	7.468523	5.834117	7.997192	7.997333	7.997374
koala.bmp	7.894208	7.849115	7.82162	7.997036	7.996995	7.997507

Table 2 Information entropy performance

Image	Proposal			Ref. [22]		
	R	G	B	R	G	B
lena.bmp	7.9972	7.9972	7.9972	7.9974	7.9970	7.9971

5.2.2 Correlation of two adjacent pixels

Image data generally has high redundancy of data and strong correlation among neighboring pixels, so it can be used as attacking information. In the experiment, we randomly selected 1000 pairs of adjacent pixels from the original image and the encrypted image and analyzed the correlations at 3 directions. The correlation coefficient is calculated by the following equation [2].

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{11}$$

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

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

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

The correlation diagram among adjacent pixels at horizontal, vertical and diagonal directions of R channel in the Lena.bmp image is shown in Fig. 6 and the correlation coefficients according to each direction of R channel of some images are shown in Table 3. As seen in

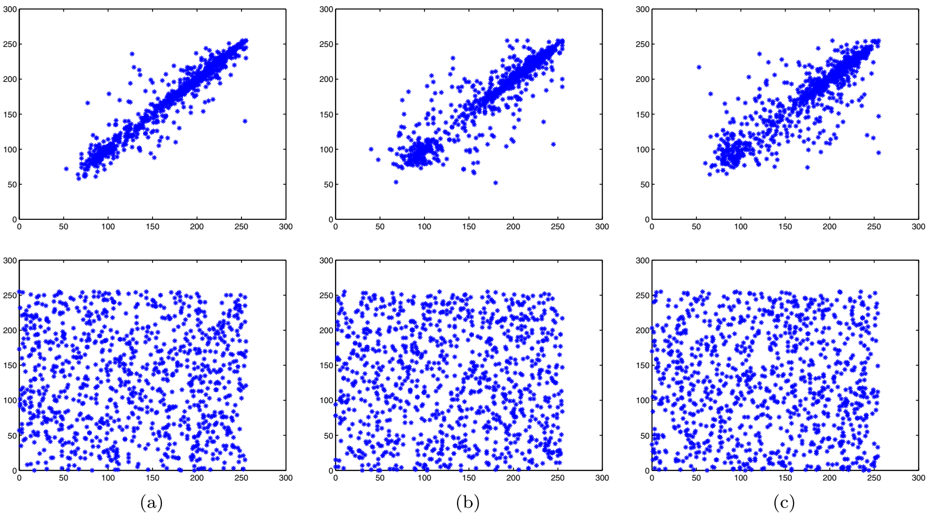


Fig. 6 Correlation analysis of image Lena in R channel. **a** horizontal correlation of original and encrypted images; **b** vertical correlation of original and encrypted images; **c** diagonal correlation of original and encrypted images

Table 3 Correlation coefficient of the some encrypted images in R channel

Image	Original image			Encrypted image		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
lena.bmp	0.9239	0.9567	0.8888	−0.0024	0.0035	0.0014
flower.bmp	0.9563	0.9542	0.9238	0.0025	−0.0017	−0.0037
greens.bmp	0.9758	0.9789	0.9622	−0.0007	0.0103	0.0047
koala.bmp	0.9078	0.9051	0.8687	0.0016	0.0021	0.0039
back.bmp	0.9178	0.9086	0.8661	−0.0036	−0.0071	−0.0019
leaf.bmp	0.8865	0.8577	0.7798	−0.0074	−0.0003	0.0007
bird.bmp	0.9494	0.9426	0.9212	−0.0089	−0.0009	−0.0004
cup.bmp	0.9526	0.9454	0.9092	0.0001	0.0009	−0.0017

Table 3, 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 of the original image.

Table 4 shows the performance comparison with the reference [22]. As seen in Table 4, the correlation coefficient of the encrypted image has the value near zero similar to that in the preceding literature.

5.2.3 Sensitivity analysis

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

$$NPCR = \frac{1}{W \times H} \sum_{i=0}^{H} \sum_{j=0}^{W} D(i, j) \times 100(\%) \tag{12}$$

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

$$UACI = \frac{1}{W \times H} \sum_{i=0}^{H} \sum_{j=0}^{W} \frac{|c_1(i, j) - c_2(i, j)|}{255} \tag{13}$$

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

Table 5 shows NPCR and UACI of 8 images. The results of encryption and decryption of two security keys x_0 and k with tiny difference are shown in Fig. 7. As shown in Table 5 and

Table 4 Correlation coefficient performance

Channel	Proposal			Ref. [22]		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
R	−0.0024	0.0035	0.0014	0.0067	−0.0127	0.0060
G	−0.0008	0.0007	0.0008	−0.0068	−0.0075	−0.0078
B	−0.0033	−0.0028	0.0014	0.0018	−0.0007	0.0026

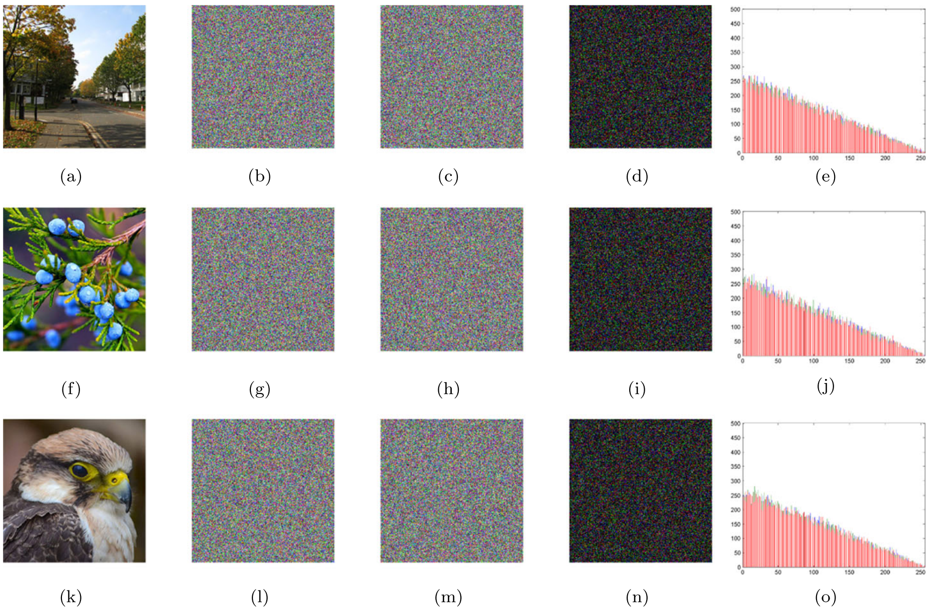


Fig. 7 Encryption results with closed initial values and their difference. **a**, **f**, **k** The original images; **b** the encrypted image(c_1) with $u = 2.56$; **c** the encrypted image(c_2) with $u = 2.560000000000001$; **d**, **e** the pixel-to-pixel difference ($|c_1 - c_2|$) and its histogram; **g** the encrypted image(c_1') with $x_0 = 0.34$; **h** the encrypted image(c_2') with $x_0 = 0.340000000000001$; **i**, **j** the pixel-to-pixel difference ($|c_1' - c_2'|$) and its histogram; **l** the encrypted image(c_1') with $k = 12$; **m** the encrypted image(c_2') with $k = 12.000000000000001$; **n**, **o** the pixel-to-pixel difference ($|c_1' - c_2'|$) and its histogram

Fig. 7, it can be seen that the proposed chaotic system is very sensitive to tiny differences of initial condition.

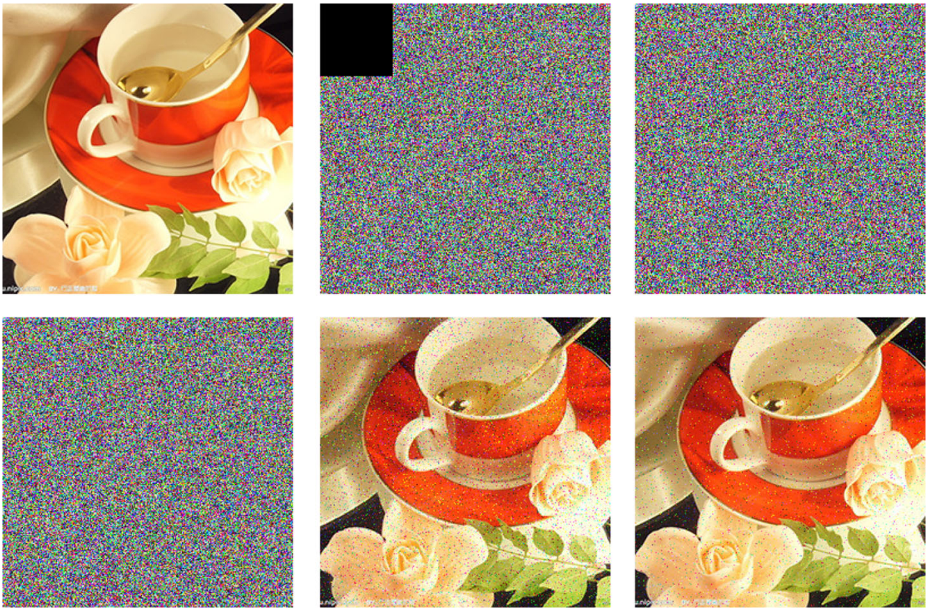
Table 6 shows the performance comparison with the reference [22]. As shown in Table 6, it can be seen that the sensitivity also has the superior performance to the previous systems.

Table 5 The mean NPCR and UACI of the some encrypted images

Image	NPCR(%)			UACI(%)		
	R	G	B	R	G	B
lena.bmp	99.6124	99.6277	99.6399	33.5715	33.3356	33.4044
flower.bmp	99.5682	99.6384	99.617	33.5319	33.5063	33.4894
greens.bmp	99.6201	99.6246	99.6231	33.4527	33.4685	33.515
koala.bmp	99.6201	99.6002	99.585	33.5346	33.4637	33.3583
back.bmp	99.6811	99.6368	99.617	33.4485	33.3744	33.5597
leaf.bmp	99.6414	99.6048	99.6048	33.5595	33.6032	33.5455
bird.bmp	99.5956	99.6246	99.559	33.2906	33.4532	33.2876
cup.bmp	99.6338	99.5956	99.6124	33.3025	33.4557	33.4035

Table 6 The NPCR and UACI performance

	NPCR(%)			UACI(%)		
	R	G	B	R	G	B
Proposal	99.6124	99.6277	99.6399	33.5715	33.3356	33.4044
Ref. [22]	99.6124	99.6134	99.6192	33.4438	33.5232	33.5010



(a) (b) (c)

Fig. 8 Data loss and noise attack (**a**) the encrypted original image and its decrypted image; (**b**) the encrypted image with 64 × 64 data loss and its decrypted image; (**c**) the encrypted image added with 3% $'salt\&pepper'$ noise and its decrypted image

Table 7 The PSNR of the some encrypted images

	lena.bmp	flower.bmp	greens.bmp	koala.bmp	back.bmp	leaf.bmp	bird.bmp	cup.bmp
Data loss	45.8046	45.4999	45.5328	45.7227	45.6335	45.4982	45.7684	45.5385
Noise attack	52.9234	52.8497	52.9709	52.9123	52.8472	53.1511	53.0019	52.6502

Table 8 The PSNR performance

	Proposal	Ref. [18]
Data loss	45.8046	47.4199
Noise attack	52.9234	48.17702

5.2.4 Data loss and noise attack

Digital images can be easily influenced by noise and data loss in different conditions. An image encryption algorithm should have an ability of resisting these abnormal phenomena. To test the ability of resisting the noise, we did some experiments on cutting attack of image data with the size of 64×64 and noise attack with $3\%\ 'salt\&pepper'$.

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

$$PSNR = 10 \times lg\frac{255^2}{MSE}(dB) \tag{14}$$

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

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

In general, the larger the value of PSNR is, the breakdown coefficient of image gets smaller, and when the value of PSNR is above 35dB, it is very difficult to distinguish the decrypted image and the original image. Figure 8 shows the results of decryption and the Table 7 shows the PSNR coefficients in some images. As shown in the experimental results, the proposed encryption algorithm has excellent performance in noise and attacks.

Table 8 shows the performance comparison with the reference [18]. As shown in Table 8, the proposed encryption system has the better superior performance to a noise attack, but has a little bad performance to a data loss, compared to previous systems.

6 Conclusion

In the paper, the improved 1D Logistic map and Sine map made by the output sequences of two same existing 1D chaotic maps were proposed. The experiments verified the chaotic behavior and the chaotic range of the improved chaotic systems. And it also verified that our new chaotic system has a better chaotic performance than existing 1D chaotic systems. We propose a bit-level image encryption algorithm to verify the applications in image encryption of the proposed chaotic system and our simulation and experiments demonstrated that the proposed algorithms have the efficiency in image encryption.

Acknowledgments I would like to take the opportunity to express my hearted gratitude to all thosewho make a contribution to the completion of my article.

References

1. Arroyo D, Diaz J, Rodriguez FB (2013) Cryptanalysis of a one round chaos-based substitution permutation network. Signal Process 67(2):1358–1364
2. Assad SE, Farajallah M (2015) A new chaos-based image encryption system. Signal Process: Image Commun 41:144–157
3. Bhatnagar G, Wu QMJ, Raman B (2012) A new fractional random wavelet transform for fingerprint security. IEEE Trans Syst Man Cybern Part A: Syst Hum 42(1):262–275
4. Bhatnagar G, Wu QMJ, Raman B (2013) Discrete fractional wavelet transform and its application to multiple encryption. Inf Sci 223(2):297–316
5. Chen TH, Wu CS (2010) Compression-unimpaired batch-image encryption combining vector quantization and index compression. Inf Sci 180(9):1690–1701
6. Diaconu AV (2015) Circular inter-intra bit-level permutation and chaos based image encryption. Inf Sci 000:1–14
7. El-Latif AAA, Niu X (2013) A hybrid chaotic system and cyclic elliptic curve for image encryption. AEU 67(2):136–143
8. François M., Grosges T, Barchiesi D, Erra R (2012) A new image encryption scheme based on a chaotic function. Signal Process: Image Commun 27(3):249–259
9. Fu C, Lin BB, Miao YS, Liu X, Chen JJ (2011) A novel chaos-based bit-level permutation scheme for digital image encryption. Opt Commun 284(23):5415–5423
10. Hua Z, Zhou Y, Pun CM, Chen CLP (2014) 2D sine logistic modulation map for image encryption. Inf Sci 297:80–94
11. Jeng FG, Huang WL, Chen TH (2015) Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes. Signal Process: Image Commun 34:45–51
12. Kassem A, Hassan HAH, Harkouss Y, Assaf R (2014) Efficient neural chaotic generator for image encryption. Digit Signal Process 25(2):266–274
13. Kumar RR, Kumar MB (2014) A new chaotic image encryption using parametric switching based permutation and diffusion. Ictact J Image Video Process 4(5):795–804(10)
14. Li S, Chen G, Cheung A, Bhargava B, Lo KT (2005) On the design of perceptual MPEG-video encryption algorithms. IEEE Trans Circ Syst Video Technol 17(2):214–223
15. Liu ZH, Wang X (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 284(16–17):3895–3903
16. Lv-Chen C, Yu-Ling L, Sen-Hui Q, Jun-Xiu L (2015) A perturbation method to the tent map based on Lyapunov exponent and its application. Chin Phys B 24(10):78–85
17. Nandeesh GS, Vijaya PA, Sathyanarayana MV (2013) An image encryption using bit level permutation and dependent diffusion. Int J Comput Sci Mob Comput 2(5):145–154
18. Pak C, Huang L (2017) A New color image encryption using combination of the 1D chaotic map. Signal Process 138:129–137
19. Sangeetha Y, Meenakshi S, Sundaram CS (2014) A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimed Tools Appl 71(3):1469–1497
20. Song CY, Qiao YL, Zhang XZ (2013) An image encryption scheme based on new spatiotemporal chaos. Optik 124(124):3329–3334
21. Teng L, Wang X (2012) A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive. Opt Commun 285(20):4048–4054
22. Wang X, Zhang HL (2015) A color image encryption with heterogeneous bit-permutation and correlated chaos. Opt Commun 342:51–60
23. Wang W, Si M, Pang Y, Ran P, Wang H, Jiang X, Liu Y, Wu J, Wu W, Chilamkurti N, Jeon G (2018) An encryption algorithm based on combined chaos in body area networks. Comput Electr Eng 65:282–291
24. Wen W, Zhang Y, Fang Z, Chen JX (2015) Infrared target-based selective encryption by chaotic maps. Opt Commun 341:131–139
25. Xu L, Li Z, Li J, Hua W (2016) A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 78(21):17–25
26. Zhang Y, Xiao D (2014) An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Commun Nonlinear Sci Numer Simul 19(1):74–82
27. Zhang W, Wong KW, Yu H, Zhu ZL (2013) A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Commun Nonlinear Sci Numer Simul 18(3):584–600
28. Zhou Y, Panetta K, Agaian S, Chen CL (2012) (N, k, p)-gray code for image systems. IEEE Trans Syst Man Cybern Part A Syst Hum 43(2):515–529

29. Zhou Y, Panetta K, Agaian S, Chen CLP (2012) Image encryption using P-Fibonacci transform and decomposition. Opt Commun 285(5):594–608
30. Zhou Y, Bao L, Chen CLP (2013) Image encryption using a new parametric switching chaotic system. Signal Process 93(11):3039–3052
31. Zhou Y, Cao W, Chen CLP (2014) Image encryption using binary bitplane. Signal Process 100(7):197–207

Chanil Pak I have already published a journal entitled “A new color image encryption using a combination of t he 1D chaotic map”. (Signal Processing, 2017, 138 :129-137) I am now reviewer of the journal “Signal Processing”, “International Journal of Electronics and Device Physics” and “American Journal of Applied Mathematics”.