Research Article GU J Sci 35(2): 542-556 (2022) DOI: 10.35378/gujs.872818

Gazi University

Journal of Science

http://dergipark.gov.tr/gujs

An Effective Image Encryption Algorithm Using Bit Reversal Permutation and a New Chaotic Map

Hidayet OGRAS[1], Mehmet Rida TUR[2,*]

[1] Batman University, Department of Electronics Communication Technology,72000, Batman, Turkey
[2] Batman University, Department of Department of Electrical and Energy Technology,72000, Batman, Turkey

Highlights

- To create a new chaotic map.
- Confidential image in power systems.
- This is a satisfactory security.

Article Info

Received: 01 Feb 2021
Accepted: 22 May 2021

Keywords

Chaotic maps
Image encryption
Logistic map
Sine map
Wind map

Abstract

In this paper, a different approach to create a new chaotic model and an effective image encryption structure using Bit reversal permutation are proposed. Compared to most frequently used and well known chaotic maps, such as Logistic map, Sine map or Tent map, a new chaotic system based on Logistic map with Sine map is designed and used as an encryption key generator in the proposed algorithm. The new map has increased initial value sensitivity according to the results of Lyapunov analysis and shown better randomness output according to the chaotic trajectory analysis. In cryptography, a good key should be a stochastic and supposed to be sufficiently random and uniformly distributed with equal probability for an effective encryption. The designed chaotic map provides these properties very well. Before the basic encryption process, the Bit reversal method makes all pixel positions of input image rearranged in order to reduce the strong relation of adjacent pixels for higher encryption strength, which will enable strategic information sharing for production planning when this method analyzes a wind energy map in power plants. Other experimental results confirm that the proposed image encryption scheme has sufficient security, an effective encryption capability and can be transferred between power systems, keeping energy planning secret strategically.

1. INTRODUCTION

Chaos is a confusion state of a complex system whose behavior appears to be random like noise and having great sensitivity to tiny changes in initial conditions and system parameters [1]. The characteristics of chaos are generally used in different scientific fields where a random and unpredictable output is required. The unpredictable behavior of chaotic systems can be used to yield random numbers. In this sense, applications of chaos have been used in many different scientific areas including communication, cryptography, steganography, big data analytics, fuzzy logic, etc. For example, chaos is used in secure communications systems in [2]; used for image encryption algorithms in [3]; for power control applications in [4]. Data security plays an extremely important role in real-time information communication in power systems, especially in the field of energy planning in power plants. Today, the confidentiality and security of information processed in the industrial field, especially in production-based planning, is extremely important for all states. Therefore, the security of digital information used and processed in this field becomes important. The first solution that comes to mind is to use data encryption algorithms to protect digital information confidentially. However, conventional encryption algorithms are not generally used for image information due to the much more processing power and longer time requirement that results low encryption efficiency. In this study, a different approach is presented for the confidentiality of data regarding energy planning, which is considered within power systems. In this sense, a chaos-based

*Corresponding author, e-mail: mrida.tur@batman.edu.tr

encryption structure for the security and protection of such important data is presented in this study and its applicability is supported by security analysis results.

Chaotic systems have two major features that open their use in data encryption in cryptography. One of them is that they exhibit random-like behavior, which makes encryption keys difficult to predict; the other one is highly sensitive to system parameters and initial condition, which provides sensitivity for both secret key and ciphered data. Such properties provide the security of the information to be encrypted and a robust cipher output against differential attacks. Besides, these features completely meet confusion and diffusion stages in cryptography which is also referred as Shannon's requirements in this field [5]. Encryption algorithms that utilize chaos are mainly based on nonlinear complex maps. The concept of map expressed here is a discrete form of iterated functions in mathematical representation. Chaotic maps are designed in a simple way and have deterministic structure that provides high uncertainty at output. The dynamics of chaotic maps highly depend on initial condition of the system and having unpredictable output that can be used to encrypt information through diffusion process. Although chaotic maps have easy implementation in software and hardware platforms and are also more efficient than analog chaotic systems, they have some drawbacks [6, 7]. For instance, Logistic map or Sine map are well-known chaotic systems but they have limited or discontinuous interval of unpredictable behaviors and demonstrate uneven distribution output against to its all control parameters. In other words, such maps generate orbits with uniform probability distribution under the limited number of control parameters [8]. In addition, they have a small Lyapunov value which means a notion of predictability and chaotically is low. These shortcomings negatively affect the system security where such maps are used, as well as the cryptographic usability of the yielded key from the maps. In order to get rid of this undesirable situation, a different and new chaotic system has been designed, which will be discussed in the following sections in this study. In the designed model, chaos dynamics will ensure that the whole system will be sensitive to key parameters and complex behaviors. Lyapunov value is an important parameter that shows the sensitivity of a dynamical system and larger Lyapunov value means more chaotic the map is, and better encryption key yielded. As a result, using chaotic system with a large Lyapunov value significantly contributes to the security of the algorithm in data encryption. The new chaotic system is designed to provide these properties well in this study.

In chaos-based encryption algorithms, improved chaotic maps are typically used as encryption key generators for presented algorithms. This is assumed to increase performance of the algorithm and whole system security of the proposed algorithm [9]. In this field, there are many studies using different approaches for improving chaotic maps in order get better chaotic properties [10]. Researchers studying in the field of image encryption believe that source image needs to be permutated before the basic encryption process and thereby creating much stronger encryption structure and better random output data [11]. In this study, an approach to the use of chaos in a very different field has been demonstrated and it is aimed to secure the image-based confidential information for energy planning of power plants through an encryption structure by using the concept of chaos. Firstly, a new chaotic map with a higher degree of chaos and more complex behavior has been designed for generating secret keys to be used for encryption of confidential image information. This design is expressed mathematically by defining the Sine map equation as a state variable in the Logistic map system. The new chaotic map, namely LOSIM is at a much better level than both the Logistic map and Sine map in terms of uncertainty and unpredictability according to the analysis results. Thus, the encryption keys obtained from the LOSIM are much better in terms of both cryptographic compatibility and generating random output. Furthermore, LOSIM has an extra system parameter in its mathematical equation that provides more complexity and larger key space which leads to improve the security of the encryption algorithm if its parameters are used as a key. The proposed encryption algorithm uses Bit reversal permutation method to scramble input image by bit-level processing and this permutated image is mixed with secret encryption keys through a diffusion function. The permutation process before the encryption will increase the encryption quality as well as the security of the whole system. The statistical and differential analyses performed in this study are provided in computer environment with MATLAB software. Some important analysis results are also compared with a similar study presented recently in this field. The rest of the paper includes five sections. Section 2 gives a brief about Logistic and Sine maps. Section 3 introduces design and analysis of the new chaotic model. In section 4, the proposed encryption algorithm is explained in detail and security analyzes of the proposed encryption algorithm are given in section 5 then conclusion is discussed in section 6.

2. CHAOTIC MAPS

2.1. Logistic Map

Logistic map is one of the well-known complex systems that exhibits an unexpected degree of complexity. It has an iterative equation mapping as its output at the end of the iteration onto the input of the next. Eventually, starting from an initial value generates a sequence of values from the map. The Logistic map is given in Equation (1)

$$x_{n+1} = r.x_n(1 - x_n)\,. \tag{1}$$

For an initial value, $x_0 \in (0,1)$ and a control parameter with $0 < r \leq 4$, the map generates a sequence of values, x_1, x_2, x_3 etc. If the control parameter is selected in the range of $r \in [3.57, 4]$, then the map behaves chaotically which means that the output of the system is not periodic, non-convergent and exhibits sensitive against the initial value. Figure 1 shows a sequence of values produced by Logistic map with $x_0 = 0.123$ and $r = 3.999$.

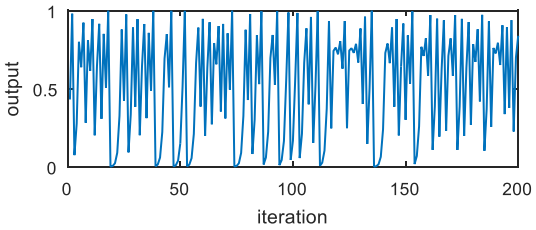


Figure 1. *Output of chaotic Logistic map*

2.2. Sine Map

Sine map is one-dimensional chaotic system like Logistic map. It is defined by the given Equation (2),

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

where the control parameter and output of the map satisfy $K \in (0,1]$ and $x_n \in (0,1)$, respectively. The map behaves chaotic under $K \in [0.87,1]$. Figure 2 shows the output of Sine map with $x_0 = 0.123$ and $K = 0.999$

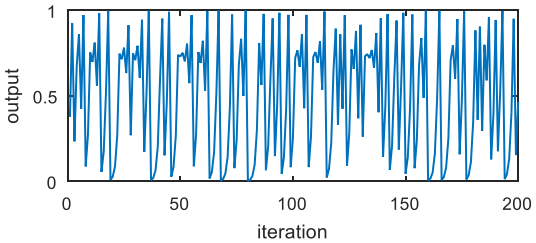


Figure 2. *Output of chaotic Sine map*

Following section describes a new chaotic map that is derived from Logistic map and Sine map, shortly LOSIM.

3. DESIGN AND ANALYSIS OF LOSIM

As mentioned earlier, both Logistic and Sine maps have some drawbacks of having easy behaviors and weak complexity which can result negative consequences for some chaos-based applications. LOSIM is designed by coupling Logistic and Sine maps, which can be defined as in Equation (3)

$$x_{n+1} = r.K\sin(\pi x_n).(1 - K\sin(\pi x_n)) . \tag{3}$$

By the help of this equation, Logistic map and Sine map can be effectively mixed that results greater complexity which produces more complex chaotic behavior and better randomness. To prove the excellence and superiority of LOSIM, chaotic performances of three maps: Logistic map, Sine map and LOSIM are compared in terms of chaotic trajectory state, Lyapunov value and entropy. For the performance comparison, system parameters of all chaotic maps are chosen as $r = 4$ and $K = 1$ with same initial condition.

3.1. Chaotic Trajectory

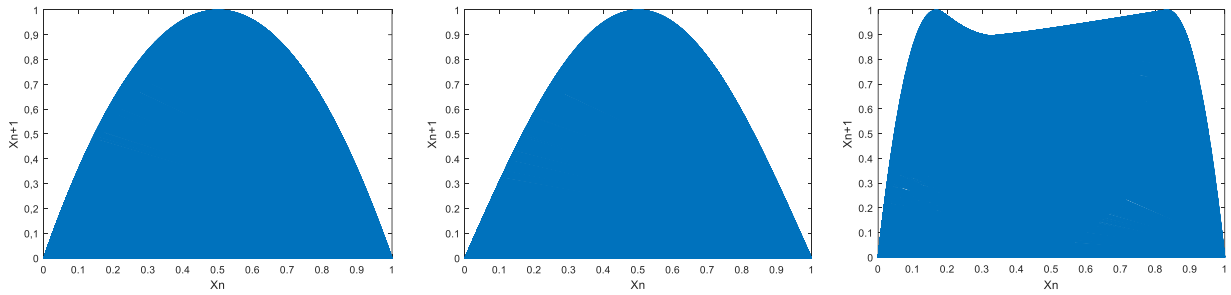
For a dynamical system, chaotic trajectory can be explained as a movement over time with a certain initial value. Since the chaotic systems demonstrate aperiodic and random behavior, the trajectory of these systems is never in the form of closed or repetitive curve. Thus, chaotic trajectory can be used to determine the degree of randomness for an output of any chaotic system [12]. A complex dynamical system shows better randomness if the trajectory of the system can cover a large area in phase space. Chaotic trajectories of the three chaotic maps are shown in Figure 3. According to the Figure 3 results, it is easily observed that the trajectory of LOSIM can occupy larger area than the other two maps. Therefore, LOSIM can generate much better output sequences in terms of randomness.

3.2. Lyapunov Analysis

Lyapunov exponent refers to a measure how close trajectories are diverging from each other. Thus, this value can be used as a measure of a system's predictability and sensitivity to changes in its initial condition. It is defined in Equation (4)

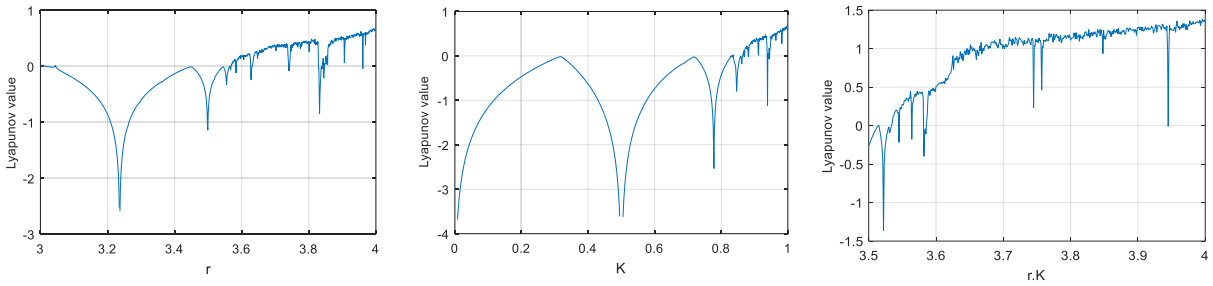
$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln\left| f'(x_i) \right| \quad . \tag{4}$$

A positive λ indicates that very close trajectories of a dynamical system change into completely different trajectories with increasing time. Thus, if Lyapunov value is positive, then the system is chaotic. Furthermore, greater Lyapunov value shows much more complicated motion in the system, hence better performance of the chaotic behavior [13]. Results of Lyapunov analyses for all chaotic maps are shown in Figure 4.



(A) (B) (C)

Figure 3. *Chaotic trajectory of (A) Logistic map (B) Sine map (C) LOSIM*



(A) (B) (C)

Figure 4. *Lyapunov analysis of (A) Logistic map (B) Sine map (C) LOSIM*

From the Lyapunov analysis, one can see that the largest values of both Logistic and Sine maps are less than 1, while the maximum Lyapunov value of LOSIM is greater than 1. Calculated maximum values of Logistic map, Sine map and LOSIM are 0.694, 0.698 and 1.383, respectively. It is concluded that LOSIM has better chaotic performance than the others.

3.3. Entropy Analysis

Entropy is a global measure of uncertainty related to a random system. Thus, the more uncertain random the system is, the more entropy it contains [14]. The entropy of a system can be calculated as:

$$H(X) = -\sum_{i=1}^{N} p(x_i).\log_2 p(x_i) \tag{5}$$

where $p(x_i)$ represents the probability of x_i. For a uniform bitstream with equal number of '0' and '1', the entropy will be 1. Zero entropy means that the system is completely certain. To perform the Entropy analysis, outputs of all chaotic maps are rounded to yield bitstream and iterated 10,000. The entropy results are listed in Table 1.

Table 1. *Entropy results*

Chaotic Map	Entropy
Logistic	0.999801
Sine	0.995516
LOSIM	0.999968

Great entropy also indicates a uniform distribution at output resulting more suitable encryption key from that system. From the Table 1 results, LOSIM has the highest entropy and thus it has a great degree of uncertainty.

4. IMAGE ENCRYPTION ALGORITHM

The proposed image encryption structure consists of two stages: Permutation and Substitution. Permutation is chosen as a first process and then confusion is performed to complete the encryption. In permutation stage, all pixel positions of the source image are rearranged without changing their values and creates permutated image. This process aims to reduce or completely break strong correlation of close pixels. Substitution is a mathematical process based arithmetic or logic operations in which the pixel values are changed sequentially by using encryption key through a cipher algorithm. The output of this stage is called cipher image. Figure 5 shows architecture of the proposed image encryption algorithm.

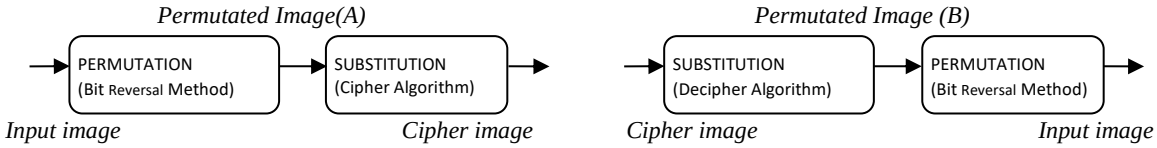


Figure 5. *Scheme of proposed algorithm (A) Encryption (B) Decryption*

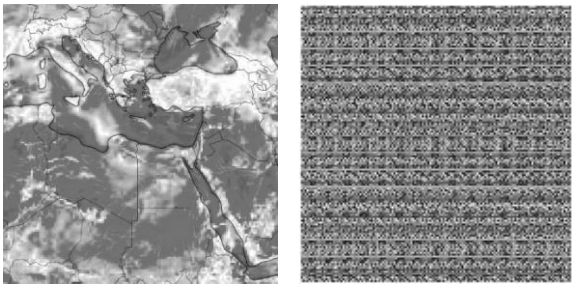
4.1. Bit Reversal Permutation

In this stage, Bit Reversal method is used to reposition for all pixels of the source image in such a way that all nearby pixels are away from each other. This will significantly reduce the strong correlation between neighboring pixels hence contributes much better cipher image at output. In applied mathematics, Bit reversal method is a permutation of *n* times for a sequence, where $n = 2^k$ is a power of two. This method focuses on an indexing of the elements in a sequence by the numbers from 0 to *n-1,* and then making the binary representation reverse for each these elements. Finally, each element is mapped to a new position according to this reversed value. For instance, Table 2 shows the numbers between 0 and 7, and also the bit reversed numbers with its index.

Table 2. *Application of Bit reversal method*

Index (*n*)	Bits (*k*)	Bit-reversed	Bit-reversed index
0	000	000	0
1	001	100	4
2	010	010	2
3	011	110	6
4	100	001	1
5	101	101	5
6	110	011	3
7	111	111	7

To get the original order on the elements, the same permutation must be performed twice. The bit reversal method is applied to the gray test image of "Wind.jpg" and the result is shown in Figure 6. The world wind map image used contains important content for wind energy-based production estimates. Thus, the coordination and production forecasts for energy planning in power systems will be more accurate and secure [15]. If the data transmitted by chaotic encryption is encoded and sent, it is more important. Basically, the selection of the wind map is to ensure that such images, which are strategically important in power prediction, are kept secret, which information is very important in ensuring supply security and energy quality in the competitive market [16].



(A) (B)

Figure 6. *Gray images of (A) Original 'Wind map' (B) Permutated 'Wind map'*

4.2. Encryption and Decryption Algorithms

For a typical image encryption process, pixel values of an input image are mixed with the secret encryption keys through a mathematical formula to obscure original pixel. Changing a pixel value with a secret key

value is the basic function of an encryption process. To do this, an algorithm that requires mathematical or logical process is needed. In this paper, the mathematical formula used for that purpose is given in Equation (6)

$$c(i) = k(i) \oplus \{ p(i) + k(i) + c(i-1) \} \bmod 256 . \tag{6}$$

Here, k(i), p(i), c(i) and c(i-1) denote secret encryption key, original pixel value, corresponding cipher pixel, and the previous cipher pixel value, respectively. The modular operation used here limits the cipher pixel value between 0 and 255. In a gray image, each pixel is 8-bit. Such an algorithm is extremely effective due to the current cipher output depends on the previous one, so a tiny change in the input image or encryption key will affect many pixel values in ciphered image and results a diffusion to all elements of ciphered image. This property of the algorithm completely increases the system security. For the proposed scheme, the initial cipher data is encoded as,

$$c(0) = round\left\{ 255^{x_0 + r + K} \right\} \bmod 256 \tag{7}$$

and its value depends on the secret parameters of LOSIM. If x_0, r and K are unknown, c(0) cannot be calculated. Hence, the ciphered image generated after encryption will be very sensitive to the system parameters.

In a gray image, each pixel has a decimal value between 0 and 255, which can be represented by 8-bits. Encryption key should be identical format with pixel value to operate the cipher algorithm. However, LOSIM generates output sequences with real floating-point value. Thus, with the help of Equation (8), suitable encryption key can be easily obtained from the output of LOSIM

$$k(i) = \left\{ round(x_i . 10^9) \right\} \bmod 256 . \tag{8}$$

Here, the output of LOSIM is multiplied by 10^9 first to make the precision up to 9 digits. Then, the '*round*' operation is used to obtain nearest integer value. The proposed encryption algorithm is symmetric that means decryption process requires identical key. Decryption is a process that works in the functional opposite of encryption and is defined in Equation (9)

$$p(i) = \{ (k(i) \oplus c(i)) - (k(i) + c(i-1)) \} \bmod 256 . \tag{9}$$

Permutation and substitution processes complete all the necessary steps in the proposed image encryption algorithm. Both processes have simple operations so the encryption and decryption time of the proposed cryptosystem will be reduced. Time consuming of encryption and decryption processes are analyzed in the speed performance of the proposed scheme. The architecture of the proposed algorithm is shown in Figure 7.

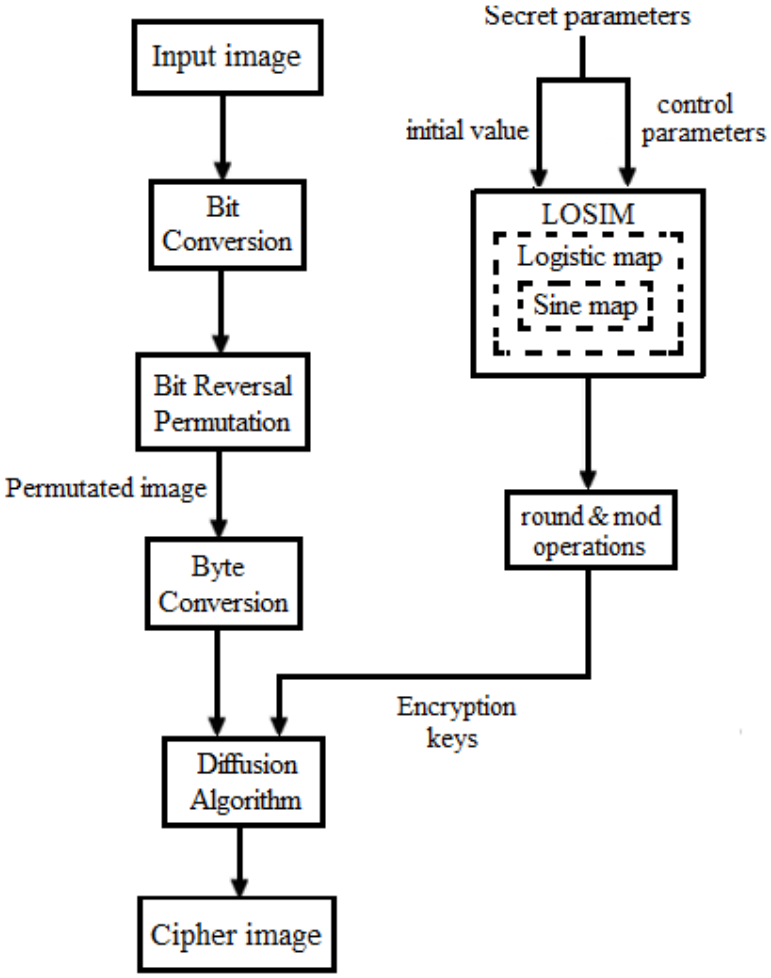


Figure 7. *Flowchart of the proposed encryption algorithm*

The work flow of the proposed encryption algorithm can be explained: firstly, the input image where each pixel value is 8-bit (Byte) must be converted to the suitable format for the Bit reversal method in order to be permutated. Then, rounding and mode operations are applied to the floating-point output of the LOSIM to obtain an encryption code of one-byte length for each pixel. Finally, the cipher image data is obtained where the original pixel value is changed by mixing it with the corresponding encryption code in diffusion stage. For example, 'Wind map' test image with 512x512 in size is encrypted using the proposed algorithm with the system parameters of LOSIM as $x_0 = 0.1234$; $r = 3.9998$ and $K = 0.9988$. The result is shown in Figure 8.

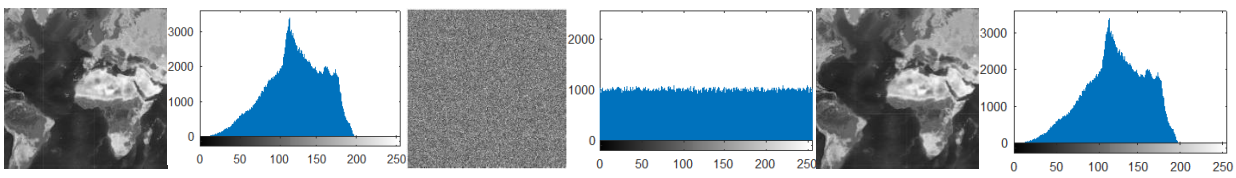


Figure 8. *Results of the proposed algorithm (A) Original 'Wind map" image (B) Histogram of (A) (C) Encrypted 'Wind map' image (D) Histogram of (C) (E) Decrypted image (F) Histogram of (E)*

In order to make a comparison with other studies presented in the similar field, other test images (Lena, Cameraman, Baboon, Airplane, Peppers and Landscape) frequently used in this field have been also applied to the prposed scheme. For instance, Lena, Airplane and Baboon gray images with size of 512 are encrypted by using the proposed encryption algorithm and the results are shown in Figure 9.

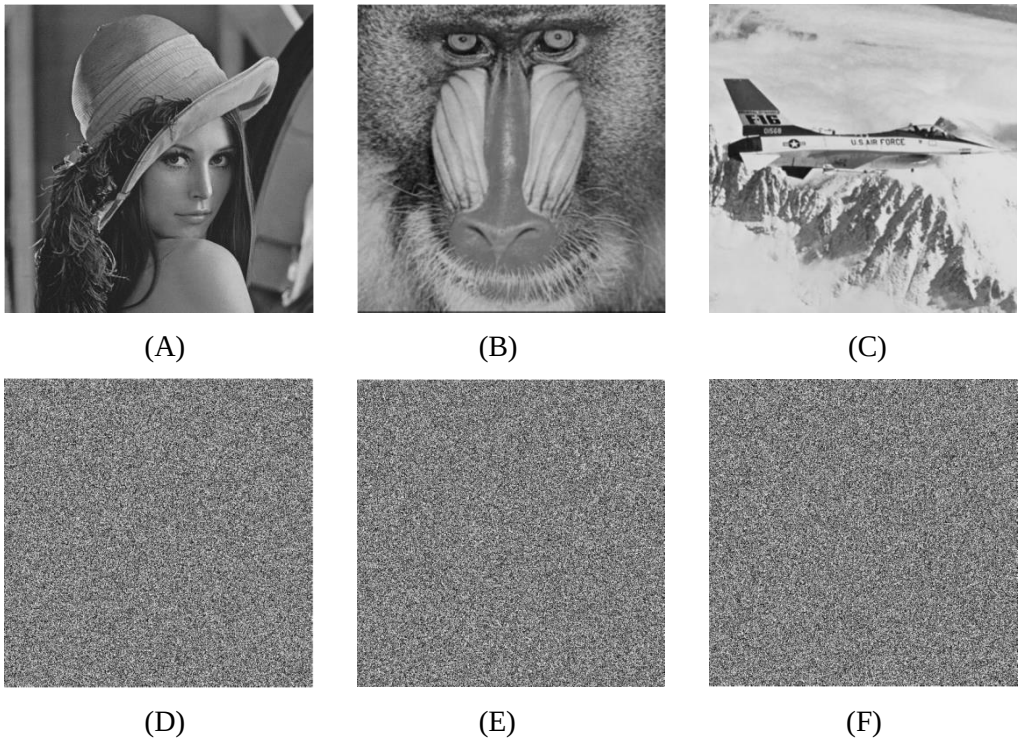


Figure 9. *Results of the encryption (A) 'Lena' image (B) 'Baboon' image (C) 'Airplane' image (D) Cipher 'Lena' image (E) Cipher 'Baboon' image (F) Cipher 'Airplane' image*

5. SECURITY ANALYZES

In order to evaluate the security level of a specified encryption structure, some important security analysis should be performed for that algorithm. This section describes some important security analyzes which are well known in the field of image encryption. In following section, security analysis evaluations for the proposed encryption structure are considered.

5.1. Key Size Analysis

In the field of cryptology, key size refers to the total number of different keys used in an encryption algorithm. For a secure cryptosystem, it should be larger than 2^{100} [17]. In this case, brute-force attacks become ineffective. Brute-force is a cryptographic attack that tries all possible combinations until the correct encryption key is found. In the proposed algorithm, there are three key parameters as x_0, r, K and each of them has a floating-point value which is a computer number format and usually occupies 64 bits in computer memory. The computational precision of 64-bit double format gives 53 bits [17]. Even the initial cipher value is ignored; the total number of key size is approximately,

$$key = 2^{3x53} = 2^{159} \tag{10}$$

which is enough for brute-force attacks.

5.2. Key Sensitivity Analysis

The very small change in the initial value or system parameter of any chaotic system will give completely different outputs by that system [18]. This feature of chaotic systems will provide excellent key sensitivity where these systems are used as key generators in cipher algorithms. In image encryption, key sensitivity

is a major criterion for security and needs to be examined. If slightly different keys are used to encrypt the same input image, then completely different ciphered images should be generated. For the analysis, four encryption keys as Key-1: $x_0 = 0.1234$, $r = 3.9998$, $K = 0.9988$; Key-2: $x_0 = 0.1235$, $r = 3.9998$, $K = 0.9988$; Key-3: $x_0 = 0.1234$, $r = 3.9999$, $K = 0.9988$; Key-4: $x_0 = 0.1234$, $r = 3.9998$, $K = 0.9987$ are used to encrypt the same 'Wind map' test image and resulting ciphered images as Cipher-1, Cipher-2, Cipher-3 and Cipher-4, respectively. Correlation coefficients between ciphered images are calculated and listed in Table 3.

Table 3*. Correlation coefficients between ciphered images*

Cipher Images	Difference at Key Parameters	Correlation Coefficients
Cipher-1 & Cipher-2	$\Delta x_0 = 0.0001$, $\Delta r = 0$, $\Delta K = 0$	0.00110
Cipher-1 & Cipher-3	$\Delta x_0 = 0$, $\Delta r = 0.0001$, $\Delta K = 0$	0.00032
Cipher-1 & Cipher-4	$\Delta x_0 = 0$, $\Delta r = 0$, $\Delta K = -0.0001$	-0.00382

Correlation coefficients of encryption keys by generating with slightly different system parameters are also calculated and given in Table 4.

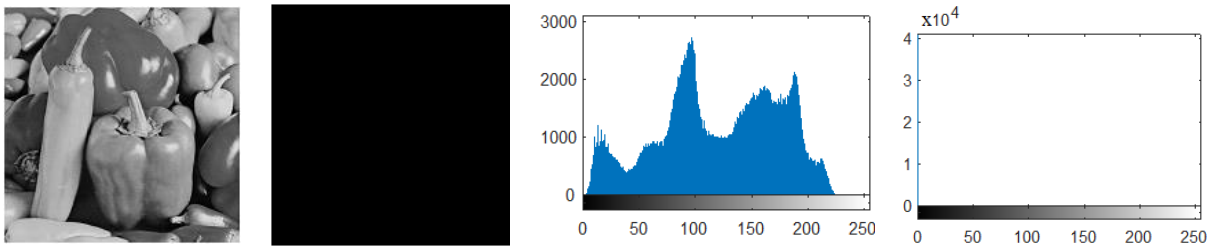
Table 4. *Correlation coefficients between encryption keys*

Encryption Keys	Difference at Key Parameters	Correlation Coefficients
Key-1 & Key-2	$\Delta x_0 = 0.0001$, $\Delta r = 0$, $\Delta K = 0$	0.00041
Key-1 & Key-3	$\Delta x_0 = 0$, $\Delta r = 0.0001$, $\Delta K = 0$	-0.00429
Key-1 & Key-4	$\Delta x_0 = 0$, $\Delta r = 0$, $\Delta K = -0.0001$	0.000162

Negative correlation coefficient means that an increase in one of two variables is related with a decrease in the other. From the Table 3 results, all correlation coefficients values are nearly zero that means although it has a very small difference at one of system parameters, corresponding encrypted images are completely different each other. From the Table 4 results, it can be concluded that encryption key generated from LOSIM is highly sensitive to the systems parameters and thus each key produces different corresponding ciphered image. Due to the having symmetric structure of this algorithm, a very small difference exists in decryption key, the ciphered image cannot be decrypted correctly in any way. As a result, the proposed encryption algorithm is quite sensitive to all keys and can resist differential attacks effectively.

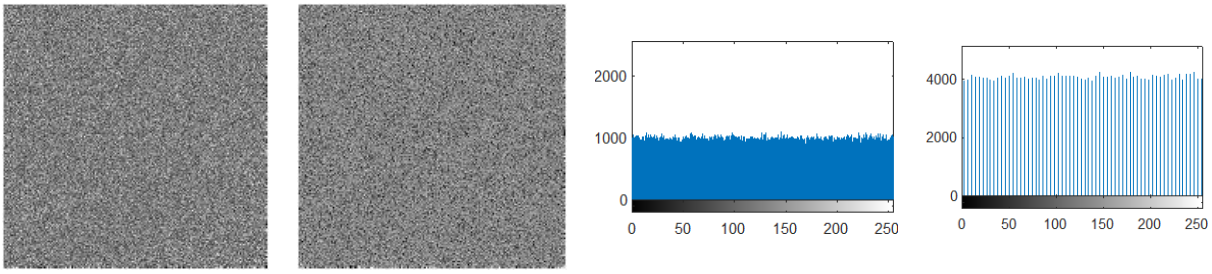
5.3. Histogram Analysis

Histogram analysis is a technique used for representing the number of pixels at each different density in an image. Pixels distribution with equal probability forms a uniform histogram that is more resistant to statistical attacks. Therefore, the histogram of an encrypted image should be as uniform as possible and exactly different from that of the original version. Figure 10 and Figure 11 shows the histograms of two distinct plain images and corresponding encrypted images, respectively.



(A) (B) (C) (D)

Figure 10. *Histograms of input images (A) 'Peppers' image (B) 'Black' image (C) Histogram of (A) (D) Histogram of (B)*



(A) (B) (C) (D)

Figure 11. *Histograms of corresponding ciphered images (A) Cipher 'Peppers' image (B) Cipher 'Black' image (C) Histogram of (A) (D) Histogram of (B)*

According to the Histogram analysis results, histograms of ciphered images are completely different than their original images and uniformly distributed over all possible intensity even the input image is simply black.

5.4. Information Entropy Analysis

Information entropy determines unpredictability of any random message and it is calculated as in Equation (5). For instance, in an entirely random source with equal probability and if it generates 256 symbols, then the information entropy for this source is 8 which means that the message has completely uncertain in theoretical. Ten randomly chosen test images with different sizes are used for Entropy analyses. These test images (Flowers, Frog, Peppers, Cameraman, Lena, Baboon, Airplane, Wind map, Landscape and White) are encrypted 20 times using the proposed algorithm with different system parameters. In addition, some important analysis results have been compared with a similar study [19] recently presented. For the entropy comparison, the average values of the R, G and B layers of the test images used by the author are taken as reference. The average entropy values are calculated and listed in Table 5.

Table 5*. Average entropy results for cipher images*

		Entropy Values	Proposed	Ref. [18]
Size	Name	Test image	Cipher image	Cipher image
128x128	Flowers	7.441183	7.988536	-
128x128	Frog	6.928970	7.988952	-
256x256	Peppers	7.574611	7.997844	-
256x256	Cameraman	7.105146	7.997580	-
512x512	Lena	7.237834	7.999479	7.999133
512x512	Baboon	7.390612	7.999263	7.999333
512x512	Airplane	6.727940	7.999573	7.998666
512x512	Wind map	7.184162	7.999322	-
1024x1024	Landscape	7.353287	7.999854	-
1024x1024	White	0	7.999805	-

It is obvious that the entropy values of the ciphered images are very close to theoretical value even if the image is truly white. In a truly white image, all pixels have a value of 255 which means that no variation in pixels and thus maximum certainty associated with the image, results zero entropy of that image. The fact that an image with such an entropy value reaches almost maximum entropy after the encryption confirms the efficiency and robustness of the proposed algorithm.

5.5. Correlation Analysis

In a meaningful image, adjacent pixels have same or very close values, so they have a strong correlation between them. An effective image encryption produces sufficiently low pixel correlation for all adjacent pixels. The formula given in Equation (11) is used to determine the correlation coefficients for all adjacent pixels that are in pair for all direction.

$$cc = \frac{\sum_{i=1}^{N}(x_i - \bar{x}).(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2 . \sum_{i=1}^{N}(y_i - \bar{y})^2}} \quad . \tag{11}$$

Here, $(\bar{x}, \bar{y})$ denotes average values of adjacent pixel pairs in a specific direction. *N* shows the total number of adjacent pixel pairs. Some randomly selected test images are used for correlation analysis to determine correlation coefficients for all directions. Correlation coefficients of test images and their corresponding ciphered images produced by the proposed algorithm are given in Tables 6 and 7, respectively.

Table 6. *Correlation coefficients of test images for all directions*

	Correlation Coefficients		
Test image	Horizontal	Vertical	Diagonal
Peppers	0.886898	0.951860	0.925176
Cameraman	0.897322	0.934574	0.892372
Lena	0.960423	0.942078	0.935210
Baboon	0.984590	0.929741	0.916277
Airplane	0.965411	0.981165	0.937368
Wind map	0.979138	0.988396	0.954013
Landscape	0.984497	0.967167	0.973207

Table 7. *Correlation coefficients of corresponding cipher images for all directions*

	Proposed scheme			Red component of Ref. [18]		
Cipher image	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Peppers	0.073146	0.028053	0.052449	-	-	-
Cameraman	-0.069231	0.074872	0.005238	-	-	-
Lena	-0.046870	-0.002649	0.014985	0.0009	0.0118	-0.0125
Baboon	-0.037114	0.018632	0.003542	-0.0267	-0.0113	-0.0120
Airplane	0.057356	0.037197	-0.064892	0.0340	-0.0133	0.0103
Wind map	0.024416	0.009624	-0.035172	-	-	-
Landscape	-0.011408	-0.046371	0.002365	-	-	-

According to the Table 6, in any test image correlation coefficients for all directions are very close to 1 as expected. However, Table 7 shows great results about the correlation coefficients for all directions of ciphered image. More clearly, coefficients values are very near to 0 that means low correlation of adjacent pixels in corresponding cipher images. Correlation of adjacent pixels in diagonal direction for both 'Wind map' test image and its cipher version are shown graphically in Figure 12.

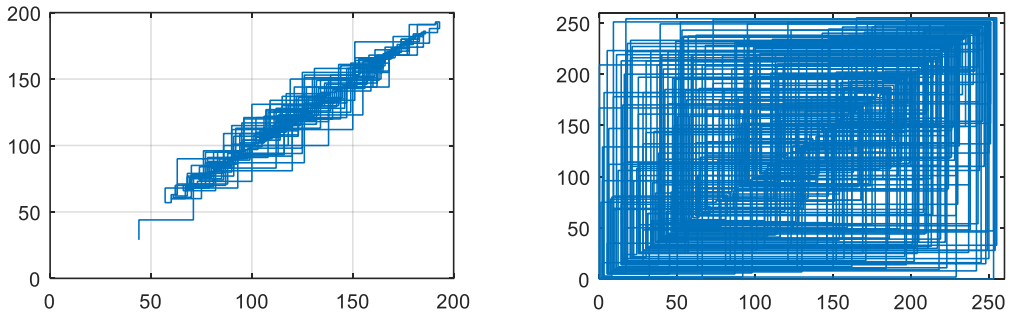


Figure 12. *Correlation distribution of adjacent pixels (A) 'Wind map' test image (B) Encrypted 'Wind map' image*

It is obvious that the diagonal correlation of 'Wind map' image has a linear spread. On the contrary, pixel distribution of encrypted 'Wind map' image has a complex distribution and scattered over the all plane as shown in Figure 12.B. 'Wind map' image is given here as an example, but identical results are also obtained for other test images. Correlation coefficients between different test images and corresponding ciphered images are given in Table 8.

Table 8. *Correlation coefficients between input images and corresponding cipher images*

Input – Cipher Image	Correlation Coefficients
Peppers	-0.000322
Cameraman	0.000477
Lena	0.000861
Baboon	0.003948
Airplane	0.001090
Wind map	-0.002894
Landscape	0.000318

Consequently, the proposed image encryption algorithm demonstrates superior correlation performance and sufficiently reduces the correlation between adjacent pixels of different input images.

5.6. Running Time Analysis

Twenty different test images (five test images for each size) are encrypted 10 times by the proposed algorithm with different system parameters and execution times for encryption and decryption are calculated using Intel Core i7 3.4 GHz CPU with 4 GB RAM running on Windows 7 and MATLAB R2015a software. The average execution time for the speed analyses can be found in Table 9.

Table 9. *Speed performance analysis of the proposed scheme*

Gray images	Encryption time (sec)	Decryption time (sec)	Encryption rate (Mbps)	Decryption rate (Mbps)
128x128	0.0215	0.0294	6.09	4.45
256x256	0.0947	0.1240	5.53	4.22
512x512	0.3708	0.4829	5.65	4.34
1024x1024	1.4930	1.9517	5.61	4.29

6. RESULTS

An effective image encryption algorithm based Bit reversal method and chaos is proposed in this paper. A new chaotic model with much better complexity and unpredictability is designed by using known chaotic maps for key generation. Performance comparison for all maps has been made in terms of Lyapunov spectrums, chaotic trajectory and entropy. Before the encryption process, all pixel positions of the input

image are changed by Bit reversal method to increase encryption strength. A very small change in the system parameters of the designed map generates completely different encryption keys, thus generating different encrypted images for the same input image. The proposed scheme based on the new chaotic map can successfully generate an encrypted image against to its original input image, providing a secure communication technique in power systems. The analysis results of this study show that the proposed encryption algorithm can be used in the secure transmission of strategically important information in power systems. Security analysis of the proposed algorithm has been performed both numerically and visually. The experimental results are satisfactory, and the proposed scheme has been verified to be of excellent quality and effectively encode and decode gray images. This study shows that in addition to the areas where chaos is widely used, it can be used in hidden information communication in the field of energy planning in power systems. The hardware implementation of the proposed image coding algorithm offers a possible direction for further work by providing accurate planning against the competitive market in markets where production systems are involved.

CONFLICTS OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] Wang, W., Si, M., Pang, Y., Ran, P., Wang, H., Jiang, X., Liu, Y., Wu, J., Wu, W., Chilamkurti, N., Jeon, G., "An encryption algorithm based on combined chaos in body area networks", Computers and Electrical Engineering, 1(65): 282-291, (2018).

[2] Chang, W. D., Shih, S. P., Chen, C. Y., "Chaotic secure communication systems with an adaptive state observer", Journal of Control Science and Engineering, 1(15): 1-7, (2015).

[3] Oğraş, H., Türk, M., "A secure chaos-based image cryptosystem with an improved sine key generator", American Journal of Signal Processing, 1(6): 67-76, (2016).

[4] Zhou, X., Li, J., Youjie, M., "Chaos phenomena in dc-dc converter and chaos control", Procedia Engineering, (29): 470-473, (2012).

[5] Kanso, A., Ghebleh, M., "A novel image encryption algorithm based on a 3D chaotic map", Communications in Nonlinear Science and Numerical Simulation, 1(17): 2943-2959, (2012).

[6] Chai, X., Fu, X., Gan, Z., Lu, Y., Chen, Y., "A color image cryptosystem based on dynamic DNA encryption and chaos", Signal Processing, Arroyo 1(55): 44-62, (2016).

[7] Alvarez, D.G., Fernandez, V., "On the inadequacy of the logistic map for cryptographic applications", arXiv preprint arXiv, 8(5): 43-55, (2008).

[8] Lu, H., Wang, X., Fei, Z., Qiu, M., "The effects of using chaotic map on improving the performance of multiobjective evolutionary algorithms", Mathematical Problems in Engineering, (14): 1-16, (2014).

[9] Alzaidi, A. A., Ahmad, M., Doja, M. N., Solami, E. A., Sufyan Beg, M. M., "A new 1D chaotic map and β-Hill climbing for generating substitution-boxes", IEEE Access, 1(6): 55405-55418, (2018).

[10] Oğraş, H., Türk, M., "A Robust chaos-based image cryptosystem with an improved key generator and plain image sensitivity mechanism", Journal of Information Security, (8): 23-41, (2016).

[11] Li, Y., Wang, C., Chen, H., "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation", Optics and Lasers in Engineering, (90): 238-246, (2017).

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

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

[14] Zhang, G., Ding, W., Li, L., "Image Encryption Algorithm Based on Tent Delay-Sine Cascade with Logistic Map", Symmetry, (12): 355-369, (2020).

[15] Tur, M.R., "Deployment of reserve requirements into the power systems considering the cost, lost, and reliability parameters based on sustainable energy", International Journal of Electrical Engineering and Education 2021, 58(2): 621–639

[16] Tur, M. R., "Reliability Assessment of Distribution Power System When Considering Energy Storage Configuration Technique", IEEE Access, (8): 77962-77971, (2020).

[17] Fu, C., Zhang, G., Zhu, M., Chen, Z., Lei, W., "A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy", Security and Communication Networks, (2018): 1-13, (2018).

[18] Arpacı, B., Kurt, E., Çelik, K., "A new algorithm for the colored image encryption via the modified Chua's circuit", Engineering Science and Technology, (23): 595-604, (2020).

[19] Arpacı, B., Kurt, E., Çelik, K., Ciylan, B., "Colored image encryption and decryption with a new algorithm and a Hyperchaotic electrical circuit", Journal of Electrical Engineering & Technology, (15): 1413-1429, (2020).