Scientific Research Publishing

Journal of Information Security, 2017, 8, 23-41
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Robust Chaos-Based Image Cryptosystem with an Improved Key Generator and Plain Image Sensitivity Mechanism

Hidayet Oğraş[1], Mustafa Türk[2]

[1]Department of Electrical Education, Batman University, Batman, Turkey
[2]Department of Electrical and Electronics Engineering, Firat University, Elazig, Turkey
Email: hidayet.ogras@batman.edu.tr

How to cite this paper: Oğraş, H. and Türk, M. (2017) A Robust Chaos-Based Image Cryptosystem with an Improved Key Generator and Plain Image Sensitivity Mechanism. *Journal of Information Security*, **8**, 23-41.
http://dx.doi.org/10.4236/jis.2017.81003

Received: November 29, 2016
Accepted: December 26, 2016
Published: December 29, 2016

Abstract

In this paper, we propose an effective gray image cryptosystem containing Arnold cat map for pixel permutation and an improved Logistic map for the generation of encryption keys to be used for pixel modification. Firstly, a new chaotic map is designed to show better performance than the standard one in terms of key space range, complexity and uniformity. Generated secret key is not only sensitive to the control parameters and initial condition of the improved map but also strongly depend on the plain image characteristic which provides an effective resistance against statistical and differential attacks. Additionally, to get higher encryption strength of the cryptosystem, both confusion and diffusion processes are performed with different keys in every iterations. Theoretical analysis and simulation results confirm that the proposed algorithm has superior security and effectively encrypts and decrypts the gray images as well.

Keywords

Chaos, Image, Cryptosystem, Logistic Map, Diffusion, Arnold Cat Map

1. Introduction

With the rapid development of information technology and widely use of computer networks, multimedia applications have become much more prevalent than the past. This situation creates security problems of transferring information in communication network and thus, confidentiality of the information is becoming a serious issue nowadays. Among the multimedia information, digital image plays an important role in people's daily life so the protection of visual information has become a major task. Encryption is an ordinary solution for the protection of information. Most of the available encryption methods such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and IDEA (International Data Encryption Algorithm) are typically used for text-structure data [1] [2] [3]. However, compared to text, digital images have some intrinsic features such as bulk data capacity, high redundancy and strong correlation among adjacent pixels [4] [5]. Hence, these algorithms are not suitable for image encryption [1] [6] due to the requirement of much more processing power, bandwidth and longer time which causes low-level efficiency during encryption and decryption processes [7].

Chaotic systems have important properties of sensitivity to initial conditions and control parameters, pseudo-randomness and ergodicity [2] [8] [9], which meet Shannon's requirements of confusion and diffusion in cryptography [10]. These characteristics make the chaotic systems a good candidate for data encryption and create the phenomena of chaos-based cryptography. Many chaos-based image cryptosystems are proposed in this field recently [1]-[11]. However, some of them are successfully broken [12]-[17] due to their small key spaces and weakly secure encryption mechanisms. Among these weaknesses, the most serious one is that the key element used in cryptosystem completely depends on the secret key which means that the same key is used to encrypt different plain images. This property allows the attacker to launch known-plaintext attack or chosen-plaintext attack for cryptanalysis.

Discrete time chaotic systems have high efficiency comparing with the continuous time chaotic systems [18] and their implementations are very easy in software and hardware platforms. However, these systems have serious disadvantages of limited or discontinuous range of chaotic behaviors and generally show non-uniform data distribution of output [11]. Using such systems in a cryptosystem creates crucial drawbacks such as small key space, weak security and poor efficiency which threat the security of the whole cryptosystem. As a result, a new improved Logistic map has been designed to overcome these weaknesses. A good pseudo-random key generator should be a stochastic and supposed to generate uniform key that should be random, non-periodic and equally distributed as possible for an effective encryption [19]. Improved map is expected to provide these properties and demonstrates better performance than the standard one.

The proposed cryptosystem utilizes Arnold Cat map (ACM) method that is used to transform all pixel positions of original image to their corresponding positions without changing their values. This part breaks the strong correlation of adjacent pixels and creates a confused image. In diffusion part, all pixels values are modified sequentially through a diffusion function as one pixel change can influences other pixels, which keeps high plain-text and cipher-text sensitivity. The rest of the paper is organized as follows: Section 2 gives brief overview of the standard Logistic map (SLM) with its dynamic defect. Section 3 introduces an improved Logistic map (ILM) with statistical analysis. In Section 4, the proposed cryptosystem is described in detail. Security and performance of the proposed algorithm are analyzed in Section 5. Finally, the conclusions will be discussed in Section 6.

2. Research Question

Standard Logistic Map (SLM)

Standard map is one of the simplest discrete systems that exhibit chaos and defined by

$$x_{n+1} = r \cdot x_n \left(1 - x_n\right) \tag{1}$$

where $0 < r \le 4$ is called control parameter and $x_n \in (0,1)$. When $r \in [3.57, 4]$, then the map is in chaos state, which means that x_n is aperiodic, non-convergent and very sensitive to initial value x_0. However, some isolated values [20], such as $r = 3.83$ appear to show non-chaotic behavior that results neither uniform nor random output distribution. Additionally, SLM demonstrates perfect chaotic properties in the case of $r = 4$ only. In cryptographic manner, this situation reduces the key space if the control parameter is used as a key parameter. As a key generator, what should be done on SLM to overcome that issue? An improved Logistic map with larger key space will be designed and its all parameters should keep the system fully chaotic.

3. Methodology

3.1. Improved Logistic Map (ILM)

We modify SLM by adding a new parameter to the map equation as the following

$$x_{n+1} = \lambda \cdot x_n \left(1 - x_n\right) + p \tag{2}$$

where x_n values are restricted to the interval of $\left[(1-\alpha)/2, (1+\alpha)/2\right]$ and $0 < \alpha < 1$. In Equation (2), maximum point occurs at $x_n = 0.5$ and its value is $(\lambda/4) + p$, while the minimum occurs at $x_n = (1-\alpha)/2$ and its value is $\lambda \cdot (1-\alpha) \cdot (1+\alpha)/4 + p$. Thus,

$$\begin{aligned} \frac{1-\alpha}{2} &= \lambda \cdot \left(\frac{1-\alpha}{2}\right) \cdot \left(\frac{1+\alpha}{2}\right) + p \\ \frac{1+\alpha}{2} &= \frac{\lambda}{4} + p \end{aligned} \tag{3}$$

by solving the above equations, we get $\lambda = 4/\alpha$ and $p = \left(\alpha^2 + \alpha - 2\right)/2\alpha$. Substituting these into Equation (2), then we get,

$$x_{n+1} = \frac{4 \cdot x_n \left(1 - x_n\right) - 1}{\alpha} + \frac{1+\alpha}{2} \tag{4}$$

where the range of α is limited by 1. To make larger key space, the interval of the α must be increased. Hence, the following transformation is applied to the map which divides α in the first term and spreads its range in the system.

$$\alpha \Rightarrow \alpha/s \tag{5}$$

Finally, we obtain the equation of ILM as

$$x_{n+1} = \frac{4sx_n\left(1-x_n\right)-s}{\alpha} + \frac{s+\alpha}{2s} \tag{6}$$

where $1 < \alpha < s$. Now, x_n values are restricted to $\left[\frac{s-\alpha}{2s}, \frac{s+\alpha}{2s}\right]$. Here, s parameter must be always bigger than α, otherwise x_n values appear out of the range (0, 1). If $\alpha = s$, then the improved map will become standard one again. Additionally, the closer α to s value, the bigger range of x_n occurs at output. We specify the relationship between s and α by the following equation.

$$\alpha = s - x_0 \tag{7}$$

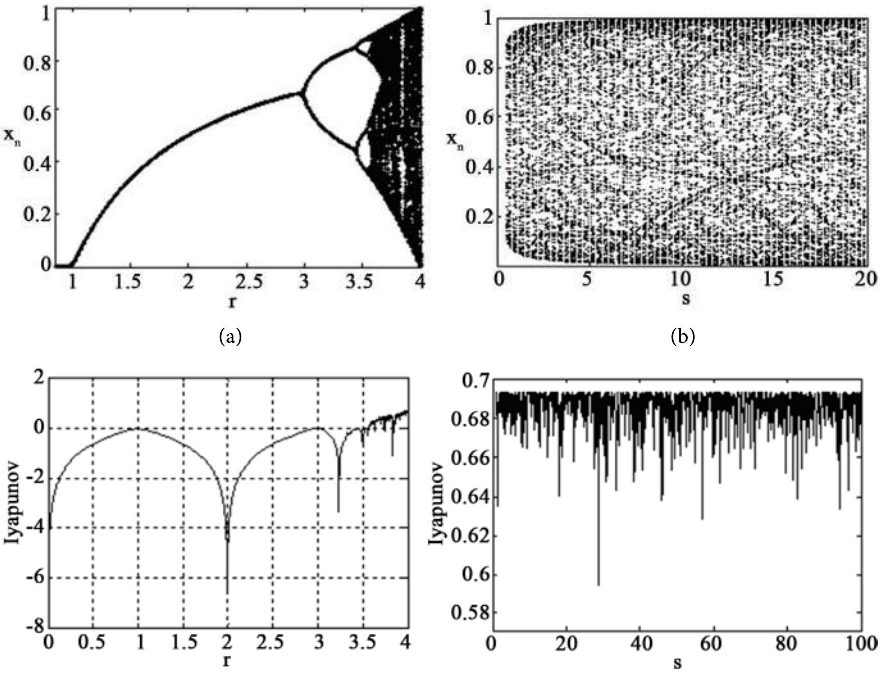
Here, α and s are used as key parameters for the proposed cryptosystem and they are not limited to a finite value for ILM to be in chaos state, whereas in standard map the control parameter is limited to 4.

3.2. Lyapunov and Bifurcation Analyses

Lyapunov exponent states a checkable criterion for sensitivity to initial conditions of a nonlinear dynamical system [20] and it is defined for discrete time systems by the following equation.

$$\lambda = \lim_{n\to\infty} \frac{1}{n}\sum_{i=0}^{n-1} \ln\left|f'\left(x_i\right)\right| \tag{8}$$

A positive Lyapunov exponent indicates that the dynamical system is chaotic [21]. The behavior of a dynamical system from a fixed point to a chaos with respect to its control parameter is given by a bifurcation diagram. Figure 1 shows



(a) (b)

(c) (d)

Figure 1. (a) Bifurcation diagram of the SLM; (b) Bifurcation diagram of the ILM; (c) Lyapunov spectrum of SLM; (d) Lyapunov spectrum of ILM.

the Lyapunov spectrums and bifurcation diagrams of the SLM and ILM. Lyapunov coefficients for ILM are always greater than or equal to the values of SLM which shows that ILM has better mixing property. **Figure 1(a)** and **Figure 1(b)** show the bifurcation diagrams of the SLM and ILM, respectively. In **Figure 1(b)**, there are no free white spaces and the entire area is almost covered. More importantly, all values of *s* can be used to build the key space.

3.3. Randomness Analysis

Randomness means the lack of predictability in a sequence of symbols [19]. We use NIST (National Institute of Standards and Technology) standard to evaluate the degree of randomness of the ILM outputs. NIST consists of fifteen tests [22] and each test produces a *p*-value which is a real number in [0, 1]. If *p*-value is greater than a predefined threshold, called significance level $(\alpha = 0.01)$, then the statistical test is passed successfully and the generator is considered as random with 99% confidence. In order to get sequential bit streams, the following transformation is applied to the output of the ILM.

$$b_n = \begin{cases} 1, & x_n \geq 0.5 \\ 0, & x_n < 0.5 \end{cases} \tag{9}$$

A threshold level of 0.5 is used to generate a bit value “1” or “0” for each x_n. We randomly choose the system parameters as $s = 999$ and $x_0 = 0.009$ in order to obtain 1,000,000 bits to carry on NIST. The results are given in **Table 1**.

According to the NIST result, it can be concluded that ILM is quite stochastic and generates chaotic sequences which has sufficient randomness.

Table 1. Results of the NIST test.

Test name	*p*-value	Result
Frequency	0.9362	Success
Block frequency	0.2736	Success
Runs	0.1597	Success
Long runs of ones	0.1484	Success
Rank	0.6484	Success
Spectral DFT	0.3684	Success
Non-overlapping templates (m = 9; B = 000000001)	0.9320	Success
Overlapping templates (m = 9)	0.8690	Success
Universal (L = 7; Q = 1280)	0.3369	Success
Linear complexity	0.0513	Success
Serial-1 (m = 5)	0.9486	Success
Serial-2 (m = 5)	0.9667	Success
Approximate entropy (m = 5)	0.8972	Success
Cumulative sums forward	0.5753	Success
Cumulative sums reverse	0.6476	Success
Random excursions (x = +1)	0.2995	Success
Random excursions variant (x = −1)	0.6508	Success

4. Proposed Cryptosystem

Chaos-based image encryption systems are generally composed of two stages: replacement of pixels called confusion and modification of pixel values called diffusion [3] [5] [6]. The flowchart of the proposed cryptosystem is shown in Figure 2.

4.1. Confusion Stage

In an ordinary image, adjacent pixels have strong correlation. This strong correlation need to be broken before encryption. Arnold Cat Map is an invertible discrete system that will be used to rearrange the pixel positions of the plain image in a way that the adjacent pixels are far enough from each other. It is represented by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{10}$$

where (x, y) are the pixel position of the plain image with a size of $N \times N$ and (x', y') is the corresponding pixel position. Control parameters of the map are p and q, which are positive integers and will be used as confusion key parameters. The inverse of ACM is determined by the following equation.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod N \tag{11}$$

ACM effectively changes all pixel positions as only linear transformation with simple mod function need to be performed. Furthermore, it has a characteristic of area-preserving which means that if it is iterated enough times, original image reappears. Shortly, ACM can be considered as a permutation method that focuses on the pixel position not the pixel value of the plain image. Hence, the cryptosystem requires a diffusion process to enhance the security.

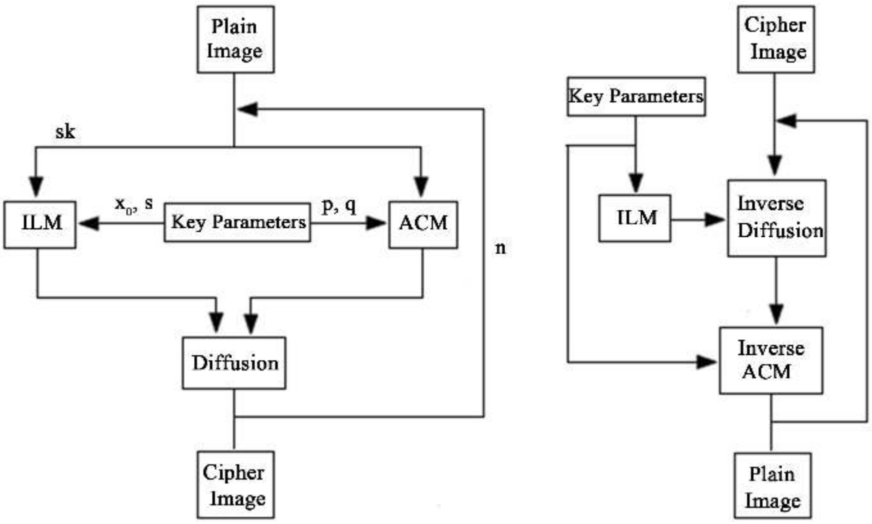


Figure 2. The flowchart of the proposed cryptosystem (a) Encryption scheme (b) Decryption scheme.

4.2. Diffusion Stage

In a gray image, each pixel is represented by 8-bit in decimal range [0, 255]. Key must be same format with the pixel in the image to operate diffusion. However, the output of the ILM is a floating-point value. Thus, the following equation is used to obtain encryption key.

$$\text{key} = \text{mod}\left(\text{round}\left(x_n \times 10^9\right), 256\right) \tag{12}$$

The proposed cryptosystem uses a *sk* parameter which is strongly depends on the pixel values and size of the plain image. It provides different keys even with the same parameters of the cryptosystem and defined by

$$\begin{aligned} sk &= \left|\sum_{i=1}^{N\times N}(-1)^i\{\text{normalized\_img}\}\right| + \max\left(\text{normalized\_img}\right) + \frac{1}{\sqrt{N}} \\ \text{normalized\_img} &= \frac{\text{plain\_img}}{256} \end{aligned} \tag{13}$$

where normalized image has a size of $1\times N^2$ pixels. This parameter is not a secret key but will be used to generate different keys by modifying the initial value of the ILM as in Equation (14).

$$X_0 = \text{mod}\left(x_0 + sk, 1\right) \tag{14}$$

Diffusion is a process in which the pixel values of confused image are modified sequentially by mixing the encryption key. Diffusion operation used in the cryptosystem is given by

$$c(i) = k(i) \oplus \left\{p(i) - c(i-1) + k(i)^2 + 256\right\} \bmod 256 \tag{15}$$

where $p(i)$, $c(i)$, $k(i)$ and $c(i-1)$ represent the current plain pixel, output cipher pixel, encryption key and the previous cipher pixel, respectively. Such a diffusion function is very efficient because simple modular arithmetic and logical operations can be performed in high speed. The current diffused pixel is depend on the previous one, so a small change in the plain image will affect more than one pixel in the cipher image and reflects the diffusion to whole cipher image. Here, we encode the first cipher pixel as

$$c(0) = \left\{\text{round}\left(\left(\alpha + sk\right)\times 10^5\right)\right\} \bmod 256 \tag{16}$$

and its value depends on s, x_0 and sk parameters of the cryptosystem. In every iteration, a new *sk* is determined from the current cipher image, so ILM runs with similar parameter of *s*, but different initial value of x_0 which allows to produce different key for the next iteration of encryption. The proposed image encryption is a symmetric algorithm which means that identical key is used for decryption process. The decryption algorithm is the reverse diffusion and defined by

$$p(i) = \left\{\left(k(i) \oplus c(i)\right) + c(i-1) - k(i)^2 + 256^2\right\} \bmod 256 \tag{17}$$

The confusion and diffusion processes complete the proposed image encryption structure. For instance, Lena image is encrypted by the proposed cryptosystem with a key of $s = 98.765432$, $x_0 = 0.123456$, $n = 7$, $p = 5$ and $q = 4$. The result is shown in Figure 3.

5. Security and Performance Analysis

5.1. Key Space Analysis

Key space size is the total number of different keys that can be used in a cryptosystem. For an ideal encryption algorithm, it should be larger than 2^{100} to make brute-force attack infeasible [6]. In the cryptosystem, the secret key parameters are x_0, s, p, q and n. According to the IEEE (Institute of Electrical and Electronics Engineers) floating-point standard [2], the computational precision of the 64-bit double precision number is about 10^{15}. Number of iteration and each confusion parameter are 8-bit key. Hence, the total number of possible key is approximately,

$$\text{key} = \left(10^{15\times 2} \times 2^{24}\right) \approx 2^{124} \tag{18}$$

which is sufficient to resist brute-force attack.

5.2. Key Sensitivity Analysis

Key sensitivity analysis can be observed in two aspects: (i) if slightly different keys are applied to encrypt the same images, then completely different cipher images should be produced; (ii) if a tiny difference exists in decryption key, then the cipher image could not be decrypted correctly. For the first key sensitivity analysis, a test plain of cameraman image is encrypted with a randomly chosen key of $s = 98.765432$, $x_0 = 0.123456$. Then a slight change 10^{-6} is applied to the one of the parameters with the other remains same, and repeats the encryption. The corresponding cipher images and the differential images are shown in Figure 4. The correlation coefficients between the cipher images are calculated and given in Table 2.

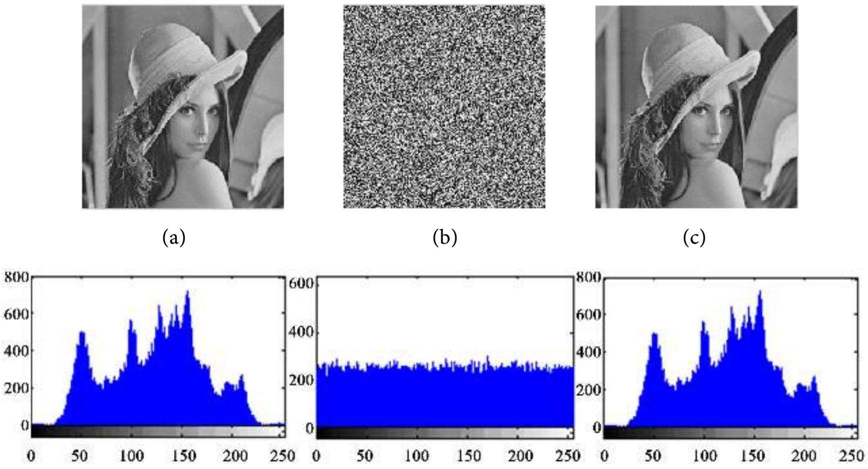


Figure 3. The result of the proposed cryptosystem (a) Original Lena image; (b) Encrypted Lena image; (c) Decrypted image; (d) Histogram of (a); (e) Histogram of (b); (f) Histogram of (c).

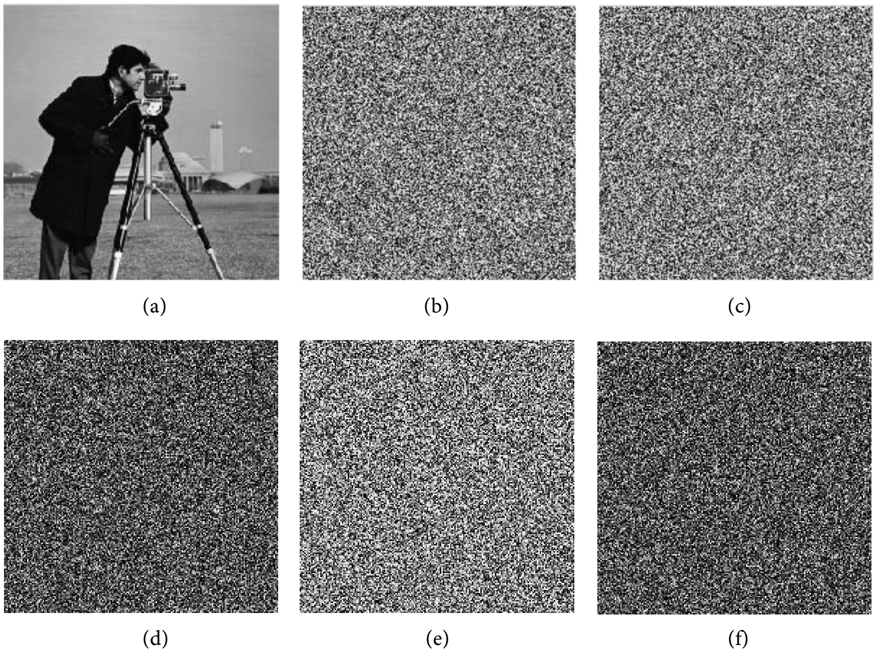


Figure 4. Key sensitivity in the first case: (a) Plain image; (b) Cipher image with $s = 98.765432$, $x_0 = 0.123456$; (c) Cipher image with $s = 98.765431$, $x_0 = 0.123456$; (d) Differential image between (b) and (c); (e) Cipher image with $s = 98.765432$, $x_0 = 0.123457$; (f) Differential image between (b) and (e).

Table 2. Correlation coefficients between cipher images produced by slightly different keys.

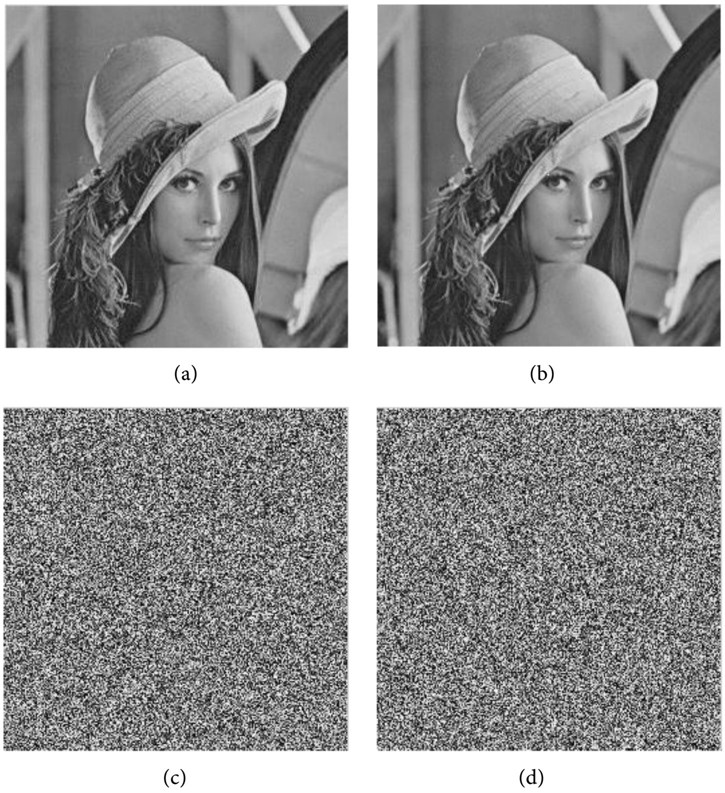
Figure 4	Key			Correlation coefficients between
	Sk	x_0	*n*	
(b)-(c)	98.765431	0.123456	2	0.00403
(b)-(e)	98.765432	0.123457	2	−0.00022

In Table 2, the negative correlation means that for two cipher images, an increase in one of them is associated with a decrease in the other. In order to observe the effect of *sk* in the cryptosystem, we use two Lena images that one of them has a central pixel difference and then proceed the encryption with same key parameters for both images. Graphical and numerical results are shown in Figure 5 and Table 3.

The proposed cryptosystem should also be sensitive to *p*, *q* and *n*. Cipher images produced by slightly different keys are shown in Figure 6 and the correlation coefficients for corresponding cipher images are given in Table 4.

These results show that despite being a very small difference at all encryption keys, corresponding cipher images are completely different. For the second case, when a slightly different key is used in decryption, then the cipher image could not be decrypted correctly. Cipher Lena image in Figure 3(b) is used for second key sensitivity analysis and the result is shown in Figure 7.

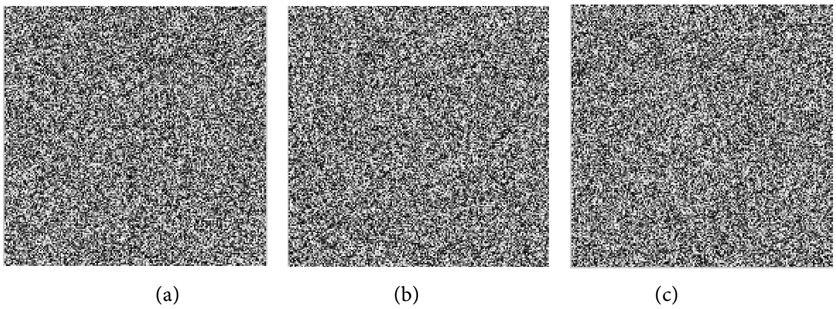
We conclude that the proposed cryptosystem is quite sensitive to all keys and can effectively resist differential attacks.



(a) (b)

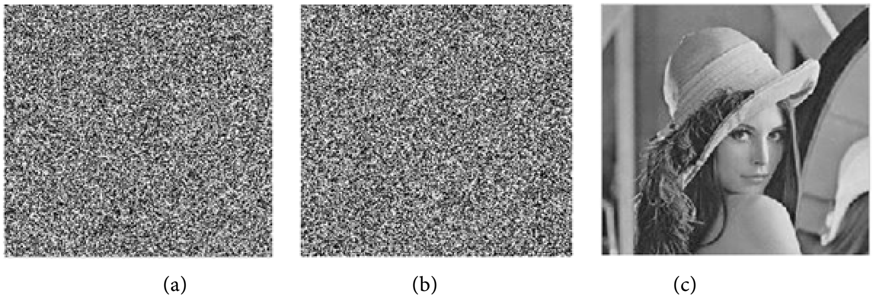
(c) (d)

Figure 5. (a) Original Lena image; (b) Lena image with central pixel difference; (c) Cipher Lena image; (d) Cipher Lena image with central pixel difference.



(a) (b) (c)

Figure 6. Key sensitivity in the first case: (a) Cipher image with $p=6$, $q=4$, $n=7$; (b) Cipher image with $p=5$, $q=3$, $n=7$; (c) Cipher image with $p=5$, $q=4$, $n=6$.



(a) (b) (c)

Figure 7. Key sensitivity in the second case: (a) Wrong decrypted image with $s=98.765433$, $x_0=0.123456$; (b)Wrong decrypted image with $s=98.765432$, $x_0=0.123457$; (c) Correct decrypted image with $s=98.765432$, $x_0=0.123456$.

Table 3. Correlation coefficients between cipher images produced by slightly different keys.

Figure 5	Key		Correlation coefficients between
	sk	*α*	
(a)	10.402343	98.641976	
(b)	10.398437	98.641976	
(a)-(b)			0.999915
(c)-(d)			0.004622

Table 4. Correlation coefficients between cipher Lena images produced by slightly different keys.

Figures	Keys			Figures between	Correlation coefficients between
	p	*q*	*n*		
3(b)	5	4	7		
6(a)	6	4	7	3(b)-6(a)	−0.0019
6(b)	5	3	7	3(b)-6(b)	0.0028
6(c)	5	4	6	3(b)-6(c)	0.0044

5.3. Histogram Analysis

In image processing, histogram is used to represent the distribution of the pixel values in an image. Equal probability of each pixel value creates a uniform histogram which is more robust against statistical attacks in terms of security [4]. Hence, the ideal histogram of a ciphered image should be fairly uniform and quite different from that of the plain image. The histograms of different plain images and corresponding cipher images produced by the proposed cryptosystem are shown in Figure 8 and Figure 9, respectively.

It is clear that the histograms of the cipher images are significantly different than the originals and uniformly distributed even the plain image is purely black.

5.4. Information Entropy Analysis

Information entropy is a measure of uncertainty associated with a random message [2] [19]. The entropy of an information source with a length of N is determined by

$$H(X) = -\sum_{i=1}^{N} p(x_i) \cdot \log_2 p(x_i) \tag{19}$$

where $H(X)$ and $p(x_i)$ represent the information entropy in bits and the probability of symbol x_i, respectively. Let us suppose a truly random source emitting 2^8 symbols as $S = \{s_1, s_2, \cdots, s_{256}\}$ with equal probability, then the entropy will be calculated to 8 which is an ideal result. For a practical information source, its entropy value is smaller than the ideal one. Generally, the more uncertain or random source is, the more information entropy it will contain [4].

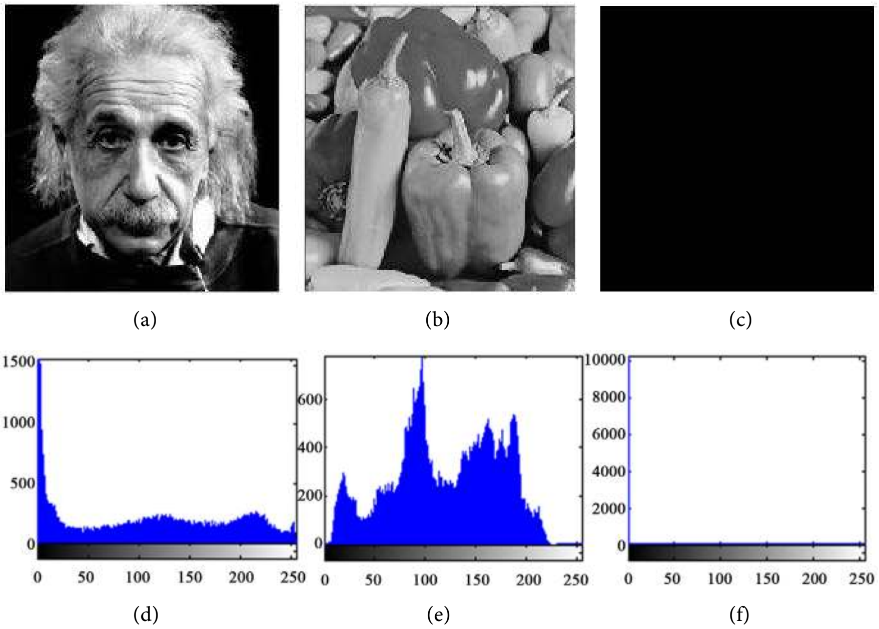


Figure 8. Histogram of different plain images: (a) Einstein; (b) Peppers; (c) Black; (d) Histogram of (a); (e) Histogram of (b); (f) Histogram of (c).

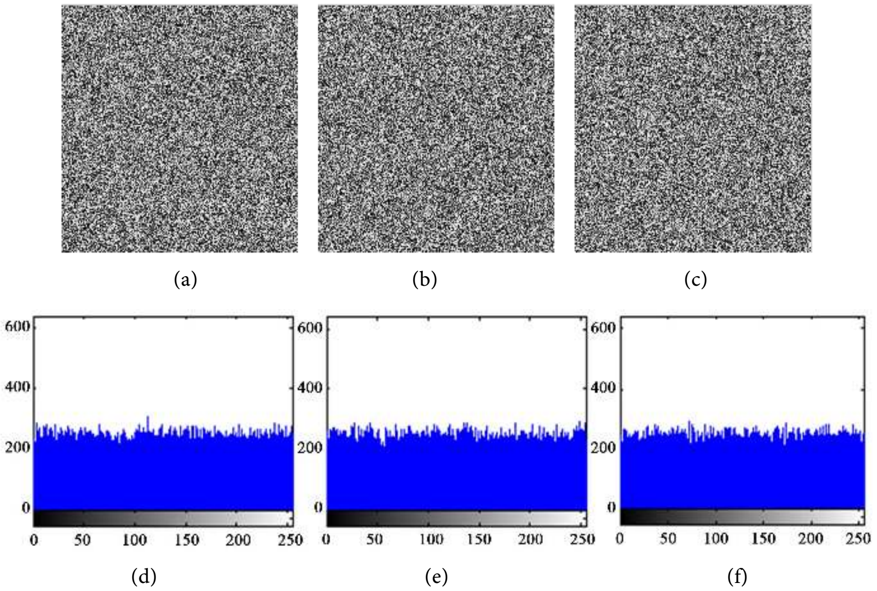


Figure 9. Histogram of corresponding cipher images: (a) Cipher Einstein; (b) Cipher Peppers; (c) Cipher Black; (d) Histogram of (a); (e) Histogram of (b); (f) Histogram of (c).

Maximum entropy is achieved in the case of a uniform probability distribution. We randomly chose eight test images (Lena, Baboon, Frog, Goldhill, Cat, Landscape, Truck and Clown) which are available on Internet, to be used for entropy analysis. Then these images are encrypted using the proposed cryptosystem. The entropy results for the test images and corresponding cipher images are listed in Table 5. The reported average entropy result (Lena, Baboon, Frog, Goldhill, Truck, Clown) in [9] is 7.999327. In our scheme, using the same plain images in [9], the average entropy is calculated to 7.999461.

Table 5. Entropy results for the plain and corresponding cipher images.

Test images	Plain image	Cipher image
Lena	7.229783	7.999247
Baboon	7.183162	7.999378
Frog	6.994144	7.999255
Goldhill	7.705715	7.999229
Cat	7.206827	7.999833
Landscape	7.353287	7.999815
Truck	7.343335	7.999842
Clown	7.766840	7.999813

It is obvious that the entropies of the cipher images are very close to the ideal value, which means that the proposed algorithm is secure against entropy attacks.

5.5. Correlation Analysis

A meaningful image has a property of strong correlation between adjacent pixels since its pixel values are close to each other. A cipher image with sufficiently low pixel correlation should be produced after the encryption. To evaluate the correlation coefficients for all the pairs of the adjacent pixels in diagonal direction, the following formula is used

$$cc = \frac{\sum_{i=1}^{N}\left(x_i - \bar{x}\right)\cdot\left(y_i - \bar{y}\right)}{\sqrt{\left(\sum_{i=1}^{N}\left(x_i - \bar{x}\right)^2\right)\cdot\left(\sum_{i=1}^{N}\left(y_i - \bar{y}\right)^2\right)}} \tag{20}$$

where $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$. N defines the total number of pairs of diagonally adjacent pixels. The results of the correlation coefficients using four test images and their corresponding cipher images are given in Table 6.

Figure 10(a) shows the diagonal correlation of the plain Lena image having a linear distribution, where the value of its adjacent pixel has a high correlation. On the contrary, correlation distribution of the cipher Lena is random where the value of a pixel and the value of its adjacent pixel have low correlation. They are scattered over the entire plain as shown in Figure 10(b).

5.6. Differential Attack Analysis

Generally, if only one pixel change in the plain image causes a significant change in the cipher image, then the image cryptosystem will resist the differential attack efficiently. Two common approaches, namely, NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are used to test the influence of only one pixel change in the plain image over the whole cipher image. They are defined [11] as in Equations (21)-(23).

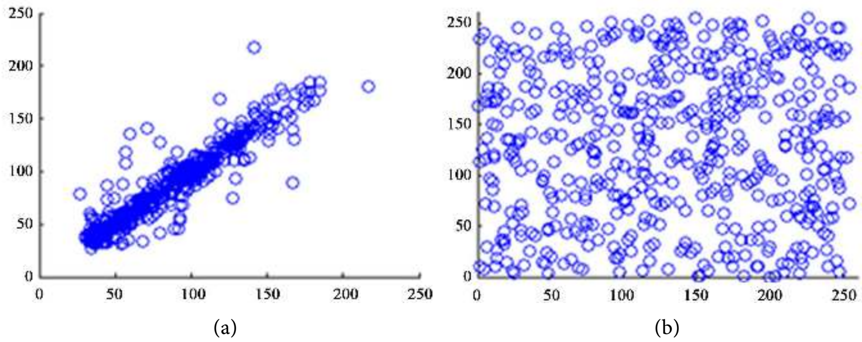


Figure 10. Correlation distribution of adjacent pixels: (a) Plain Lena image (b) Cipher Lena image.

Table 6. Correlation coefficients diagonally.

Test images	Plain image	Cipher image
Flowers	0.89561	−0.00348
Cameraman	0.89237	0.01957
Liberty statue	0.95275	−0.02114
Landscape	0.97320	0.01522

$$\text{NPCR} = \frac{1}{W \times H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)\right] \times 100\% \tag{21}$$

where $D(i,j)$ is defined as

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{22}$$

$$\text{UACI} = \frac{1}{W \times H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H} \frac{\left|C_1(i,j) - C_2(i,j)\right|}{255}\right] \times 100\% \tag{23}$$

With W and H are the width and height of the cipher image. C_1, C_2 are the two cipher images corresponding to two plain images with only one pixel difference. NPCR measures how many pixels are different between two cipher images by using same encryption key. UACI is used to measure the average intensity of differences between C_1 and C_2. NPCR and UACI values [3] for two random images, which are an expected estimates for an ideal image cryptosystem should be 99.60% and 33.46% respectively. Lena test image is used to measure NPCR and UACI. Firstly, Lena is encrypted to C_1. Then, we have changed the gray value 96 of the pixel at $(128,128)$ by 97 and the image with small change is encrypted to C_2. We present a comparison of a reference [9] and our result in **Table 7**. From the **Table 7**, the simulation results show that the NPCR and UACI performance of the proposed scheme can reach 99.62% and 33.45% in the first iteration of encryption, respectively. On the other hand, other algorithm in [9] gets the close ideal value after 5 iterations.

It is obvious that our proposed scheme is stable under NPCR and UACI analysis and highly sensitive at plain image even in the first iteration.

Table 7. Differential analysis of the proposed scheme.

n	Proposed scheme		Reference [9]	
	NPCR	UACI	NPCR	UACI
1	99.62	33.45	0.422	0.136
2	99.55	33.51	81.19	27.38
3	99.58	33.57	99.60	33.39
4	99.63	33.44	99.59	33.47
5	99.62	33.45	99.63	33.48

5.7. Data Loss and Noise Attack Analysis

A powerful image cryptosystem should resist data loss during transmission. Figure 11 shows a simulation result of the data loss attack. A test image of Liberty statue is first encrypted using the proposed algorithm. Then, generated cipher image is applied with a data cut size of 50×50 and decryption is performed to the cipher image. According to the result, the decrypted image contains most of the original information although there are limited data losses in cipher image. This result also demonstrates another important property of the pixels replacement in encryption.

For noise attack analysis, Lena image is encrypted and then "Salt & Pepper" with 1% noise is added to create noisy encrypted image. The result of the noise attack is shown in Figure 12. As it is shown below, recovered image is highly similar to the original one.

5.8. Encryption Speed Analysis

In order to evaluate the running speed of the proposed cryptosystem, enough number of test images are encrypted. Then, we have analyzed the average encryption/decryption rate of the proposed algorithm on Intel Core i7 3.4 GHz CPU with 4 GB RAM running on Windows 7 by using MATLAB 7.9 software. The average execution time for the results can be found in Table 8.

5.9. Performance Comparison

In this section, we will compare the performance of the SLM and ILM in the proposed cryptosystem with the same key parameters. The effects of these two maps on the cipher images will be evaluated under the same conditions. Histogram, entropy and correlation coefficient analysis are performed for the corresponding cipher images. Lena image is used for both encryption processes. Cryptosystem-1 uses the SLM as a key generator with the parameters of $r = 3.83$, $x_0 = 0.1$, $p = 5$, $q = 4$ and $n = 1$. Cryptosystem-2 uses the ILM as a key generator with the parameters of $s = 3.83$, $x_0 = 0.1$, $p = 5$, $q = 4$ and $n = 1$. After the encryption, obtained histograms of the corresponding cipher images are shown in Figure 13.

From the histogram results, it is obvious that the output of the Cryptosystem-1 is not as uniform as the Cryptosystem-2 and vulnerable to statistical attacks.

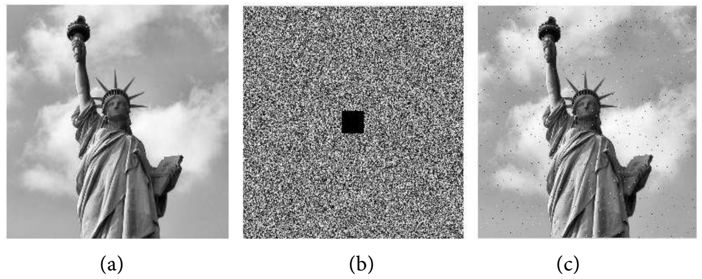


Figure 11. Data loss analysis: (a) Original Libert statue image; (b) Cipher image with 50×50 data cut; (c) Decrypted image of (b).

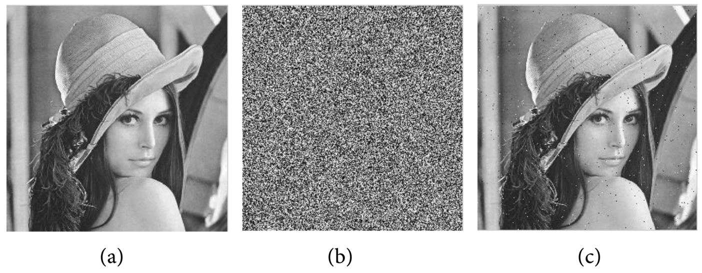


Figure 12. Noise attack analysis: (a) Original Lena image; (b) Cipher image added with 1% "salt & pepper" noise; (c) Decrypted image of (b).

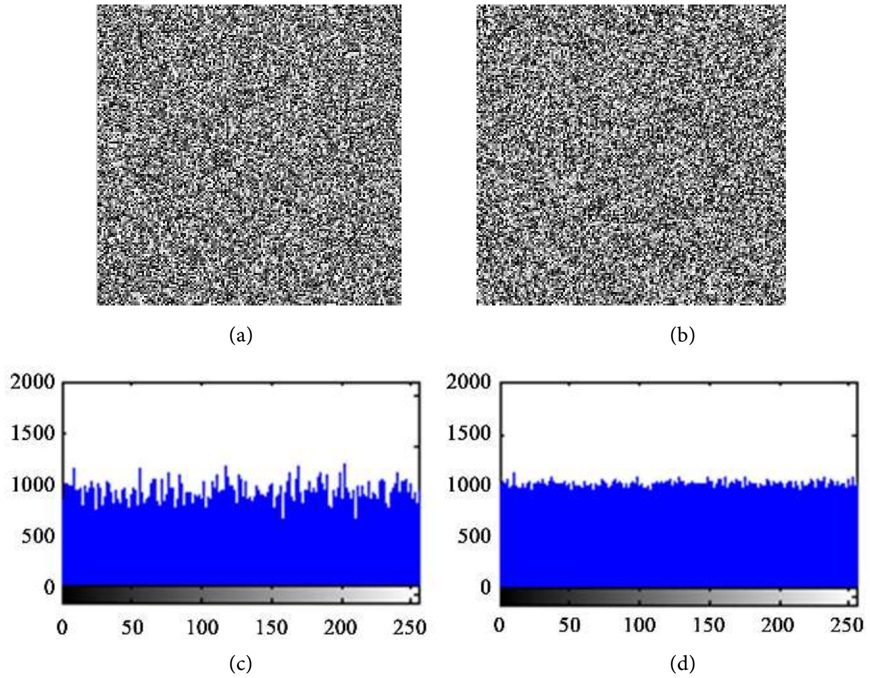


Figure 13. Performance comparison: (a) Cipher Lena image from Cryptosystem-1; (b) Cipher Lena image from Cryptosystem-2 (c) Histogram of the cipher Lena image from Cryptosystem-1; (d) Histogram of the cipher Lena image from Cryptosystem-2.

Entropy values and correlation coefficients between plain and cipher images are listed in Table 9.

Visual and numerical results show that the positive contribution and validity of the ILM in the proposed cryptosystem.

Table 8. Differential analysis of the proposed scheme.

Test images	Average confusion & diffusion time (sec)	Decryption time (sec)	Encryption rate (Mbps)	Decryption rate (Mbps)
128 × 128	0.0211	0.0238	6.21	5.50
256 × 256	0.0842	0.0947	6.22	5.53
512 × 512	0.3368	0.3804	6.22	5.51
1024 × 1024	1.3190	1.4869	6.35	5.64

Table 9. Entropy and correlation coefficients analysis.

	Cryptosystem-1	Cryptosystem-2
Entropy	7.987539	7.999285
Correlation Coefficient	0.01039	−0.00141

6. Conclusion

An efficient gray image cryptosystem based on chaos is proposed in this paper. The entire range of the control parameter of the improved map can be used to build the key space due to the having unlimited value of control parameter. A small change in the plain image or any parameters of the cryptosystem will provide totally different keys even with the same encryption key is used. Both confusion and diffusion processes are iterated with different keys in order to get higher encryption strength of the cryptosystem. Security and performance analysis is performed numerically and visually. Both theoretical and simulation results are satisfactory and show that the proposed cryptosystem is highly secure thanks to its large key space, high sensitivity to the encryption keys and plain images. The implementation of the proposed cryptosystem using a digital hardware is possible direction for our future work.

References

[1] Liu, Q., Li, P.-Y., Zhang, M.-C., Sui, Y.-X. and Yang, H.-J. (2015) A Novel Image Encryption Algorithm Based on Chaos Maps with Markov Properties. *Communications in Nonlinear Science and Numerical Simulation*, **20**, 506-515. https://doi.org/10.1016/j.cnsns.2014.06.005

[2] Chen, J.-X., Zhu, Z.-L., Fu, C., Yu, H. and Zhang, L.-B. (2015) A Fast Chaos-Based Image Encryption Scheme with a Dynamic State Variables Selection Mechanism. *Communications in Nonlinear Science and Numerical Simulation*, **20**, 846-860. https://doi.org/10.1016/j.cnsns.2014.06.032

[3] Wang, Y., Wong, K.-W., Liao, X. and Chen, G. (2011) A New Chaos-Based Fast Image Encryption Algorithm. *Applied Soft Computing*, **11**, 514-522. https://doi.org/10.1016/j.asoc.2009.12.011

[4] Zhu, H., Zhao, C. and Zhang, X. (2013) A Novel Image Encryption-Compression Scheme Using Hyper-Chaos and Chinese Remainder Theorem. *Signal Processing: Image Communication*, **28**, 670-680. https://doi.org/10.1016/j.image.2013.02.004

[5] Ye, R. (2011) A Novel Chaos-Based Image Encryption Scheme with an Efficient Permutation-Diffusion Mechanism. *Optics Communications*, **284**, 5290-5298. https://doi.org/10.1016/j.optcom.2011.07.070

[6] Zhu, H., Zhao, C., Zhang, X. and Yang, L. (2014) An Image Encryption Scheme Using Generalized Arnold Map and Affine Cipher. *Optik*, **125**, 6672-6677. https://doi.org/10.1016/j.ijleo.2014.06.149

[7] Som, S. and Sen, S. (2013) A Non-Adaptive Partial Encryption of Grayscale Images Based on Chaos. *Procedia Technology*, **10**, 663-671. https://doi.org/10.1016/j.protcy.2013.12.408

[8] Yoon, J.W. and Kim, H. (2010) An Image Encryption Scheme with a Pseudorandom Permutation Based on Chaotic Maps. *Communications in Nonlinear Science and Numerical Simulation*, **15**, 3998-4006. https://doi.org/10.1016/j.cnsns.2010.01.041

[9] Zhu, Z.-L., Zhang, W., Wong, K.-W. and Yu, H. (2011) A Chaos-Based Symmetric Image Encryption Scheme Using a Bit-Level Permutation. *Information Sciences*, **181**, 1171-1186. https://doi.org/10.1016/j.ins.2010.11.009

[10] Patidar, V., Pareek, N.K., Purohit, G. and Sud, K.K. (2011) A Robust and Secure Chaotic Standard Map Based Pseudorandom Permutation-Substitution Scheme for Image Encryption. *Optics Communications*, **284**, 4331-4339. https://doi.org/10.1016/j.optcom.2011.05.028

[11] Cruz-Hernandez, M.A.C., Abundiz-Perez, F., Lopez-Gutierez, R.M. and Acosta Del Campo, O.R. (2015) A RGB Image Encryption Algorithm Based on Total Plain Image Characteristics and Chaos. *Signal Processing*, **109**, 119-131. https://doi.org/10.1016/j.sigpro.2014.10.033

[12] Ye, R. and Guo, W. (2014) An Image Encryption Scheme Based on Chaotic Systems with Changeable Parameters. *International Journal of Computer Network and Information Security*, **4**, 37-45. https://doi.org/10.5815/ijcnis.2014.04.05

[13] Zhang, L.Y., Li, C., Wong, K.-W., Shu, S. and Chen, G. (2012) Cryptanalyzing a Chaos-Based Image Encryption Algorithm Using Alternate Structure. *The Journal of Systems and Software*, **85**, 2077-2085. https://doi.org/10.1016/j.jss.2012.04.002

[14] Jeng, F.-G., Huang, W.-L. and Chen, T.-H. (2015) Cryptanalysis and Improvement of Two Hyper-Chaos-Based Image Encryption Schemes. *Signal Processing*, **34**, 45-51. https://doi.org/10.1016/j.image.2015.03.003

[15] Tu, G., Liao, X. and Xiang, T. (2013) Cryptanalysis of a Color Image Encryption Algorithm Based on Chaos. *Optik*, **124**, 5411-5415. https://doi.org/10.1016/j.ijleo.2013.03.113

[16] Rhouma, R. and Belghith, S. (2008) Cryptanalysis of a New Image Encryption Algorithm Based on Hyper-Chaos. *Physics Letters A*, **372**, 5973-5978. https://doi.org/10.1016/j.physleta.2008.07.057

[17] Guo, W., Wang, X., He, D. and Cao, Y. (2009) Cryptanalysis on a Parallel Keyed Hash Function Based on Chaotic Maps. *Physics Letters A*, **373**, 3201-3206. https://doi.org/10.1016/j.physleta.2009.07.016

[18] Xue, H., Wang, S. and Meng, X. (2013) Study on One Modified Chaotic System Based on Logistic Map. *Research Journal of Applied Sciences, Engineering and Technology*, **5**, 898-904.

[19] Marton, K., Sucıu, A., Sacarea, C. and Cret, O. (2012) Generation and Testing of Random Numbers for Cryptographic Applications. *Proceedings of the Romanian Academy*, **13**, 368-377.

[20] Pande, A. and Zambreno, J. (2013) A Chaotic Encryption Scheme for Real-Time Embedded Systems: Design and Implementation. *Telecommunication Systems*, **52**, 551-561.

[21] Hathal, H.M., Abdulhussein, R.A. and Ibrahim, S.K. (2014) Lyapunov Exponent Testing for AWGN Generator System. *Communications & Network*, **6**, 201-208.

https://doi.org/10.4236/cn.2014.64022

[22] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., *et al.* (2010) A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22 rev1, 2-40.