American Journal of Signal Processing 2016, 6(3): 67-76
DOI: 10.5923/j.ajsp.20160603.01

# A Secure Chaos-based Image Cryptosystem with an Improved Sine Key Generator

**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

**Abstract** A secure cryptosystem for gray images based on chaos is proposed in this paper. The cryptosystem utilizes an improved sine map as a key generator and a diffusion function for changing pixel values of the plain image. Firstly, we have designed the improved map which has better performance than the standard sine map in terms of key space range, complexity and chaotic substantiality. Improved sine map yields continuous chaos that provides chaotic keys at output all the time. Hence, the map avoids discontinuous chaotic behavior which arises in standard sine map. Generated key is not only sensitive to the control parameter and initial condition of the improved map, but also strongly depend on the plain image characteristic, therefore proposed scheme can resist statistical attack, differential attack, known-plaintext attack and chosen-plaintext attack. To get higher encryption strength of the cryptosystem, the diffusion process is iterated with different keys in every iteration. Theoretical analysis and simulation results are satisfactory and confirm that the proposed image cryptosystem has high level of security and effectively encrypts and decrypts the gray images with different sizes as well.

**Keywords** Chaos, Cryptography, Image, Sine map

## 1. Introduction

With the widely use of computer networks, the protection of digital information against illegal usage has become a serious issue. Among the multimedia information, digital image plays an important role in people's daily life due to the increasing demand for real-time visual communication in social society. Thus, security of the information is becoming a major problem nowadays. Most of the available encryption methods such as DES, AES and IDEA are generally used for text data [1, 2]. However, compared to text, digital images have some intrinsic features, such as bulk data capacity, high redundancy and strong correlation of adjacent pixels [2-4]. Hence, traditional encryption algorithms cannot be used effectively for image data [5, 6] due to the requirement of much more processing power, bandwidth and longer time which causes low-level efficiency and significant latency during the encryption process [7].

Chaos in nonlinear dynamics systems has been attracted much attention of several different scientific areas especially in engineering science [8] such as secure communication and cryptography for the last decades. For instance, chaos is applied in communication systems in [9-21]; used for image cryptosystems in [1-5, 7, 8, 22-27]; for power systems in [28-33]. Chaotic systems exhibit similar features of sensitivity to initial conditions and control parameters, random-like behavior and ergodicity [22, 34, 35], which meet Shannon's requirements of confusion and diffusion in cryptography [23, 36]. Furthermore, chaotic cryptography techniques are mainly based on nonlinear complex maps that are simple and deterministic structure providing fast and secure data protection [37]. These special features 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 [1-5, 7, 25, 35] and most of them contain confusion and diffusion structures [4]. However, some of them are successfully broken [6, 24-27] due to their small key spaces and weakly secure encryption algorithms. For example, in [38], a novel image encryption based on hyper-chaos is proposed. The algorithm uses only one round diffusion process and the sum of image data. However, encryption keys in [38] have been revealed using known/chosen plaintext attacks by [39]. As a result, some image cryptosystems in this field have been demonstrated insecure and they have exposed some inner weaknesses. Among these weaknesses, the most serious one is that the key stream is completely depending on the secret key which means that identical key stream will be used to encrypt different plain images. This property allows the attacker to launch known-plaintext attack or chosen-plaintext attack for cryptanalysis. Hence, encryption key need to be calculated from not only the secret key but also plain image

* Corresponding author:
Hidayet.Ogras@batman.edu.tr (Hidayet Oğraş)
Published online at http://journal.sapub.org/ajsp

characteristic. Recent methods have been reported [24, 40] to avoid successful known/chosen plain image attacks by using plain image diffusion strategies. For instance, in [24] all plain image pixels are summed with chaotic sequences from Logistic map to increase the security of the proposed cryptosystem. In another study [40], key streams produced by Chen's chaotic system, are circularly shifted under the control of plain pixel, so the encryption key is also related the plain image which makes known/chosen plaintext attacks practically infeasible.

Chaos-based cryptosystems are either discrete or continuous chaotic systems. Discrete time chaotic systems are very simple and have low complexity, but having high efficiency comparing with the continuous time chaotic systems [41]. The advances in the research of chaotic maps applications performed a lot of achievements especially in the field of cryptology. Particularly, one-dimensional chaotic systems are very easy to implement in software and hardware but they have serious problems such as limited or discontinuous range of chaotic behaviors and non-uniform distribution of output sequences [24]. This situation may create serious drawbacks in a cryptosystem such as small key space, weak security and poor efficiency which threat the security of the whole cryptosystem [24, 42]. Small key space can cause brute-force cracking under cryptanalysis [43]. For a key generator, continuous chaotic output is essential if it is used in a cryptosystem. Because, such a feature of a chaotic system produces output series having same features. The rest of the paper is organized as follows: Section 2 gives a brief overview of the standard sine map (SSM) and introduces an improved sine map (ISM) with its statistical analysis. In Section 3, the proposed image cryptosystem is described in detail. Then, the security and performance of the proposed scheme are analyzed through key space analysis, key sensitivity analysis, histogram analysis, entropy analysis, correlation analysis and differential attack analysis in Section 4. Finally, the conclusions will be discussed in Section 5.

# 2. Designing a Key Generator

Sine map is one of the discrete chaotic systems having a following iterated equation

$$x_{n+1} = K.\sin(\pi.x_n) \tag{1}$$

where $K \in (0,1]$ and $x_n$ is in (0,1). For instance, if $K = 1$, then the map is in chaos state, which means that output sequence $x_n$ is aperiodic, non-convergent and very sensitive to initial value $x_0$. However, some isolated values such as $K = 0.941$ appear to show non-chaotic behavior and generates periodic sequences at output which are not random and unsuitable for encryption. In cryptographic manner, if the control parameter is used as a key, then this situation will reduce the key space size. Consequently, a new one-dimensional chaotic map should be designed and its all parameters make the system truly chaotic and provide larger key space.

### 2.1. Improved Sine Map

SSM has drawbacks of small key space, weak security, poor efficiency and low complexity. In this section, some modifications are applied on that system to overcome its weaknesses. We modify the SSM by adding a parameter to the map equation and get a new equation as

$$x_{n+1} = \lambda.\sin(\pi.x_n) + p \tag{2}$$

where $x_n$ values are restricted to the interval of $[\,1/\alpha, 1-(1/\alpha)\,]$ with $2 < \alpha < \infty$. In Eq. (2), the maximum point occurs at $x_n = 0.5$ and its value is $\lambda + p$, while the minimum occurs at $x_n = 1/\alpha$ and its value is $\lambda.\sin(\pi/\alpha) + p$. Thus,

$$\begin{aligned} 1 - \frac{1}{\alpha} &= \lambda + p \\ \frac{1}{\alpha} &= \lambda.\sin(\frac{\pi}{\alpha}) + p \end{aligned} \tag{3}$$

On solving the above equations, we get $\lambda = \dfrac{\alpha - 2}{\alpha\left[1 - \sin(\frac{\pi}{\alpha})\right]}$ and $p = \dfrac{\alpha - 1}{\alpha} + \dfrac{2 - \alpha}{\alpha\left[1 - \sin(\frac{\pi}{\alpha})\right]}$.

Substituting these values to the (2), we obtain the following final equation.

$$x_{n+1} = \frac{\alpha - 2}{\alpha\left[1 - \sin(\frac{\pi}{\alpha})\right]}.\left[\sin(\pi x_n) - 1\right] + \frac{\alpha - 1}{\alpha} \tag{4}$$

Adding one extra key parameter to the map provides more complexity, unpredictability and larger key space which leads to improve the security of the cryptosystem. Another advantage of the ISM equation is that the value of $\alpha$ determines the interval in which range $x_n$ distributes.

### 2.2. Lyapunov and Bifurcation Analyses

Lyapunov exponent states a checkable criterion for sensitivity to initial conditions of a nonlinear dynamical system [44]. It is defined for discrete time systems by the following equation.

$$\lambda = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln\left|f'(x_i)\right| \tag{5}$$

A positive Lyapunov exponent indicates that the dynamical system is chaotic [44]. Lyapunov spectrums for SSM and ISM are plotted in Fig. 1. Lyapunov coefficients for ISM are always positive and equal to or greater than the value of SSM. This shows that ISM has chaotic substantiality and better mixing property.

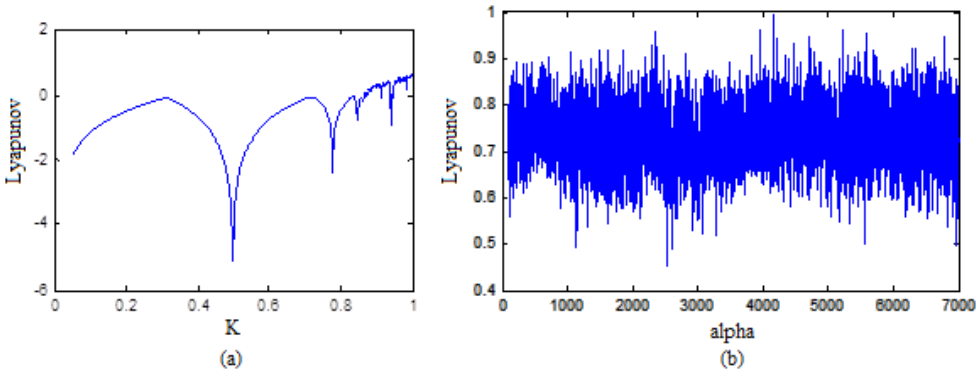


**Figure 1.** Lyapunov values (a) SSM (b) ISM

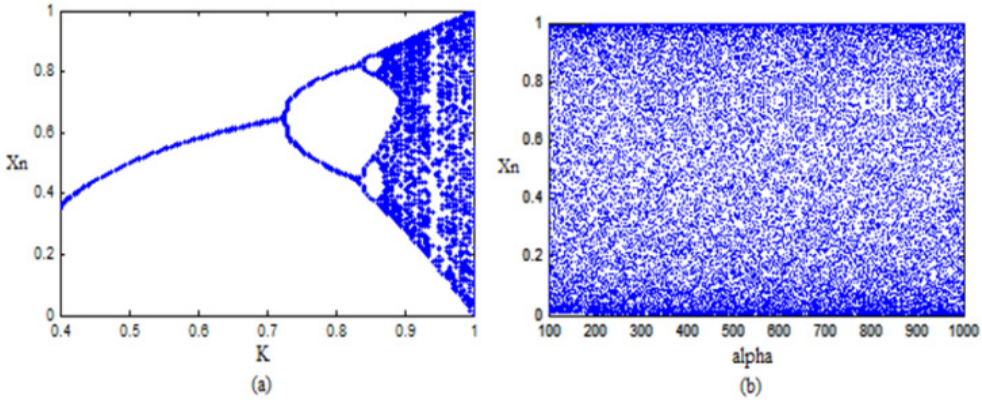


**Figure 2.** Bifurcation diagrams (a) SSM (b) ISM

The behavior of a dynamical system from a fixed point to a chaos with respect to control parameter is given by a bifurcation diagram. Fig. 2(a) and Fig. 2(b) show the bifurcation diagrams of the SSM and ISM, respectively. In Fig. 2(b), there are no free white spaces indicating no isolated values and the entire area is almost covered. More importantly, too many values of $\alpha$ can be used to generate different outputs which improves the key space of the cryptosystem.

### 2.3. Randomness Analysis

Randomness means the lack of predictability in a sequence of symbols [45]. We use NIST (National Institute of Standards and Technology) standard to evaluate the degree of randomness of the outputs. NIST consists of fifteen tests [46] 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. NIST uses bit streams for analysis. In order to get sequential bit streams, the following transformation is applied to the output of the ISM.

$$b_n = round(\mathrm{mod}(x_n * alpha, 1)) \quad (6)$$

Here, *round* function is used to get the nearest integer value and *mod* operation limits $x_n$ value to (0,1). Using Eq. (6), a bit value '1' or '0' is generated for each $x_n$. For instance, the system parameters of $\alpha = 500$ and $x_0 = 0.123$ are chosen to generate 1,000,000 bits to carry on NIST. The results are given in Table 1.

**Table 1.** NIST results

| Test name | p-value | Result |
|---|---|---|
| Frequency | 0.1159 | Success |
| Block frequency | 0.7441 | Success |
| Runs | 0.1597 | Success |
| Long runs of ones | 0.4036 | Success |
| Rank | 0.4344 | Success |
| Spectral DFT | 0.3833 | Success |
| Non-overlapping templates (m=9; B=000000001) | 0.9320 | Success |
| Overlapping templates (m=9) | 0.2518 | Success |
| Universal (L=7; Q=1280) | 0.8510 | Success |
| Linear complexity | 0.0513 | Success |
| Serial-1 (m=5) | 0.8750 | Success |
| Serial-2 (m=5) | 0.8389 | Success |
| Approximate entropy (m= 5) | 0.0204 | Success |
| Cumulative sums forward | 0.2254 | Success |
| Cumulative sums reverse | 0.0805 | Success |
| Random excursions (x= +1) | 0.0453 | Success |
| Random excursions variant (x= -1) | 0.4264 | Success |

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

## 3. Proposed Cryptosystem

The architecture of the proposed image cryptosystem is shown in Fig. 3.

In a gray image, each pixel is represented by 8-bit in decimal range [0, 255]. Key must be same format that a pixel has for the operation of encryption. However, the output of the ISM generator is a floating-point value. Thus, the following equation is used to obtain sufficient number of key for encryption.

$$key = \mathrm{mod}(round(x_n \times 10^9), 256) \tag{7}$$

The proposed cryptosystem uses a parameter which is strongly depend on the pixel values and size of the plain image, having a formula of (8). It provides different keys even with the same parameters of the cryptosystem.

$$pk = \left| \sum_{i=1}^{N \times N} (-1)^i \{normalized\_img\} \right| + \max(normalized\_img) + \frac{1}{\sqrt{N}}$$
$$normalized\_img = \frac{plain\_img}{256} \tag{8}$$

In Eq. (8), $N$ defines the total number of pixels which is related with the size of plain image. Here, *pk* parameter is not a secret key but it will be used to generate different keys by modifying the initial condition of the ISM as it is given in (9). Different initial values will create different keys hence different cipher image in every iteration. Table 2 shows some values of *pk* against various plain images.

$$X_0 = \mathrm{mod}(x_0 + pk, 1) \tag{9}$$

**Table 2.** Some *pk* values of different plain images

| Gray Images | Size | *pk* |
|---|---|---|
| Birds | (255x198) | 14.012262 |
| Bears | (300x213) | 3.214893 |
| Baboon | (512x512) | 63.216796 |

Here, $x_0$ is the first initial secret key which will be modified by *pk*.

If only one pixel is changed by a bit value in the plain image, then it will be a slight change in *pk* which supplies a small change in the initial condition of the ISM and results totally different keys for encryption. For example, when the value of one pixel in the birds image, $P(1,1) = 82$ is changed to $P(1,1) = 83$ (one bit different), with the same key parameters of $x_0$ and $\alpha$, then the some part of the obtained encryption keys are listed in Table 3.

**Table 3.** Different keys generated with a small difference of *pk* values

| Key-1 (pk =14.012262) | Key-2 (pk=14.008356) |
|---|---|
| 117 | 55 |
| 210 | 37 |
| 238 | 152 |
| 29 | 190 |
| 244 | 165 |
| 64 | 98 |
| 187 | 212 |

As a result, a very small change in any plain image causes completely different encryption keys hence a significant change in the cipher image. So, the proposed structure in the algorithm will resist differential attack efficiently. In the cryptosystem, the following mixing operation as a diffusion function is used to change the pixel values of the plain image sequentially,

$$c(i) = k(i) \oplus \left\{ p(i) + k(i)^2 \right\} \bmod 256 \tag{10}$$

where $p(i)$, $c(i)$ and $k(i)$ represent current plain pixel, output cipher pixel and secret key, respectively. Modular operation is used to limit the cipher data to the range of [0, 255]. Such a diffusion function is very efficient because simple modular arithmetic and logical operations can be performed in high speed. To increase the security of the cryptosystem, encryption process is iterated several times with different keys. The proposed scheme has a symmetric algorithm which means that identical key is used for decryption. The decryption algorithm is the reverse encryption and defined by the following equation.

$$p(i) = \left\{ (k(i) \oplus c(i)) - k(i)^2 + 256^2 \right\} \bmod 256 \tag{11}$$

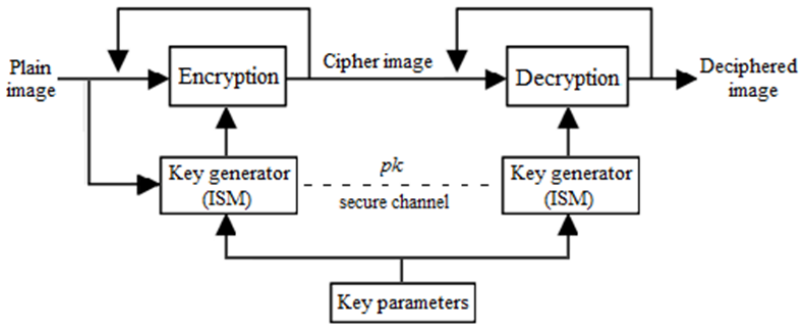


**Figure 3.** The architecture of the proposed cryptosystem

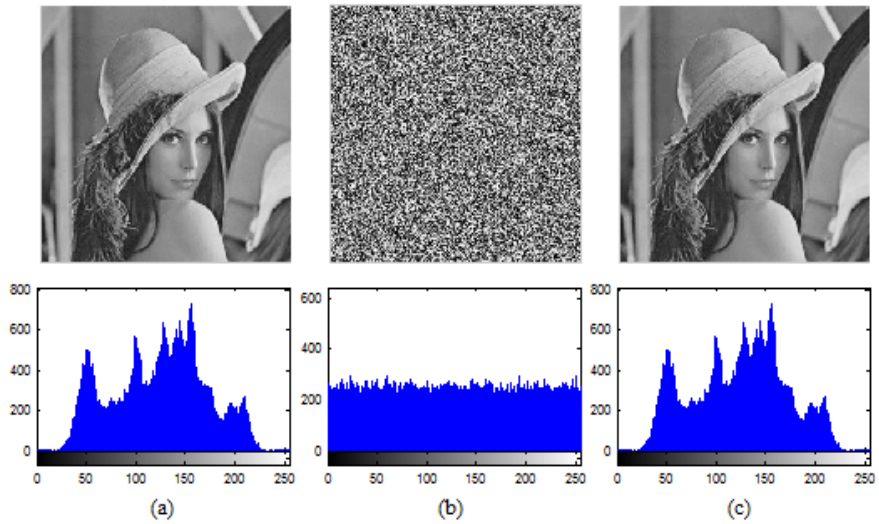


**Figure 4.** Images with histograms (a) Plain image (b) Cipher image (c) Decrypted image

For instance, Lena image is encrypted by using the proposed scheme with the key parameters of $\alpha = 500$, $x_0 = 0.123456789$ and $n = 4$. The result is shown in Fig. 4.

# 4. Security and Performance Analysis

## 4.1. Key Space Analysis

The 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 $2^{100}$ [5] to make brute-force attack infeasible. In our encryption scheme, key parameters are: $x_0$, $\alpha$ and $n$. According to the IEEE floating-point standard [2], the computational precision of the 64-bit double precision number is about $10^{15}$. In our cryptosystem, $x_0$ and $\alpha$ keys are floating point and $n$ is 8-bit key. Hence, the total number of possible secret key is approximately,

$$Key = (10^{15\times 2} \times 2^8) \approx 2^{108} \tag{12}$$

which is sufficient to resist brute-force attack.

## 4.2. Key Sensitivity Analysis

Key sensitivity can be observed in two aspects: (i) if slightly different keys are applied to encrypt the identical 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 image of Lena is encrypted with a randomly chosen Key-1 as $\alpha = 500$, $x_0 = 0.123456789$ and $n = 4$. Then a slight change is applied to the one of the parameters with others remain same, then repeats the encryption. Key-2 is $\alpha = 499.999999999$, $x_0 = 0.123456789$, $n = 4$; Key-3 is $\alpha = 500$, $x_0 = 0.123456788$, $n = 4$ and Key-4 is $\alpha = 500$, $x_0 = 0.123456789$, $n = 3$. Then we have computed correlation coefficients for the ciphered images and the results have been given in Table 4.

**Table 4.** Key sensitivity Analysis-1 for cipher Lena

| Key | Correlation coefficients between cipher images |
|---|---|
| Key-1 vs Key-2 | 0.00129 |
| Key-1 vs Key-3 | -0.00244 |
| Key-1 vs Key-4 | 0.00083 |

In Table 4, the negative correlation means that for two cipher images, an increase in one of them is associated with a decrease in the other. All the correlation coefficients are very close to zero indicating that despite being a very small difference at all encryption keys, corresponding cipher images are highly different between each other. For the second key sensitivity analysis, another test plain image 'Baboon' is encrypted using Key-1. The decryption will then proceed with three slightly different keys of Key-2 to Key-4. Now, correlation coefficients between the plain and decrypted images are calculated. The results are given in Table 5.

**Table 5.** Key sensitivity Analysis-2 for Baboon image

| Key | Correlation coefficients between plain and cipher images |
|---|---|
| Key-1 vs Key-2 | -0.00162 |
| Key-1 vs Key-3 | 0.00096 |
| Key-1 vs Key-4 | -0.00308 |

It is clear that if a slightly different key is used in decryption process, then the cipher image could not be decrypted correctly. We conclude that the proposed encryption and decryption schemes are quite sensitive to all secret keys.

### 4.3. Histogram Analysis

In image processing, histogram is used to display the number of pixels at each different intensity value in an image. Equal probability of each pixel value creates a uniform histogram which is more robust against statistical attacks [3]. 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 (Mountain, Liberty Statue and Cat) with different sizes and corresponding cipher images are shown in Fig. 5 and Fig. 6, respectively.

The histogram results show that cipher image is significantly different from that of the plain image and uniformly distributed over the all possible intensity values.

### 4.4. Entropy Analysis

Entropy is a measure of uncertainty associated with a random message [47] and determines unpredictability of the message. If $H(X)$ represents the entropy of an information source $X=(x_0,x_1,...,x_{N-1})$ with a length of $N$, then the entropy will be:

$$H(X)=-\sum_{i=0}^{N-1} p(x_i).\log_2 p(x_i) \tag{13}$$

where $p(x_i)$ the probability of symbol $x_i$ and the entropy is expressed in bits. If a truly random source emitting $2^8$ symbols as $S=\{s_1,s_2,...,s_{256}\}$ with equal probability, then, the entropy will be calculated to 8. 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 [3]. Maximum entropy is achieved in the case of a uniform probability distribution. Ten gray test images (Cameraman, Lena, Peppers, Baboon, Barbara, Boat, Bears, Landscape, Liberty statue and Mountain) are encrypted using the proposed cryptosystem with Key-1. Table 6 shows the entropy results and comparison with other existing algorithms. Entropy values of the proposed scheme are greater than the values obtained by [43] and [48].

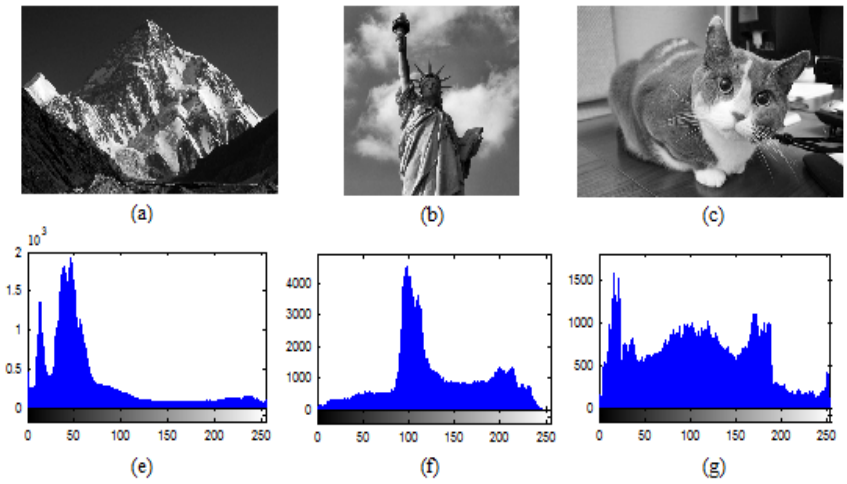


**Figure 5.** Histogram of the plain images (a) mountain (1203 × 799) (b) liberty statue (512 × 512) (c) cat (505 × 330)

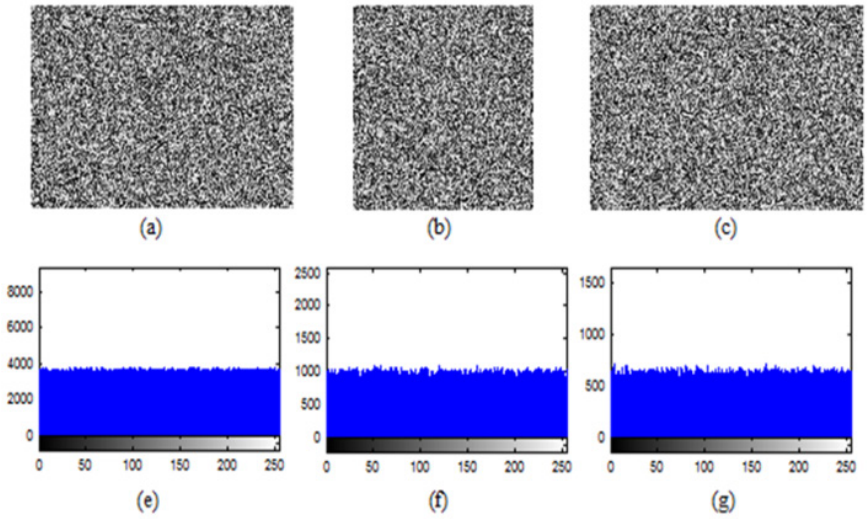


**Figure 6.** Histogram of the corresponding cipher images (a) mountain (b) liberty statue (c) cat

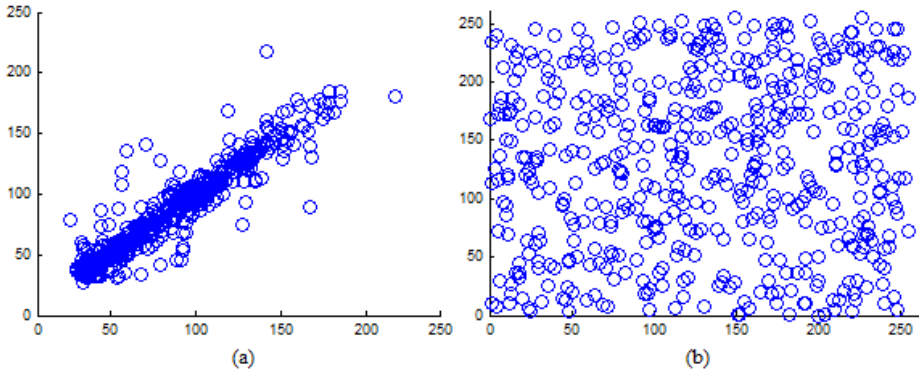


**Figure 7.** Correlation distribution of adjacent pixels (a) plain Lena image (b) cipher Lena image

**Table 6.** Entropy Results

| Test images | Entropy values | | | |
|---|---|---|---|---|
| | Plain image | Cipher image | Ref.[43] | Ref.[48] (Average) |
| Cameraman | 7.10514 | 7.99717 | 7.9834 | - |
| Lena | 7.46571 | 7.99753 | 7.9832 | 7.9862 |
| Peppers | 7.57461 | 7.99766 | 7.9977 | 7.9946 |
| Baboon | 7.18316 | 7.99945 | 7.9979 | 7.9976 |
| Barbara | 7.44390 | 7.99942 | - | 7.9972 |
| Boat | 7.21544 | 7.99938 | 7.9973 | - |
| Bears | 7.11658 | 7.99721 | - | - |
| Landscape | 7.35328 | 7.99981 | - | - |
| Liberty statue | 7.49462 | 7.99916 | - | - |
| Mountain | 7.22035 | 7.99983 | - | - |

It is obvious that the entropies of the cipher images are very close to ideal value, which means that the diffusion process in encryption produces high unpredictability at output and the proposed algorithm is secure against entropy attacks.

### 4.5. Correlation Analysis

A meaningful image has a property of strong correlation between adjacent pixels since its values are very 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 equation is used

$$cc = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x}).(y_i - \bar{y})}{\sqrt{(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2).(\frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2)}} \tag{14}$$

where $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$. In (14), $N$ shows the total number of pairs of diagonally adjacent pixels. Five test images are used in the proposed cryptosystem to determine the correlation coefficients of adjacent pixels for diagonally. The result of the correlation coefficients and their corresponding cipher images produced by Key-1 are given in Table 7. From Table 7, compared with the results in [43], our scheme shows superior correlation performance. It is also clear that the proposed scheme significantly reduces the correlation between adjacent pixels of the plain images.

**Table 7.** Correlation coefficients diagonally

| Test images | Correlation coefficients | | |
|---|---|---|---|
| | Plain image | Cipher image | Ref. [43] |
| Lena | 0.9238 | 0.0026 | 0.0062 |
| Cameraman | 0.8923 | -0.0043 | 0.0062 |
| Peppers | 0.9351 | 0.0055 | 0.0062 |
| Boat | 0.8644 | 0.0039 | -0.0015 |
| Baboon | 0.9573 | 0.0012 | 0.0056 |

Fig. 7(a) shows the diagonal correlation of the Lena image having a linear distribution, where the value of its adjacent pixel has a high correlation. On the contrary, pixel 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 Fig. 7(b). We only give the visual result of the Lena image but similar results have been obtained for other test images.

### 4.6. Differential Attack Analysis

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 analysis methods, NPCR (number of pixels change rate) and UACI (unified average changing intensity) are used to test the effect of only one-pixel change in the plain image over the corresponding cipher image. They are defined in (15)-(17).

$$NPCR = \frac{1}{W \times H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)\right] \times 100\% \tag{15}$$

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

$$D(i,j) = \begin{cases} 0, & if \ C_1(i,j) = C_2(i,j) \\ 1, & if \ C_1(i,j) \neq C_2(i,j) \end{cases} \tag{16}$$

and

$$UACI = \frac{1}{W \times H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (17)$$

Here, $W$ and $H$ are the width and height of the cipher image and $C_1, C_2$ are the two cipher images corresponding to two plain images with only one pixel difference. NPCR measures how many pixels are different between $C_1$ and $C_2$ using same encryption key. UACI is used to measure the average intensity of differences between two images. NPCR and UACI values [25] for two random images, which are an expected estimates for an ideal image cryptosystem should be 99.60% and 33.46% respectively. Seven test images are randomly chosen to evaluate the differential attack analysis of the proposed cryptosystem. First, all the test images are encrypted with Key-1, one by one. Then, the pixel value in the middle of the each test image is incremented by one. Afterwards, these images with one pixel difference (just one bit) are encrypted with same Key-1 and results the corresponding cipher test images. For instance, Lena test image $(512 \times 512)$ is encrypted to $C_1$ by using Key-1. Then, the value of the pixel in the middle of the Lena image, $P(256,256) = 89$ is changed to $90$ and the same encryption is performed and results $C_2$. The results of the NPCR and UACI analysis for all test images are shown in Table 8. We also present a performance comparison of [37] and [48] with our differential results in Table 8.

**Table 8.** Differential analysis of the proposed scheme

| | Proposed scheme | Ref. [37] | Ref. [48] |
|---|---|---|---|
| Images | NPCR UACI | NPCR UACI | NPCR UACI |
| Lena | 99.21 33.43 | 99.6 28.6 | 99.60 33.51 |
| Baboon | 99.19 33.50 | 90.5 26.9 | 99.40 33.32 |
| Peppers | 99.26 33.41 | - | 99.33 33.15 |
| Barbara | 99.24 33.52 | - | 99.58 33.46 |
| Boat | 99.22 33.44 | - - | - - |
| Plane | 99.22 33.53 | 91.1 27.8 | - - |
| Man | 99.28 33.55 | 90.9 25.2 | - - |

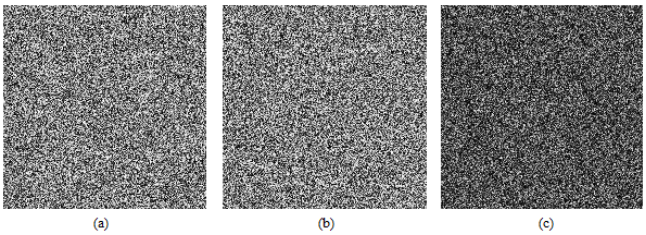


**Figure 8.** Differential analysis (a) cipher image of original Lena (b) cipher image of Lena with one pixel difference (c) differential image between (a) and (b)

From Table 8, our results are close to the [48], but they are better than [37]. It is obvious that our proposed scheme is stable for different plain images according to the differential analysis. Both NPCR and UACI values are very close to their ideal values so the proposed algorithm is highly sensitive at plain image and has a good ability against differential attacks. Fig. 8 shows the corresponding cipher Lena images, $C_1$ and $C_2$ with their difference image.

## 5. Conclusions

An efficient image cryptosystem based on chaos is proposed in this paper. Encryption key is related with plain image characteristics that is a tiny change in the image will provide totally different key elements even the same secret key is used in the cryptosystem. Encryption process is iterated with different keys in order to get higher encryption strength. Security and performance analysis of the proposed scheme are performed numerically and visually. Both theoretical and simulation results are satisfactory and show that the proposed scheme is highly secure thanks to its large key space, high sensitivity to the cipher keys and plain images. The implementation of the proposed algorithm using a digital hardware is possible direction for our future work.

## REFERENCES

[1] L. Quan, L. Pei-Yue, Z. Ming-chao, S. Yong-xin, Y. Huai-jiang, "A novel image encryption algorithm based on chaos maps with Markov properties," Communications in Nonlinear Science and Numerical Simulation, vol. 20, pp. 506-515, 2015.

[2] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, L.-B. Zhang, "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism," Communications in Nonlinear Science Numerical Simulation, vol. 20, pp. 846-860, 2015.

[3] H. Zhu, C. Zhao, X. Zhang, "A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem," Signal Process: Image Communication, vol. 28, pp. 670-680, 2013.

[4] Y. Wang, K.-W. Wong, X. Liao, G. Chen, "A new chaos-based fast image encryption algorithm," Applied Soft Computing, vol. 11, pp. 514-522, 2011.

[5] H. Zhu, C. Zhao, X. Zhang, L. Yang, "An image encryption scheme using generalized Arnold map and affine cipher," Optik, vol. 125, pp. 6672-6677, 2014.

[6] L. Y. Zhang, C. Li, K.-W. Wong, S. Shu, G. Chen "Cryptanalyzing a chaos-based image encryption algorithm using alternate structure," Journal of Systems and Software, vol. 85, pp. 2077-2085, 2012.

[7] S. Som, S. Sen, "A Non-adaptive partial encryption of grayscale images based on chaos," Procedia Technology, vol. 10, pp. 663-671, 2013.

[8] M. Türk, H. Oğraş, "Recognition of multi-scroll chaotic attractors using wavelet-based neural network and performance comparison of wavelet families," Expert Systems with Applications, vol. 37, pp. 8667-8672, 2010.

[9] J.-H. Lee, H.-G. Ryu, "High security wireless CDSK-based chaos communication with new chaos map," Military communications conference IEEE, MILCOM, pp. 786-790, 2013.

[10] S.-W. Yoon, J.-H. Lee, H.-G. Ryu, "Chaos communication system using MIMO technique," Advanced communication technology conference ICACT, pp. 579-583, 2014.

[11] N. Jiang, et al. "Chaos synchronization and communication in multiple time-delayed coupling semiconductor lasers driven by a third laser," IEEE Journal of Selected Topics in Quantum Electronics, vol. 17, pp. 1220-1227, 2011.

[12] Z. Kang, J. Sun, L. Ma, Y. Qi, S. Jian, "Multimode synchronization of chaotic semiconductor ring laser and its potential in chaos communication," IEEE Journal of Quantum Electronics, vol. 50, pp. 148-157, 2014.

[13] J. Yang, Y. Chen, F. Zhu, "Associated observer-based synchronization for uncertain chaotic systems subject to channel noise and chaos-based secure communication," Neurocomputing, vol. 167, pp. 587-595, 2015.

[14] M. Eisencraft, et al. "Chaos-based communication systems in non-ideal channels," Communications in Nonlinear Science and Numerical Simulation, vol. 17, pp. 4707-4718, 2012.

[15] G. A. Abib, M. Eisencraft, "On the performance of a digital chaos-based communication system in noisy channels," Modelling, identification and control of nonlinear systems conference MICNON, vol. 48, no. 11, pp. 976-981, 2015.

[16] G. Kaddoum, M. Coulon, D. Roviras, P. Charge, "Theoretical performance for asynchronous multi-user chaos-based communication systems on fading channels," Signal Processing, vol. 90, pp. 2923-2933, 2010.

[17] J. Hu, J. Ma, J. Lin, "Chaos synchronization and communication of mutual coupling lasers ring based on incoherent injection," Optik, vol. 121, pp. 2227-2229, 2010.

[18] J. Yang, F. Zhu, "Synchronization for chaotic systems and chaos-based secure communications via both reduced-order and step-by-step sliding mode observers," Communications in Nonlinear Science and Numerical Simulation, vol. 18, pp. 926-937, 2013.

[19] X.-L. An, et al. "Design of a new multistage chaos synchronized system for secure communications and study on noise perturbation," Mathematical and Computer Modelling, vol. 54, pp. 7-18, 2011.

[20] A. A. Zaher, A. Abu-Rezq, "On the design of chaos-based secure communication systems," Communications in Nonlinear Science and Numerical Simulation, vol. 16, pp. 3721-3737, 2011.

[21] M. Türk, H. Oğraş, "Classification of chaos-based digital modulation techniques using wavelet neural networks and performance comparison of wavelet families," Expert Systems with Applications, vol. 38, pp. 2557-2565, 2011.

[22] Z.-L. Zhu, W. Zhang, K.-W. Wong, H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," Information Sciences, vol. 181, pp. 1171-1186, 2011.

[23] V. Patidar, N. K. Pareek, G. Purohit, K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," Optics Communications, vol. 284, pp. 4331-4339, 2011.

[24] M. A. Murillo-Escobar, C. Cruz-Hernandez, F. Abundiz-Perez, R. M. Lopez-Gutierez, O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," Signal Processing, vol. 109, pp. 119-131, 2015.

[25] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," Optics Communications, vol. 284, pp. 5290-5298, 2011.

[26] R. Ye, W. Guo, "An image encryption scheme based on chaotic systems with changeable parameters," I. J. Computer network and Information Security, vol. 4, pp. 37-45, 2014.

[27] A. N. K Telem, C. M. Segning, G. Kenne, H. B. Fotsin, "A simple and robust gray image encryption scheme using chaotic Logistic map and artificial neural network," Advanced in Multimedia, vol. 2014, 13 pages, 2014.

[28] W. Yibei, L. Man, X. Yanting, C. Hougui, "Research on chaos phenomena in power system," Power Engineering and Automation Conference, vol. 2, pp. 453-456, 2011.

[29] I. M. Ginarsa, A. Soeprijanto, M. H. Purnomo, "Controlling chaos and voltage collapse using an ANFIS-based composite controller-static var compensator in power systems," International Journal of Electrical Power & Energy Systems, vol. 46, pp. 79-88, 2013.

[30] H.-T. Yau, M.-H. Wang, T.-Y. Wang, G. Chen, "Signal clustering of power disturbance by using chaos synchronization," International Journal of Electrical Power & Energy Systems, vol. 64, pp. 112-120, 2015.

[31] M. Ghasemi, S. Ghavidel, J. Aghaei, M. Gitizadeh, H. Falah,, "Application of chaos-based chaotic invasive weed optimization techniques for environmental OPF problems in the power systems," Chaos, Solitons & Fractals, vol. 69, pp. 271-284, 2014.

[32] Q. Chen, X. Ren, J. Na, "Robust finite-time chaos synchronization of uncertain permanent magnet synchronous motors," ISA Transactions, vol. 58, pp. 262-269, 2015.

[33] X. Zhou, J. Li, Y. Ma, "Chaos phenomena in DC-DC converter and chaos control," Procedia Engineering, vol. 29, pp. 470-473, 2012.

[34] E. Avaroğlu, İ. Koyuncu, A. B. Özer, M. Türk, "Hybrid pseudo-random generator for cryptographic systems," Nonlinear Dynamics, vol. 82, pp. 239-248, 2015.

[35] J. W. Yoon, H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 15, pp. 3998-4006, 2010.

[36] E. Avaroğlu, T. Tuncer, A. B. Özer, B. Ergen, M. Türk, "A novel chaos-based post-processing for TRNG," Nonlinear Dynamics, vol. 81, pp. 189-199, 2015.

[37] F. Elgendy, et al. "Chaos-based model for encryption and decryption of digital images," Multimedia Tools and Applications, vol. 75, pp. 11529-11553, 2016.

[38] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," Multimedia Tools and Applications, vol.

71, pp. 1469-1497, 2014.

[39] Y. Zhang, D. Xiao, W. Wen, M. Li, "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process," Nonlinear Dynamics, vol. 76, pp. 1645-1650, 2014.

[40] C. Fu, S. Hou, W. Zhou, W.-Q. Liu, D.-L. Wang, "A Chaos-based image encryption scheme with a plaintext related diffusion," International Conference on Information, Communications and Signal Processing, pp. 1-5, 2013.

[41] H. Xue, S. Wang, X. Meng, "Study on one modified chaotic system based on Logistic map," Research Journal of Applied Sciences, Engineering and Technology, vol. 5, pp. 898-904, 2013.

[42] A. Pande, J. Zambreno, "A chaotic encryption scheme for real-time embedded systems: design and implementation," Telecommunication systems, vol. 52, pp. 551-561, 2013.

[43] J. Ahmad, S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," Multimedia Tools and Applications, vol. 75, pp. 13951-13976, 2016.

[44] H. M. Hathal, R. A. Abdulhussein, S. K. Ibrahim, "Lyapunov exponent testing for AWGN Generator system," Communications and Network, vol. 6, pp. 201-208, 2014.

[45] K. Marton, A. Sucıu, C. Sacarea, O. Cret, "Generation and testing of random numbers for cryptographic applications," Proceedings of the Romanian Academy, vol. 13, pp. 368-377, 2012.

[46] A. Rukhin, et al. "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Publication 800-22 rev1, 2010.

[47] H. Liu, A. Kadir, Y. Niu, "Chaos-based color image block encryption scheme using S-box," International Journal of Electronics and Communications, vol. 68, pp. 676-686, 2014.

[48] X.-J. Tong, M. Zhang, Z. Wang, J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," Nonlinear Dynamics, vol. 84, pp. 2333-2356, 2016.