SERBIAN JOURNAL OF ELECTRICAL ENGINEERING
Vol. 16, No. 2, June 2019, 247-265

UDC: 004.056.55:004.4`273 **DOI: https://doi.org/10.2298/SJEE1902247T**

A Chaotic Image Encryption Scheme with Complex Diffusion Matrix for Plain Image Sensitivity

Janani Thiyagarajan[1], Brindha Murugan[1], Ammasai Gounden Nanjappa Gounder[1]

Abstract: A chaotic cipher is presented in this paper using 1-Dimensional and 2-Dimensional chaotic maps like logistic, Chebyshev and Arnold cat map. Permutation phase utilizes logistic map followed by Arnold cat map whereas in diffusion phase, Chebyshev's map is used. Subsequently, another complex diffusion matrix is generated from the original image. This matrix is employed to enhance the diffusion effect further. Eventually, strong input image sensitivity is explored due to this diffusion. Simulation results exhibit that the recommended cipher ensures not only high key and entropy value but also less correspondence between nearby pixels along all directions. The key point of this cipher is the high Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) values. Due to this impact, the proposed cipher produces completely random encrypted images.

Keywords: Logistic Map, Chebyshev's map, Confusion, Diffusion, NPCR, Chaos, UACI, Image encryption.

1 Introduction

Recently, online media sharing and social networking become popular over Internet. This led to frequent flow of digital images and videos in huge volume across communication media. Apparently, there is a need to secure them from leakages during storage and transmission. The need for digital image security has shown the way for developing encryption ciphers so that attackers' access is restricted. Rivest Shamir Adleman (RSA), Data Encryption Standard (DES), etc. also called traditional ciphers, are not appropriate for the real time encryption of media. Certain characteristics of images such as redundant information and huge file sizes are the obstacles for real time encryption. Chaos, which is a complex nonlinear dynamical system possesses pseudo randomness property, vigorous sensitivity to initial seed value and ergodicity that suit the needs for image encryption [1 − 7]. Chaotic ciphers are normally implemented by chaotic maps.

[1]Department of Computer Science and Engineering, National Institute of Technology, Tiruchirapalli, Tamilnadu, India; E-mails: saijanani.308@gmail.com; brindham@nitt.edu; ammas@nitt.edu

The very first chaotic cipher was proposed by Mathews [8] in 1989. After this, it becomes a tradition to use chaotic maps for image encryption. Normally, a variety of chaotic maps like Arnold, Chebyshev, logistic, Tent map etc., are adopted because of their easy implementation [9 – 10]. In any encryption cipher, there are two phases for encryption: permutation and diffusion. The first phase shuffles the pixel's location of an image whereas to render the image in an unintelligible way, the other phase i.e., diffusion phase modifies the pixel's value of an image. This paper proposes permutation-diffusion architecture. Cipher's resistance to attacks is determined by various measures. Histogram analysis and correlation between neighboring pixels are good determinant of statistical attack. Entropy is a very good measure of randomness. NPCR and UACI values are good determinant of differential attack.

In Ye's [11] method, using generalized Arnold cat map, two index order sequences are generated which in turn employed in the permutation process. Another two random gray level series produced by the generalized Arnold cat map and Bernoulli shift map are used to perform two-way diffusion. In this scheme, for the standard Lena image, UACI and NPCR values are 27% and 98.5% respectively. For a single pixel change, the two-way diffusion effect is not effective enough to spread across the entire cipher image which leads to the above said low metrics. Xing et.al. [12] method uses one dimensional discrete chaotic maps. Confusion is executed by generating a pseudo-random sequence with Baker map and combines pixels to block randomly. The UACI values are only 27% however it has adequate NPCR values. This is due to the weak diffusion process of the algorithm. Even though the quantity of pixel change rate for a change in single pixel is high, the average change in the intensity values is low due to the weak diffusion effect. Referring to Lin et.al. [13] scheme, which uses spatiotemporal chaotic system as well as self-adaptive method for bit-level image encryption, the NPCR value falls down to 93.67%. This scheme encrypts the higher four bits of binary images part using lower four bits of binary images part in order to achieve plain image sensitivity. The encrypted value at each and every point does not strongly relate to the processed plain-image due to which there is a degradation of the NPCR values.

Enayatifar et.al. [14] use deoxyribonucleic acid (DNA) and the chaotic logistic map to obtain a number of primary DNA masks and then the best mask is decided for encryption by applying the genetic algorithm (GA). The keyspace of this algorithm is only 10^{36} since 120-bit secret key is used. Also, for some of the test images like Baboon, Boat and Pepper, the NPCR value falls down to 98.692, 98.923 and 99.2995 respectively. This is due to the non-uniform distribution of the diffusion effect spread over the entire image. In Chen et al. [15] scheme, substitution based on nonlinear inter-pixel calculating method and

permutation based on swapping is employed. Even though this cipher yields good performance metrics, the key space of the cipher is only 10^{60}. Liu et al. [16] propose a new couple map lattice and using this map, a novel encryption algorithm is presented for images. The key is disturbed using a true arbitrary number to modify the permutation matrix as well as the key stream dynamically. The average NPCR is fairly nearer to the theoretical limit of 99.6094% but the correlation values along vertical, horizontal and diagonal directions are somewhat high like 0.023, 0.028 and 0.023 respectively. This low performance metric is due to the weak diffusion effect of the algorithm.

In Liu G et al. [17] scheme, a pathological colour image encryption algorithm is proposed using chaos. The hash value is calculated from the combination of original image and an arbitrary number to produce one-time keys for chaotic Chebyshev maps and it is applied in the process of permutation. Further, the image after permutation is split into long blocks of 256-bit and each block undergoes XOR operation with the previous block's hash value for diffusion. This algorithm yields an entropy of 7.98 which is a sign of indication of somewhat less randomness of the ciphered image. This leads to the probability of accidental information leakage. In Murillo [18] scheme, colour image encryption is done using its plain image features. The UACI value is 33.36 and the keyspace is only about 10^{38}.

Erdem [19] used content sensitive based dynamic function for chaotic image encryption. Author's content-sensitive dynamic switching function gives random behavior for ensuring sensitivity to changes in plain image pixels. Author has also utilized local Shannon entropy as a measure to compute and portray the amount of uncertainty in the cryptosystem. The experiment result shows that the average value of entropy is 7.902450 by considering 44×44 image blocks. In Souyah et. al [20] scheme, another chaotic cipher is proposed for medical image content preservation using confusion and diffusion modules. An enhanced 1D logistic tent framework is used for both confusion and diffusion stages. The plain medical image is subjected to a shuffling in non-linear bit level and circular shifting confusion based on for achieving bit balancing effect. Additionally, expanded XOR operation is used for pixel value transformation in diffusion phase. The author focused on image content preservation under single encryption round. Also Erdem et. al [21] suggested a method with two independent chaotic functions for performing confusion and diffusion principles. Authors tested the scheme under statistical and differential attacks and the outcome demonstrates that the correlations along horizontal and vertical correlation directions of the encrypted image are high like 0.014593 and 0.036587 respectively. This indicates that the scheme is less resistant towards attacks.

Zhang [22] uses hyper-chaotic Lorenz system for image encryption where the encryption and decryption procedures are indistinguishable. The hyper chaotic Lorenz framework is utilized to create the confidential code streams for encrypting the original image and a diffusion procedure is incorporated with XOR. In this paper, plain image is utilized only for scrambling and not for diffusion. In Rim et al. [23] technique, beta maps are utilized to generate chaotic sequences for encryption algorithm. They additionally adopt permutation-substitution network structure for encrypting the images. Similarly, Chunyan Han [24] proposed a new logistic map using conventional scrambling and diffusion method. This modified logistic map is served as a pseudo random generator for the encryption algorithm. But both the aforementioned schemes are not associated with the plain image and this prompts to the possibility of chosen plaintext or known plaintext attack. S Dhall et.al. [25] suggested another chaos based probabilistic method with adaptable block size. The paper also utilized a Random Bits Insertion stage succeeded by 4 iterations of two-staged diffusion including simple XOR (exclusive-OR). The images are encrypted using symmetric keys and produce a cipher image which is double the given plaintext size and this will lead to a high computational complexity. Additionally, the aforementioned scheme possesses low NPCR and UACI value for the standard Lena image. Juan et.al. [26] use synchronization of fractional chaotic system based encryption method for encrypting color RGB images and text. The security of the image is ensured by utilizing the properties of chaotic fractional system.

The proposed cipher uses the combination of two methods, permutation and diffusion. Permutation is done using random sequences generated from the logistic map whereas diffusion is performed using two steps. The odd numbered vector produced by the Chebyshev's map is utilized for modifying the pixel values and it act as the first step of diffusion. The subsequent step changes the pixel values by the complex diffusion matrix achieved from the original image. The novelty of the proposed methodology in addition to the combination of logistic, Arnold and Chebyshev maps in permutation and diffusion processes is the complex diffusion matrix produced from the weighted series of the input image pixel content. Due to this complex diffusion matrix, there is strong plain image sensitivity and the diffusion influence is extended over the entire enciphered image. This matrix plays a significant role in contributing reasonably high NPCR and UACI. Also, it overcomes the disadvantages of the existing solutions like high correlation, low randomness and low NPCR and UACI. The recommended encryption methodology yields a very good key space of 10^{90} and entropy of 7.9947. The encrypted image has a nearly straight histogram. The main feature of this proposed solution is the high NPCR (99.6076%) and high UACI (33.4481%).

2 Brief Review of Logistic, Chebyshev's and Arnold Cat Map

A brief illustration of the chaotic maps utilized in the suggested solution is discussed at length in this section.

2.1 The logistic map

The 1-D (one dimensional) chaotic logistic map is represented like,

$$L_{n+1} = \mu(1 - L_n), \tag{1}$$

where $L_n \in [0,1]$ denotes the value at every iteration, L_0 is the initial value, $\mu = [3.5699456.4]$, with this value of μ the system exhibits chaotic behavior so that a slight modification in the initial value yields a random chaotic sequence.

2.2 Chebyshev's map

The equation for this map is given by,

$$C_{k+1} = \cos(\rho \times \cos^{-1} C_k), \tag{2}$$

C_0 lies within a range of –1 and +1 and ρ, where ρ is approximately set between 3.98 and 4.00 to produce highly chaotic sequences.

2.3 Arnold cat map

The traditional Arnold map is stated as,

$$\begin{pmatrix} A_{n+1} \\ C_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} A_n \\ C_n \end{pmatrix} \bmod G, \tag{3}$$

where (A_n, C_n) are the original pixel positions, (A_{n+1}, C_{n+1}) are the scrambled pixel positions and *G* is the number of rows in an image.

3 Proposed Algorithm

The suggested algorithm uses the combination of logistic map and Arnold cat map for permutation and Chebyshev's map for diffusion. This section discusses the proposed algorithm in detail. The algorithm has been implemented in MATLAB, using the standard Lena image as test input.

3.1 Permutation process

The steps formulated in the permutation stage of encryption are:

Step 1: The seed value $L_0^{(1)}$ and the control parameter $\mu^{(1)}$ are assigned for the logistic map.

Step 2: The sequence of values, $\left\{IL_k^{(1)}, k = 1,2,\ldots,GH\right\}$ is got by iterating the logistic map for *GH* times, where *G* and *H* represent the image's height and width.

Step 3: The seed value $L_0^{(2)}$ and the control parameter $\mu^{(2)}$ is assigned for the logistic map.

Step 4: The sequence of values $\left\{L_k^{(2)}, k=1,2,\ldots,GH\right\}$ is got by iterating the logistic map for GH times.

Step 5: The two sequences $\left\{L_k^{(q)}, k=1,2,\ldots,GH\right\}$ and $\left\{L_k^{(2)}, k=1,2,\ldots,GH\right\}$ got from the logistic map is sorted to obtain the two index order series $\left\{IL_k^{(1)}, k=1,2,\ldots,GH\right\}$ and $\left\{IL_k^{(2)}, k=1,2,\ldots.GH\right\}$.

Step 6: The original plain image *PI* of size *GH* is transformed into a one dimensional (1-D) vector $\left\{IV, k=1,2,\ldots,GH\right\}$.

Step 7: The vector $\left\{IV, k=1,2,\ldots,GH\right\}$ is permuted using the sorted index series, $\left\{IL_k^{(1)}, k=1,2,\ldots,GH\right\}$ and $\left\{IL_k^{(2)}, k=1,2,\ldots,GH\right\}$, in the following manner to get the permuted vector $\left\{P_k, k=1,2,\ldots.GH\right\}$.

$$\begin{aligned} H_k &= IV_{IX_k}, \quad k=1,2,\ldots,GH, \\ P_k &= H_{IY_k}, \quad k=1,2,\ldots,GH. \end{aligned} \tag{4}$$

Step 8: The permuted vector $\boldsymbol{P}_k$ is resized to obtain the two dimensional matrix $\boldsymbol{B}$.

Step 9: All elements in *I* is summed up to obtain *Q*, which in turn is utilized to calculate $U = Q \bmod M$. For U such iterations matrix $\boldsymbol{B}$ is scrambled by utilizing classical Arnold cat map in order to attain the permuted image.

3.2 Diffusion process

By means of diffusion, any cipher can effectively resist statistical as well as differential attack. The cipher image's histogram looks fairly even so that it can significantly resist statistical attack. If the diffusion process is strong enough, even for two slightly different input images of single pixel change, the cipher may produce completely different cipher image, the diffusion process is carried out using the succeeding steps:

Step 1: The seed C_0 and control parameter ρ is assigned for the Chebyshev's map.

Step 2: An odd numbered vector is generated using Chebyshev's map by checking the following condition

$$\bmod\left(\text{fix}\left(256\times C_k\right),2\right)\neq 0 \text{ and } \left(256\times C_k\right)>0, \tag{5}$$

where C_k is calculated using Chebyshev's map, $0\le k\le 3\times GH$, Z is computed using (6):

$$Z_i = \text{fix}\left(256 \times C_{K+1}\right), \quad 1 \le i \le GH\,, \tag{6}$$

where $\text{mod}(a,b)$ is the modulus operator which provides the remainder when a divides b, $\text{fix}(a)$ is a round function that rounds a to 0.

Step 3: The odd numbered vector $\{Z_i, i = 1,2,\ldots,GH\}$ is converted to a $G \times H$ matrix $\boldsymbol{J}$ in row first order.

Step 4: The plain image PI is changed into a $1 \times GH$ vector $\boldsymbol{T}_1$. Then using (7) another $1 \times GH$ vector $\boldsymbol{T}_2$ is constructed from $\boldsymbol{T}_1$:

$$T_2(1) = T_1(1) \times 1 + T_1(2), \ldots, T_1(i-1) \times (i-1) + T_1(i) \times (i)\,, \tag{7}$$

where $i = \{x \mid x \in N, x \le GH\}$.

Step 5: Similarly, another vector T_3 is obtained using $T_3 = T_2 \bmod (F+1)$, where F represents the potential gray levels in an image.

Step 6: T_3 is utilized to generate yet another vector T_4 of size $1 \times (GH)$ using (8):

$$\begin{aligned} T_4(i) = {} & T_3(GH) \times 1 + T_3((GH)-1) \times 2 + T_3((GH)-2) \times 3 + \\ & + \cdots + T_3((GH) - (i-1)) \times i, \end{aligned} \tag{8}$$

where $i = \{x \mid x \in N,\ x \le GH\}$.

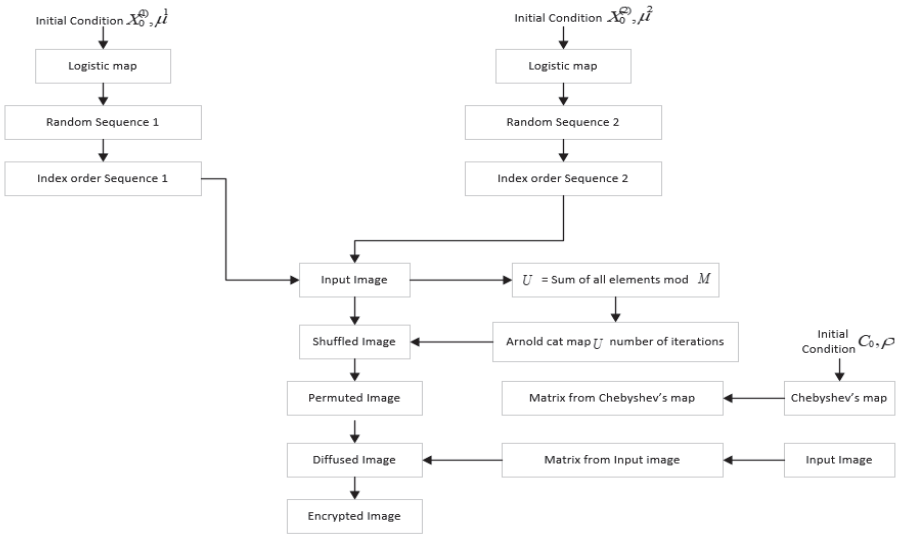


Fig. 1– *Block diagram of the suggested framework.*

Step 7: Then vector $T_5 = T_4 \bmod(F+1)$ is determined. T_5 is converted into a *GH* matrix $\boldsymbol{B}$ in row first order.

Step 8: The corresponding elements of *S* is XOR-ed with the elements of *J* to get a *GH* matrix $\boldsymbol{B}$.

Step 9: The enciphered image *E* is got by doing XOR operation on the elements of *V* and *D*. Fig. 1 illustrates the block diagram of above steps associated with permutation and diffusion process.

Fig. 2a depicts the plain image whereas Figs. 2b and 2c are the permuted and encrypted images.

Fig. 2 – *Results of the suggested algorithm: (a) Plain image; (b) Permuted image; (c) Encrypted image.*

4 Security Analysis

As per the cryptology principles [27 – 28], an ideal cipher should be very strong against various types of attacks like brute force, statistical, cryptanalytic attack, etc. This is needed to guarantee the effectiveness of any encryption algorithm. The brute force attack can be made infeasible by making the key space extremely large enough. It should also have adequate complexity to withstand the most vulnerable attacks like the differential attack, statistical attack, chosen plain text attack, etc. Randomness of any cipher image is better determined by means of entropy analysis. An entropy of 8 for gray scale image denotes a completely random image. Histogram analysis is a better way to determine a cipher's resistance to statistical attack. Differential attack is evaluated by means of NPCR and UACI measures. In this section, some of these fundamental security examinations are carried out to validate the proposed cipher's resistance against different attacks.

4.1 Key space analysis

The keys utilized in the suggested cipher are the seed and control values of logistic and Chebyshev's map, plus total iterations in Arnold cat map.

Table 1
Keys used in the proposed algorithm.

S. No.	Map	K	Value
1	Logistic map	$X_0^{(1)}$	$0.78899\,e^{-11}$
2		$\mu^{(1)}$	$3.63727\,e^{-11}$
3		$X_0^{(2)}$	$0.23654\,e^{-11}$
4		$\mu^{(2)}$	$3.57727\,e^{-11}$
5	Chebyshev's map	C_0	$0.76599\,e^{-11}$
6		ρ	$3.57727\,e^{-11}$

IEEE floating point standard [29] states that, for a double precision number of 64-bit, the computational precision is 10^{-15}. The same precision is considered for all the initial seed and the control values of the proposed cipher, so that the keyspace reaches about 10^{90}. This keyspace can effectively prevent any sort of brute force attacks.

4.2 Keysensitivity analysis

High key sensitivity is a mandatory requirement for any secure cipher. It is required to prevent the more advanced attack such as chosen plain text attack that includes linear and differential cryptanalysis. For this test, the initial seed and control values of the various kinds of maps are partially changed and the sensitiveness of the encryption method is determined. The keys of the suggested algorithm are listed in **Table 1**. The steps involved in testing key sensitivity are as follows:

1. A collection of initial seed and control values are assigned for the different maps as in **Table 1**.
2. Using values in **Table 1**, cipher image H is attained by applying the suggested encryption algorithm in the plain image PI.
3. A very small boost up of 10^{-15} is given to any one of the key value listed in **Table 1** and PI undergoes the suggested encryption again to get the new encrypted image H_+ (increment).
4. Then for the same key value chosen in step 3, the same magnitude is decremented and PI is encrypted again to produce another encrypted image K (decrement).
5. The chosen key's sensitivity is measured using (9), (10):

$$KS(a) = \frac{\sum_{c=1}^{G} = \sum_{d=1}^{H} R\left(K(c,d), K\_(c,d)\right) + R\left(K(c,d), K_{+}(c,d)\right)}{2 \times (GH)} \times 100\% \text{ , (9)}$$

where, G and H stands for the height and width of the image respective:

$$R(r,c) = \begin{cases} 1, & \text{if } r \neq c; \\ 0, & \text{if } r = c. \end{cases} \tag{10}$$

Table 2
Key sensitivity test.

S. No.	Map	a	Value [$\times e^{-11}$]	Inc./Dec.	KS(a) [%]
1	Logistic map	$L_0^{(1)}$	0.78899	10^{-15}	99.6117
2		$\mu^{(1)}$	3.63727		99.6132
3		$L_0^{(2)}$	0.23654		99.6167
4		$\mu^{(2)}$	3.57727		99.5982
5	Chebyshev' Map	C_0	0.76599		99.6166
6		ρ	3.57727		99.6151

The sensitivity of various key values used in the proposed cipher is specified in **Table 2**. It is apparent from **Table 2** that, more than 99.5% of the pixel changes in the cipher image for a minor change in key values.

4.3 Entropy analysis

Information entropy is the regularly utilized measurement to manifest the uncertainty and arbitrariness of data. With respect to image data, the dissemination of its grayscale esteems is evaluated so that, nearer the entropy to its hypothetical value, indicates a better uniform in the dispersion of image grayscale values. The proposed method carries out two entropy analysis for identifying the image randomness (i) Shannon entropy and (ii) Local Shannon Entropy.

4.3.1 Shannon Entropy

For randomness, the most prominent feature is entropy. The global Shannon entropy measure is evaluated using (11).

$$H(m) = -\sum_{i=0}^{F-1} p\left(m_i \times \log_2\left(p(m_i)\right)\right), \tag{11}$$

where F denotes the image's potential gray levels, and $p(m_i)$ indicates the likelihood of occurrence of i gray level in an image. For an image that is

completely random with 256 potential gray levels, the entropy is 8 and it is treated as an ideal value. Satisfyingly, the entropy of the suggested cipher (for the encrypted Lena image) is 7.9943 which is closer to the ideal value.

4.3.2 Local Shannon Entropy

Local Shannon entropy is the metric for calculating randomness of an image by utilizing Shannon entropy over local image blocks. Maximum entropy value i.e., equal to 8 which is measured by Global Shannon entropy is not enough to conclude the true randomness of the image. Hence it is necessary to measure the randomness with respect to local image blocks. For an image the local Shannon entropy is measured as:

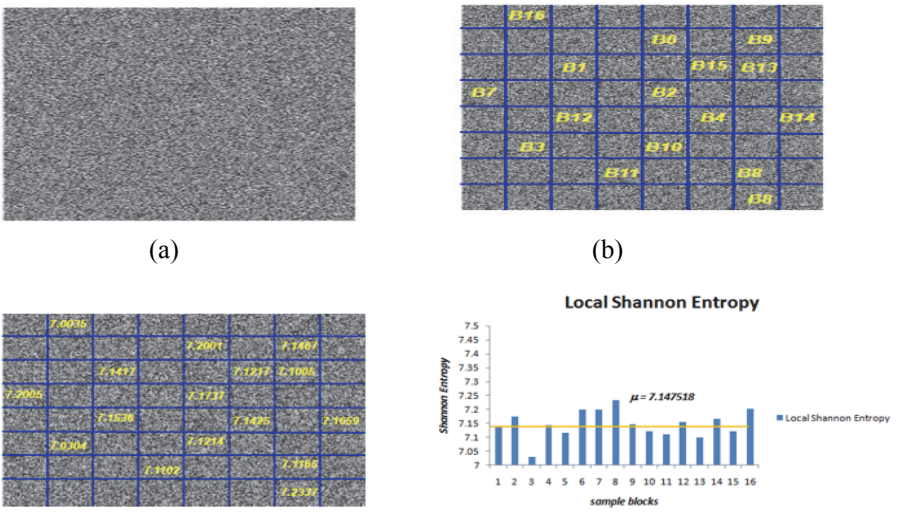
$$H_{k,T_B}^{-} = \sum_{i=1}^{k} \frac{H(S_i)}{k}, \tag{12}$$

where T_B is the local block size and k is the number of blocks indicated by S_i. The ciphered image randomness is measured by utilizing the local Shannon entropy H_{k,T_B}^{-}. As mentioned in [31], experiment has been carried out for standard Lena image with size 256×256 over randomly chosen 16 blocks. Fig. 3 depicts the image randomness measure using local Shannon entropy, where Fig. 3a shows the input standard Lena ciphered image of size 256×256. Similarly as in Fig. 3b, for randomness calculation, proposed work has taken 16 image blocks randomly and the local Shannon entropy study is carried out. Fig. 3c shows the entropy value for each block and these values are plotted with mean of 7.147518 and it is nearer to the standard mean value say 7.174966 for 16×16 by [30]. This outcome demonstrates that the proposed work produces the image with high randomness by utilizing both global and local Shannon entropy value.

The local Shannon entropy test is performed for various standard images by considering the block value as 16 and the values are tabulated in **Table 3**.

Table 3
Local Shannon entropy.

S. No.	Image	Local Shannon Entropy value
1	Lena	7.147518
2	Pepper	7.126796
3	Baboon	7.140573
4	Couple	7.132789



(a) (b)

(c) (d)

Fig. 3 – *Results of Local Shannon Entropy: (a) Ciphered image; (b) Random 16 image blocks; (c) Shannon entropy value for each block; (d) Average value obtained from local Shannon entropy.*

4.4 Correlation coefficient analysis

For a secure encryption algorithm, minimum correlation of neighboring pixels is required along various directions like horizontal, vertical and diagonal. Correlation of the suggested cipher is calculated using (13) – (15) by choosing six thousand random samples of neighboring pixels of plain and encrypted images

$$C_r = \frac{\operatorname{cov} a(m,n)}{\sqrt{D(m) \times D(n)}}, \tag{13}$$

where

$$\operatorname{cov} a(m,n) = \frac{1}{S}\sum_{i=1}^{S}\left(m_i - H(m)\right)\left(n_i - H(n)\right),$$

$$H(t) = \frac{1}{S}\sum_{i=1}^{T} t_i, \tag{14}$$

$$D(t) = \frac{1}{S}\sum_{i=1}^{S}\left(t - H(t)\right)^2, \quad t = m,n, \tag{15}$$

where (m_i, n_i) denotes two neighboring pixel values, $H(t)$ denotes the average and $D(t)$ denotes the variance. $H(t)$ and $D(t)$ are computed for all m and n individually and $S = (6000)$ denotes the chosen sample pixel pairs.

Table 4
Correlation value comparison among different schemes.

S. No.	Encryption Method	Correlation		
		Horizontal	**Vertical**	**Diagonal**
1	Enayatifar, Abdullah and Isnin [14]	0.0007	0.0017	0.0001
2	Ye's [11]	$-8.19\,e^{-4}$	0.0016	0.0115
3	Murillo, Cruz, Abundiz, López & Acosta [18]	0.0135	0.0835	0.0170
4	Chen, Xin, Zhu, Fu, Zhang and Zhang [15]	0.0037	0.0018	-0.0011
5	Quan, Li, Zhang, Sui and Yang [16]	0.023	0.028	0.023
6	Guoyan, Li and Liu [17]	0.0036	-0.0012	0.0002
7	**Proposed scheme**	**0.00482**	**0.00113**	**0.00873**

The plain image correlation is nearer to 1 due to redundancy. A good encryption algorithm should yield less correlation with an ideal value of zero along all the three directions. The coefficients obtained from the suggested cipher are compared against earlier schemes and are recorded in **Table 4**. It is inferred from **Table 4** that the suggested cipher is competent with other existing schemes.

4.5 Histogram analysis

Shannon's masterpiece indicates that, statistical attack is able to break any cryptosystem. Thus, any cryptosystem is said to be strong enough if it is robust against any statistical attack. By means of histogram analysis, the resistance of a cipher to statistical attack can be easily examined. An image histogram indicates the rate of gray level distribution of images. The cipher image's histogram (Fig. 5) has unfluctuating distribution of gray levels compared to plain image's histogram (Fig. 4), which demonstrates that the plain image's characteristic distribution of pixels along the whole range is vanished. Accordingly it is demonstrated that the proposed cipher is not vulnerable to the statistical attack. Also the histogram uniformity is obtained by Chi-square test [31]. So, the chi-square test is simulated for various sample images and recorded in **Table 5**. It demonstrates that the proposed cipher acquires null hypothesis. The p values are

also higher than 0.05(5%) significance for the encrypted images. From this, histogram uniformity is shown. Additionally, one more observation is that the repetition of pixels are totally hidden which also confirms the inability to statistical attack.

Table 5

Histogram uniformity assessment test.

Metrics	Lena	Baboon	Pepper	Brick wall	Couple	Girl	Grass
P value	0.4546	0.3421	0.5128	0.4289	0.3319	0.4735	0.6542
Decision (0 or 1)	0; Agree	0; Agree	0; Agree	0; Agree	0; Agree	0; Agree	0; Agree

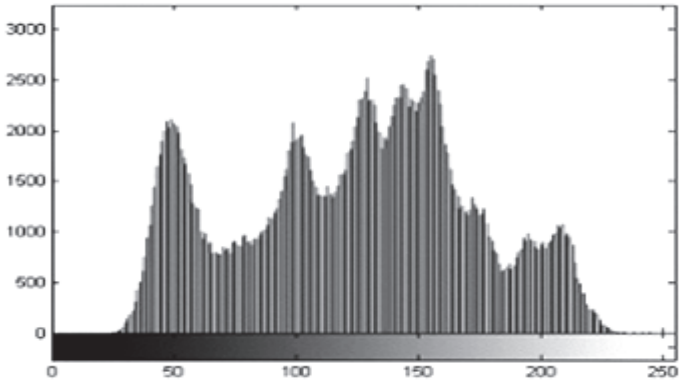


Fig. 4 – *Histogram of input image*

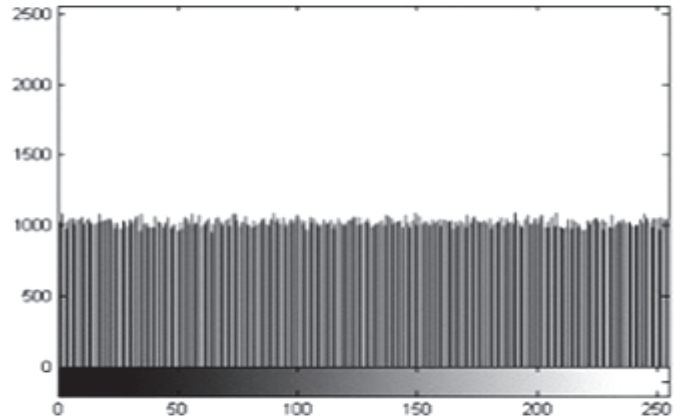


Fig. 5 – *Histogram of output image.*

4.6 Differential attack

To make the differential cryptanalysis infeasible, slightly different plain images should produce completely different cipher images. A slight change such as a single pixel may be altered in the original image and the related modifications of the enciphered image are examined to determine the change-in pixel values between the input and enciphered image. NPCR and UACI measures are utilized to evaluate this change.

4.6.1 NPCR

NPCR calculates the change rate in number of pixels between two enciphered images that are achieved from two slightly different input images-the original image and yet another image which is got by varying some random pixel in the input image. To develop an effective cryptosystem, NPCR value should be close to 100% which indicates its maximum sensitivity. For different test images, the NPCR value is determined using (16) and (17) for three trials and are furnished in **Table 6**.

$$\mathrm{NPCR} = \frac{\sum_{a=1}^{G}\sum_{b=1}^{H} Z(a,b)}{GH}, \tag{16}$$

where

$$Z(a,b) = \begin{cases} 1, & \text{if } CI_1 \neq CI_2; \\ 0, & \text{if } CI_1 = CI_2. \end{cases} \tag{17}$$

4.6.2 UACI

UACI calculates the mean variation of pixel strength in same locations of two enciphered images with the maximal intensity value F (for gray scale images F =255) and it is denoted as percentage. For different test images, the UACI value is determined using (18) and it is furnished in **Table 6**.

$$\mathrm{UACI} = \frac{\sum_{a=1}^{G}\sum_{b=1}^{H} \left| \mathrm{C}_1(a,b) - \mathrm{C}_2(a,b) \right|}{255 \times (GH)}, \tag{18}$$

where CI_1 and CI_2 denote the two enciphered images of the slightly different plain images.The NPCR & UACI values for three trials for several input images are illustrated in **Table 6**. From **Table 6**, it is inferred that even though there is a slight variation between two input images, the NPCR and UACI measures are ideal across various trials. Moreover, it also exhibits good performance for various test images. It is also observed that the mean NPCR and UACI values are respectively 99.6076% and 33.4481%. **Table 7** shows the critical values of NPCR and UACI with three different α levels [32] and from the analysis of the

proposed result in **Table 8** using **Table 7**, the NPCR and UACI esteems of the standard images are non-critical and it passes the randomness test. These non-critical values indicate the efficiency of the suggested scheme. To validate the efficacy of the recommended cipher, the current strategies are compared and are illustrated in **Table 9**.

Table 6
NPCR & UACI values for three trials for different input images.

Image	1st Trial		2nd Trial		3rd Trial	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
Lena	99.6165	33.4645	99.6198	33.4511	99.6012	33.4545
Baboon	99.6023	33.4356	99.6156	33.4745	99.6133	33.4366
Pepper	99.5898	33.4734	99.6089	33.4512	99.6154	33.4457
Grass	99.5989	33.3945	99.6012	33.4654	99.6173	33.4423
Brick wall	99.6132	33.4678	99.5943	33.4532	99.5934	33.4562
Girl	99.6267	33.4467	99.6134	33.4232	99.6176	33.4578
Couple	99.6213	33.4043	99.6078	33.4026	99.5936	33.4827
Airplane	99.6011	33.4678	99.6134	33.4254	99.6205	33.4687
Sailboat	99.5843	33.4531	99.6132	33.4438	99.5917	33.4566

Table 7
Theoretical critical values of NPCR & UACI for different α-levels.

S. No.	Image Size	Level	NPCR (%)	UACI (%)
1.	256×256	0.05	99.5693	33.2824 – 33.64447
		0.01	99.5527	33.2255 – 33.7016
		0.001	99.5341	33.1594 – 33.7677
2.	512×512	0.05	99.5893	33.3730 – 33.5541
		0.01	99.5810	33.3445 – 33.5826
		0.001	99.5717	33.3115 – 33.6156

Table 8
NPCR & UACI randomness test for different input images with different sizes.

S. No.	Image Size	Image	NPCR (%)	UACI (%)	NPCR test [30]	UACI test [30]
1.	256×256	Lena	99.6165	33.4645	Pass	Pass
		Baboon	99.5981	33.4746	Pass	Pass
2.	512×512	Lena	99.6081	33.4321	Pass	Pass
		Baboon	99.5997	33.4334	Pass	Pass

Table 9
NPCR & UACI measures for different schemes.

S. No.	Existing Scheme	NPCR(%)	UACI(%)
1	Enayatifar, Abdullah and Isnin [14]	98.6928	33.4674
2	Ye's [11]	99.2453	36.4973
3	Murillo, Cruz, Abundiz, López & Acosta [18]	99.61	33.36
4	Chen, Xin, Zhu, Fu, Zhang and Zhang [15]	99.61	33.46
5	Quan, Li, Zhang, Sui and Yang [16]	99.6094	-
6	Guoyan, Li and Liu [17]	99.6253	33.4312
7	**Proposed Scheme**	**99.6076**	**33.4481**

4.6.3 Speed and Performance analysis

The encryption speed and computational complexity are the crucial feature for any encryption technique. The actual running time for the suggested scheme is determined by utilizing the machine with following features: Windows 10, 64 bit, Matlab R2018a, Intel Pentium N3540, CPU @ 2.16 GHZ processor, with RAM of 8 GB memory. The computational complexity of the recommended algorithm relies on the confusion and diffusion procedures. The time taken for the permutation process is $O(GHU)$, where G and H are the number of rows and columns in the image respectively and U is the number of iterations. Similarly, diffusion takes only $O(G \times H)$ which is very less compared to other existing schemes. In the proposed algorithm, since simple mathematical operation is used, it leads to very less encryption and decryption time. The running time of the suggested encryption machine is given in **Table 10** which is very less compared with other algorithms.

Table 10
Execution time for various sizes of images.

S. No.	Image Size	Execution time (s)			
		Ref[19]	Ref[20]	Ref[21]	Proposed
1	256×256	0.022	0.048	0.032	0.018
2	512×512	0.085	0.139	0.110	0.065
3	1024×1024	0.322	0.481	0.437	0.247

5 Conclusion

A new encryption scheme has been proposed using chaotic maps for high plain image sensitivity. Two permutation sequences are constructed from the logistic map and one diffusion matrix is constructed from the Chebyshev's map. Additionally, one more weighted sequence is constructed from the plain image which adds strong sensitivity. It has been proved by various experimental

results that the proposed cipher exhibits a very high resistance to statistical, differential and Brute force attack. Besides, the encryption algorithm possesses exceptionally good key space, a very good entropy value and very less correlation among neighboring pixels, which demonstrates the viability of the ciphering algorithm. This proves that the suggested cipher is extremely secure.

6 References

[1] C. E. Shannon: Communication Theory of Secrecy System, The Bell System Technical Journal, Vol. 28, No. 4, October 1949, pp. 656 – 715.

[2] M. S. Baptista: Cryptography with Chaos, Physics Letters A, Vol. 240, No. 1-2, March 1998, pp. 50 – 54.

[3] J. Fridrich: Symmetric Ciphers Based on Two-Dimensional Chaotic Maps, International Journal of Bifurcation and Chaos, Vol. 8, No. 6, June 1998, pp. 1259 – 1284.

[4] Z. Hua, F. Jin, B. Xu, H. Huang: 2D Logistic-Sine-Coupling Map for Image Encryption, Signal Processing, Vol. 149, August 2018, pp. 148 – 161.

[5] X. Chai, X. Zheng, Z. Gan, D. Han, Y. Chen: An Image Encryption Algorithm Based on Chaotic System and Compressive Sensing, Signal Processing, Vol. 148, July 2018, pp. 124 – 144.

[6] L. Kocarev, G. Jaimovsvski: Chaos and Cryptography- From Chaotic Maps to Encryption Algorithms, Springer, New York, 2007.

[7] X. Zhang, X. Wang: Multiple-Image Encryption Algorithm Based on Mixed Image Element and Chaos, Computers & Electrical Engineering, Vol. 62, August 2017, pp. 401 – 413.

[8] R. Matthews: On the Derivation of a "Chaotic" Encryption Algorithm, Cryptologia, Vol. 13, No.1, January 1989, pp. 29 – 42.

[9] N. K. Pareek, V. Patidar, K. K. Sud: Image Encryption Using Chaotic Logistic Map, Image and Vision Computing, Vol. 24, No. 9, September 2006, pp. 926 – 934.

[10] X. Tong, M. Cui: Image Encryption with Compound Chaotic Sequence Cipher Shifting Dynamically, Image and Vision Computing, Vol. 26, No. 6, June 2008, pp. 843 – 850.

[11] R. Ye: A Novel Chaos-Based Image Encryption Scheme with Efficient Permutation-Diffusion Mechanism, Optics Communications, Vol. 284, No. 22, October 2011, pp. 5290 – 5298.

[12] X. Wang, F. Chen, T. Wang: A New Compound Mode of Confusion and Diffusion for Block Encryption of Image Based on Chaos, Communications in Nonlinear Science and Numerical Simulation, Vol. 15, No. 9, September 2010, pp. 2479 – 2485.

[13] L. Teng, X. Wang: A Bit-Level Image Encryption Algorithm Based on Spatiotemporal Chaotic System and Self-Adaptive, Optics Communications, Vol. 285, No. 20, September 2012, pp. 4048 – 4054.

[14] R. Enayatifar, A. H. Abdullah, I. F. Isnin: Chaos-Based Image Encryption Using a Hybrid Genetic Algorithm and a DNA Sequence, Optics and Lasers in Engineering, Vol. 56, May 2014, pp. 83 – 93.

[15] J. Chen, Z. Zhu, C. Fu, L. Zhang, Y. Zhang: An Image Encryption Scheme Using Nonlinear Inter-Pixel Computing and Swapping Based Permutation Approach, Communications in Nonlinear Science and Numerical Simulation, Vol. 23, No. 1-3, June 2015, pp. 294 – 310.

[16] Q. Liu, P. Li, M. Zhang, Y. Sui, H. Yang: A Novel Image Encryption Algorithm Based on Chaos Maps with Markov Properties, Communications in Nonlinear Science and Numerical Simulation, Vol. 20, No. 2, February 2015, pp. 506 – 515.

[17] G. Liu, J. Li, H. Liu: Chaos-Based Color Pathological Image Encryption Scheme Using One-Time Keys, Computers in Biology and Medicine, Vol. 45, February 2014, pp. 111 – 117.

[18] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, O. R. Acosta Del Campo: A RGB Image Encryption Algorithm Based on Total Plain Image Characteristics and Chaos, Signal Processing, Vol. 109, April 2015, pp. 119 –131.

[19] E. Yavuz: A Novel Chaotic Image Encryption Algorithm Based on Content-Sensitive Dynamic Function Switching Scheme, Optics & Laser Technology, Vol. 114, June 2019, pp. 224 – 239.

[20] S. Amina, F. K. Mohamed: An Efficient and Secure Chaotic Cipher Algorithm for Image Content Preservation, Communications in Nonlinear Science and Numerical Simulation, Vol. 60, July 2018, pp. 12 – 32.

[21] E. Yavuz, R. Yazici, M. C. Kasapbaşı, E. Yamaç: A Chaos-Based Image Encryption Algorithm with Simple Logical Functions, Computers & Electrical Engineering, Vol. 54, August 2016, pp. 471 – 483.

[22] Y. Zhang: A Chaotic System Based Image Encryption Scheme with Identical Encryption and Decryption Algorithm, Chinese Journal of Electronics, Vol. 26, No. 5, September 2017, pp. 1022 – 1031.

[23] R. Zahmoul, R. Ejbali, M. Zaied: Image Encryption Based on New Beta Chaotic Maps, Optics and Lasers in Engineering, Vol. 96, September 2017, pp. 39 – 49.

[24] C .Han: An Image Encryption Algorithm Based on Modified Logistic Chaotic Map, Optik, Vol. 181, March 2019, pp. 779 – 785.

[25] S. Dhall, S. K. Pal, K. Sharma: A Chaos-Based Probabilistic Block Cipher for Image Encryption, Journal of King Saud University-Computer and Information Sciences, 2018.

[26] J. J. Montesinos-García, R. Martinez-Guerra: Colour Image Encryption via Fractional Chaotic State Estimation, IET Image Processing, Vol. 12, No. 10, October 2018, pp. 1913 – 1920.

[27] A. Akhavan, A. Samsudin, A. Akhshani: Cryptanalysis of an Image Encryption Algorithm Based on DNA Encoding, Optics & Laser Technology, Vol. 95, October 2017, pp. 94-99.

[28] S. Lian, J. Sun, Z. Wang: Security Analysis of a Chaos-Based Image Encryption Algorithm, Physica A: Statistical Mechanics and its Applications, Vol. 351, No. 2-4, June 2005, pp. 645 – 661.

[29] IEEE standard for binary Floating-Point Arithmetic, ANSI/IEEE std. 754, IEEE Computer Society, 1985.

[30] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, P. Natarajan: Local Shannon Entropy Measure with Statistical Tests for Image Randomness, Information Sciences, Vol. 222, February 2013, pp. 323 – 342.

[31] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, R. Amirtharajan: Chaos Based Crossover and Mutation for Securing DICOM Image, Computers in Biology and Medicine, Vol. 72, May 2016, pp. 170 – 184.

[32] Y. Wu, J. P. Noonan, S. Agaian: NPCR and UACI Randomness Tests for Image Encryption, Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April 2011, pp. 31– 38.