Journal of Information Security and Applications 46 (2019) 70–83

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Cryptographic construction using coupled map lattice as a diffusion model to enhanced security

professors AP

Subodh kumar[b], Rajendra kumar[b,*], Sushil kumar[c], Sunil Kumar[a,*]

[a] Institute of Informatics and Communication, University of Delhi, South Campus Benito Juarez Road, New Delhi 110021, India
[b] Dept. of Computer Science, Jamia Millia Islamia University, Delhi, India
[c] Shyam Lal College(M), University of Delhi, North Campus, Delhi, India

ARTICLE INFO

Article history:
Available online 11 March 2019

Keywords:
Intertwining logistic map
Coupled map lattice
Confusion
Diffusion
Encryption

ABSTRACT

In this study, a new color image encryption model that uses an intertwining logistic map based confusion mechanism and coupled map lattice based diffusion process. It incorporates mixing based on pseudo random number generator to ensure shuffling incase of same pixels, intertwining logistic map based confusion mechanism enhance the key sensitivity in the model. Finally, Couple map lattice based diffusion is utilized in the model to change the pixels in a way that even one-bit change in a pixel of plain image leads to a change in large number of pixels of the cipher image. The proposed encryption method enhance the security and results in better Number of pixel change rate (NPCR) and Unified average change intensity (UACI) scores. The correlation among the pixels of cipher image is reduced to be negligible. Corresponding results suggest that the proposed model is highly secure as compared with chaos based algorithms for image encryption application.

1. Introduction

Due to the advancement in the field of information and communication technology and medicine, the need of transferring medical images over the communication network has been increased drastically. Digital medical images play an important role in diagnosis and remedying diseases. Medical images contains the confidential, sensitive information of the patients [1–3]. An attacker can utilize these images for their personal usage i.e. fraudulent insurance and medical marketing, therefore protection of the medical images is the main concern. In the past, various technologies have been emerged to different types of medical images. In comparison with various technologies, encryption is the most effective way to transform medical images into unrecognized or cipher image. One can decrypt the cipher image only with correct secret key [4,5]. Recently, various image encryption models have been developed to secure medical information [6–12] and detailed suggestion are provided on the recent chaos based cryptosystems [13–17].

Hua et al., developed medical image encryption technique using high speed scrambling and pixel adaptive diffusion process. Random data is inserted in the plain image. Then to shuffle the image pixels and to spread the effect of random data over the entire image, two rounds of speed scrambling and pixel adaptive diffusion mechanism is applied respectively. Bitwise XOR and modulo arithmetic operation are performed to provide high efficiency in hardware platform and fast speed in software platform respectively [18]. Cao et al., presented an image encryption technique based on edge maps derived from a medical image. The method, first generate edge maps using various edge detectors and thresholds, then medical image is decomposed into different bit-planes. Each bit plain is XORed with the corresponding generated edge map. At the end bit-level scrambling is applied followed by pixel rearrangement [19]. Similarly, Laiphrakpam et al., proposed medical image encryption model based on improved ElGamal encryption scheme. The system uses Arnold's transformation to scramble the image. Then, to encrypt the medical image using Koblitz encoding technique based on elliptic curve coordinate [20]. Further, Laiphrakpam et al. [21] suggested a better way of security after proving the non-robustness in key generation method [22].

Another cryptographic model proposed by Ravichandran et al. [23], an medical image encryption model based on coupling of logistic-tent and logisticsine system. Both crossover and mutation processes were deduced to confuse and diffuse the image pixels respectively. Further, differential attacks analysis were performed to check the feasibility of the model. Ravichandran et al. [24] proposed a cryptographic model based on deoxyribo nucleic acid and chaotic maps. Multiple chaotic maps were utilized to generate

* Corresponding authors.
E-mail addresses: rkumar1@jmi.ac.in (R. kumar), sunilkumar104@gmail.com (S. Kumar).

https://doi.org/10.1016/j.jisa.2019.02.011
2214-2126/

random keys. Further permutation, encoding and diffusion were applied to the color image making it resistive against statistical and differential attacks.

To address the issues of existing cryptographic models of the protection of medical images, a new cryptographic model for better information security is proposed. It utilizes the well known confusion diffusion architecture. First, in the mixing process scaled random numbers are XORed with the image pixels to ensure the effectiveness of shuffling when all pixel values are same. Then shuffling and confusion process are performed to shuffle the positions of image pixels and to deduce the confusion among image pixels respectively. Finally, coupled map lattice based diffusion mechanism is introduced to diffuse image pixels. It helps in disseminating a change in single-bit to most of the image pixels and make the cipher image more sensitive to even a minor change in data or secret key. It is to be noted that the coupled map lattice based diffusion mechanism present pixel not only binds the previous pixel but also the next pixel and depends on the parameters μ and ϵ.

As compared with the existing chaotic dynamical systems, coupled map lattice has been investigated as a better diffusion model. Coupled map lattice provides the wide range of initial conditions and control parameters that further resulted into a larger keyspace. As CML has many space units that make the model highly efficient because it can be used in parallel for encryption and decryption. To encapsulate the properties of nonlinear dynamics, CML is utilized into the proposed cryptographic model as a diffusion model. Superiority of the CML is further explained in details [25–28]

The rest of the paper is organized as follows: In Section 2.1, Key generation and control parameters used are explained. In Section 2.2, intertwining logistic map and coupled map lattice is used in the proposed cryptographic model. In Section 2.3, mixing process using pseudo random number generator and shuffling process is discussed. Confusion algorithm based on intertwining logistic map and details of diffusion process using CML is given in Sections 2.4 and 2.5. Performance and security analysis to evaluate the key space, histogram, correlation, key sensitivity and differential attack etc. is done in Section 3. The last section provides the various results arrived at in the paper.

2. The design of coupled map lattice based image encryption algorithm

2.1. Key generation

A 280-bit long random binary secret key (K) is used to generate control parameters and initial conditions that are utilized in intertwining logistic map and coupled map lattice. This key is further divided into 35 blocks (K_1 to K_{35}) of 8-bits, to produce initial condition for intertwining logistic map and coupled map lattice.

$$K = K_1\ K_2\ K_3\ K_4 \ldots .\ K_{35} \tag{1}$$

$$\mu = 3.99 + ((K_2 + K_5) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{35}))\ mod\ 2)/100 \tag{2}$$

$$\epsilon = (((K_{24} + K_{19}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{35}))/(K_8 + K_{21}))\ mod\ 1 \tag{3}$$

$$x_1 = (((K_{35} + K_{11}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{35}))/(K_{32} + K_{12}))\ mod\ 1 \tag{4}$$

$$x_2 = (((K_{30}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{35}))/(K_{20} + K_{15}))\ mod\ 1 \tag{5}$$

$$x_3 = (((K_{21} + K_{19})\ \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{35}))/(1 + K_{30}))\ mod\ 1 \tag{6}$$

$$y_1 = (((K_{31} + K_{27}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{35}))/(K_{14} + K_{16}))\ mod\ 2 \tag{7}$$

$$y_2 = (((K_9 + K_{22}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{35}))/(K_{25} + K_{26}))\ mod\ 2 \tag{8}$$

$$y_3 = (((K_{34} + K_{33}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{35}))/(1 + K_{28}))\ mod\ 2 \tag{9}$$

$$S_f = K_1 \times K_{35} + (K_{21} \times K_{12})\ \oplus K_9 + 113 \tag{10}$$

Here $\oplus$ denotes bitwise XOR operation, $x_1, x_2, x_3, y_1, y_2, y_3$, $K_1,\ K_2, \ldots\ K_{35}$ are initial parameters and keys. From the above equations, it can be seen that the primary conditions and control parameters of intertwining logistic map are key dependent. keys = 2^280

Although many different parameters can be generated from single key (not practical for having smae formula)

2.2. Intertwining logistic map and coupled map lattice (CML)

Wang and Xu et al. [29], proposed an intertwining logistic map based on three dimensional logistic map. The three dimensional (3D) intertwining logistic map is mathematically expressed as: Intertwining logistic map equation

$$x_{n+1} = [\mu \times k_1 \times y_n \times (1 - x_n) + z_n]\ mod\ 1 \tag{11}$$

$$y_{n+1} = [\mu \times k_2 \times y_n + z_n \times (1 + x_{n+1}^2)]\ mod\ 1 \tag{12}$$

$$z_{n+1} = [\mu \times (y_{n+1} + x_{n+1} + k_3) \times \sin\ (z_n)]\ mod\ 1 \tag{13}$$

Where $0 < \mu \leq 3.999, |k_1| > 34.9, |k_2| > 38.9, |k_3| > 36.7$

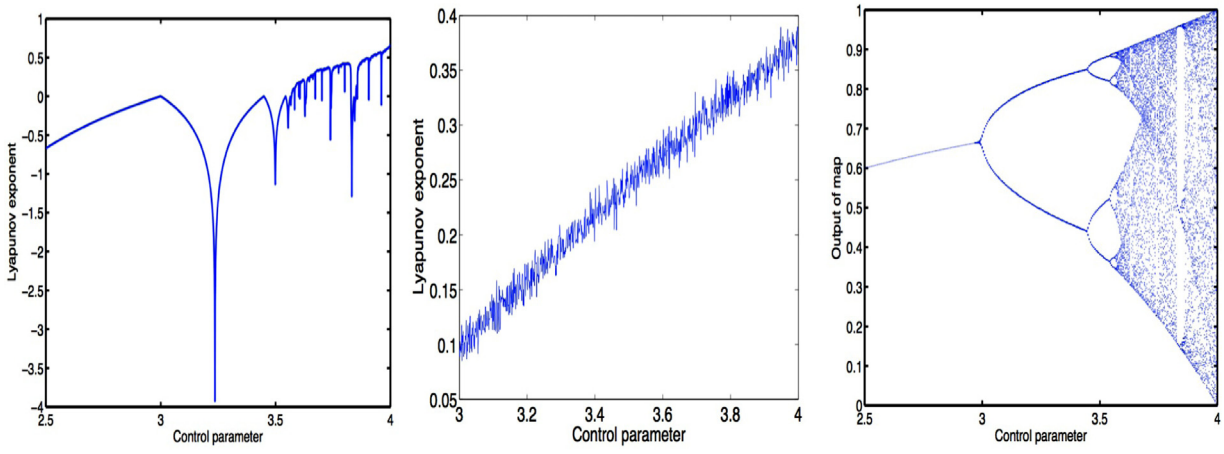
From the above equations, it is to be noted that output of one sequence depends upon the other two sequences. Intertwining logistic map uses more number of keys that results into large key space and also overcomes the problem of blank and stable window and uneven distributions of iterated sequences as shown in Fig. 1(c) for logistic map. As compare to logistic map, all the values of Lyapunov exponents for intertwining logistic map are positive [30,31] (Fig. 2).

Lyapunov exponent is used to measure the chaotic behavior of dynamical systems, and, a system is said to be chaotic in nature if it has positive lyapunov exponent.

From the above analysis of Lyapunov exponents and random sequence distribution, intertwining logistic map has turned out to be more complex, random and suitable for encryption. In the proposed cryptographic model, pseudo random key stream generated from the intertwining logistic map are used in mixing process to change the image pixel values. Hence mixing process makes the cipher image more reliant on intertwining logistic map.

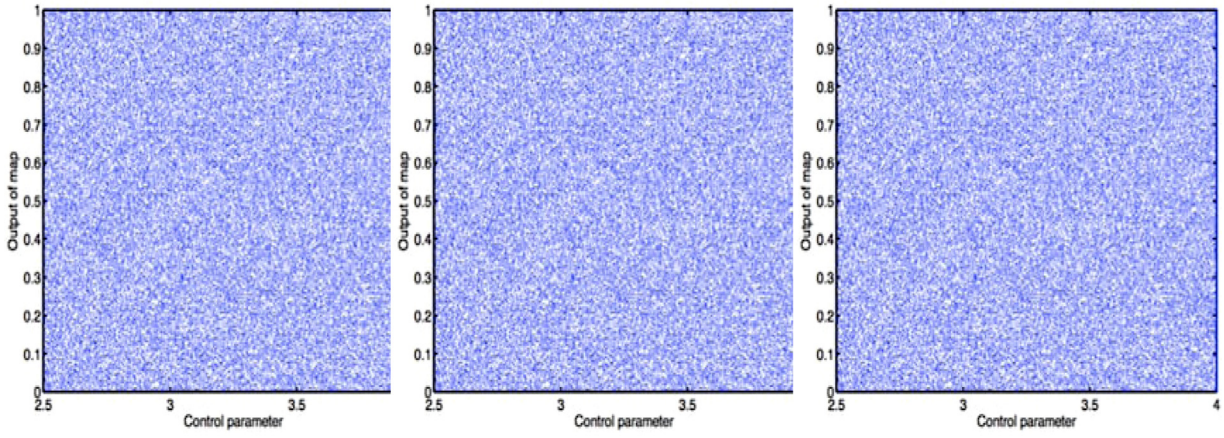
Chaotic maps are highly sensitive to initial condition due to their intrinsic features. Coupled map lattice (CML) is basically a type chaotic function that utilizes logistic map to generate the chaotic sequence. As compare to one-dimensional chaotic map based cryptographic system, CML system contains wide range of parameters, strong chaotic behaviour, less periodic window and better pseudo random chaotic sequences. Hence, it is to be noted that CML based generated pseudo random chaotic sequence is more secure as compared to one dimensional chaotic system. In the recent years, CML is widely utilized to develop image cryptosystems [32–39] due to excellent chaotic properties. The two dimensional CML is defined as [28,40]: This is 1d i think

$$x_{n+1}(k) = (1 - \epsilon) f(x_n(k)) + \frac{\epsilon}{2}[f(x_n(k-1)) + f(x_n(k+1))] \tag{14}$$



(a) (b) (c)

Fig. 1. (a) and (b) show the Lyapunov exponent for Logistic map with Control parameter $r = 3.998$ and Intertwining Logistic map with Control parameter $\mu = 3.999$. (c) shows the Bifurcation of logistic map.



(a) (b) (c)

Fig. 2. (a), (b) and (c) show Bifurcation of Intertwining Logistic map for $\mu = 3.999$, $k_1 = 34.913$, $k_2 = 38.942$, $k_3 = 36.709$, $x_0 = 0.361$, $y_0 = 0.259$ and $z_0 = 0.785$ for x, y and z output values respectively.

$$f(x) = 1 - \mu x^2 \tag{15}$$

Here, $f(x)$ is a mapping function, μ is constant ranges between 0 and 2. ϵ denotes the coupling coefficient and ranges between 0 and 1. For $\mu = 1.9$ and $\epsilon = 0.09$, CML shows the chaotic behavior. It is to be noted here that the effects of the number of lattices play a significant role in image encryption. CML substitutes the chaotic sequence to resist the statistical and differential attacks because mutual information for the chaotic sequence between lattices is not zero [41].

2.3. *Mixing and shuffling*

In the mixing process, the relationship between plain image pixels and the randomly generated keystream is made complex and interdependent. In the proposed mixing process, pixel values of the plain image are modified based on the pseudo random generated keystream using intertwining logistic map. Each pixel of the image is XORed with the keystream sequentially i.e. first pixel of the image is XORed with first value of the keystream and second pixel of the image is XORed with the second value of the keystream and so on. This process is repeated for all the pixels of the image respectively (Fig. 3).

Mathematically, the process of mixing is explained in equation given below:

$$P_{i+1} = P_i \oplus RNG_i \tag{16}$$

In the above process the range of i is taken as $i = 1$ to Size of image. P_i is the original image and RNG_i is the randomly generated key stream. The above mixing process, not only changes pixel values of the original image, but also make the cipher image more sensitive to key because each pixel of the image is altered with the keystream.

First, the color image is represented into one dimensional array and then converted into two dimensional matrix [42].

Step 1: First, Lozi map [43] based chaotic matrix is generated and further sorted in ascending order.

Step 2: Sorted pixel position is retained and further indexed column-wise.

Step 3: Then, Plain image pixels are represented in two dimensional matrix and shuffled using column-wise indexed matrix that was obtained earlier.

Step 4: Matrix obtained in row-wise sorting is sorted column-wise and sorted column-wise in ascending order.

Step 5: After that, position of the sorted matrix is retained and then further, sorted matrix is indexed row-wise.

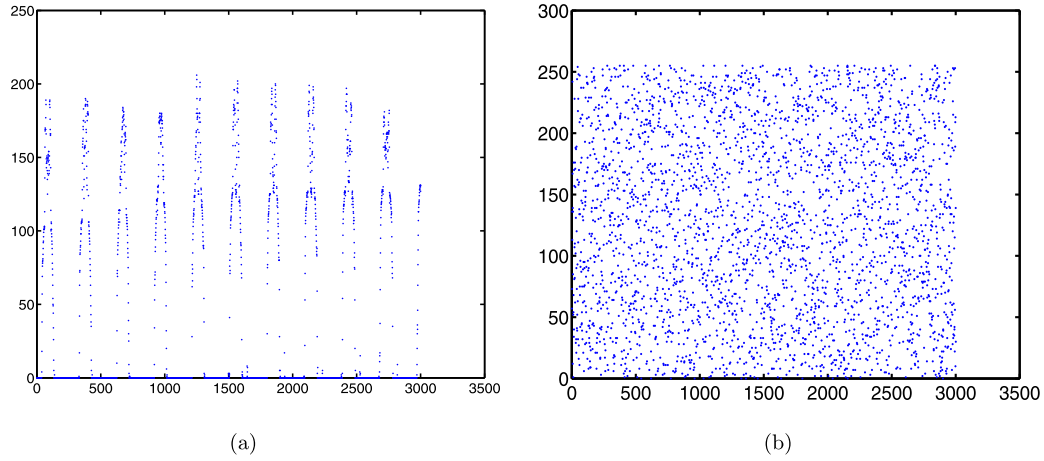


Fig. 3. It shows the result of shuffling process on numbers ranging from 0 to 3000. Original numbers are shown in (a) and shuffled numbers are shown in (b). Pixel values are represented on *y*-axis and their positions are represented on *x*-axis.

Step 6: Column-wise sorted matrix is further subjected to the shuffling based on row-wise indexed matrix.

This process is repeated for the complete matrix and finally resulted into shuffled matrix. In this process, two-tier shuffling (i.e. pixel positions are changed in both horizontal and vertical direction), is utilized to ensure the maximum confusion among the pixels of the image. Hence correlation among image pixels reduced and it helps in enhancing sensitivity and make the algorithm resistive against differential attacks.

2.4. Confusion

Confusion is a process in which each part of the ciphertext is made dependent not only on plain image but also on the several part of the secret key. It not only modify the image pixel values but also makes more complex relationship between plain and cipher image. In literature, many cryptosystems utilizes only initial condition and control parameters to generate the cipher image. Hence, one can retrieve the secret key using differential attack. In the proposed model following equation represent the confusion process that only utilized the secret key but also keystream generated using intertwining logistic map.

$$C_{i+1} = C_{i-1} \oplus K_i \oplus C_i \oplus ILM_i \quad (17)$$

is ki part of 280long secret key or 1d chaos ?

In the above process the range of i is taken as $i = 1$ to Size of the Image. This operation is performed bit-by-bit and lasts until all pixels of the image are computed according to the Eq. (17).

2.5. Diffusion

Diffusion is used to bind the image pixels with each other such that if any one-bit of the plain image, it affects most of pixels of the cipher-image. As neighboring pixels of the plain image poses high correlation. To reduce this correlation between adjacent pixels the diffusion process is applied. In literature, various diffusion model existed based on chaotic systems. In the proposed cryptographic model, CML is generated based on initial conditions x_1, x_2, x_3 and the parameters μ, and ϵ. The generated key stream is first scaled up using factor S_f. This operation is defined as follows [44]:

$$C_i = [(C_i \oplus C_{i-1}) + [CML_i \times S_f \ MOD \ 256] \oplus C_{i+1}] \ MOD \ 256$$

In the above process, the range of i = 1 to $M \times N \times 3$. C_i, C_{i-1} and C_{i+1} represent current pixel, previous pixel and next pixel of the image respectively. CML_i represent ith key stream generated using coupled map lattice and scaled up by factor S_f. The above coupled map lattice based diffusion process changes the statistical properties of the image by dispersing the effect of each pixel of the image over complete cipher image and makes it resistive against chosen and known plaintext attacks.

2.6. The proposed CML based cryptographic model

The proposed cryptographic model consists of the following five stages:

(*I*) Key generation process, (*II*) Mixing process, (*III*) Shuffling process, (*IV*) Confusion process, and (*V*) Diffusion process.

Step 1: First all the three Red, Green and Blue channels of the image are arranged into a linear array.

Step 2: A 280-bit external random key is generated using PRNG(Pseudo random number generator) and further initial conditions alongwith the parameters of the coupled map lattice and intertwining logistic map are generated.

Step 3: Intertwining logistic map based generated keystream of the same size of linear array is XORed with linear array of the image pixels obtained in Step 1.

Step 4: Array is represented into a matrix and Shuffled according to the shuffling process as explained in Section 2.3. It results into a matrix of mixed pixels.

Step 5: Then for the higher degree of confusion between pixels of the image, intertwining logistic map and secret key based confusion model is applied.

Step 6: In last, Coupled map lattice based diffusion process is applied. It spreads the change in a pixel to a large number of pixels of the image.

In the proposed coupled map lattice based diffusion model, a set of medical images and other color images are taken from SPIE-AAPM-NCI database for the simulation.

3. Simulation result and discussion

The proposed encryption model using a coupled map lattice based diffusion mechanism helps in secure transmission of plain image over the communication network. Each process utilized in the encryption model enhance the properties of the cipher image that makes the model resistive against statistical and differential attacks [45,46]. Secret key and cipher image were subjected to various security analysis that validate the robustness of the encryption model. Security analysis and corresponding results are explained in the following section as mentioned below.

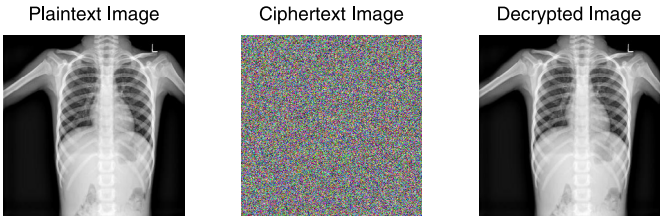


Fig. 4. Encryption and decryption of medical image.

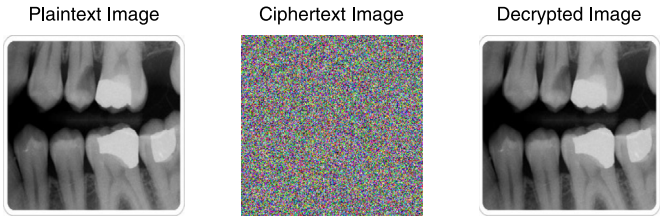


Fig. 5. Encryption and decryption of medical image.

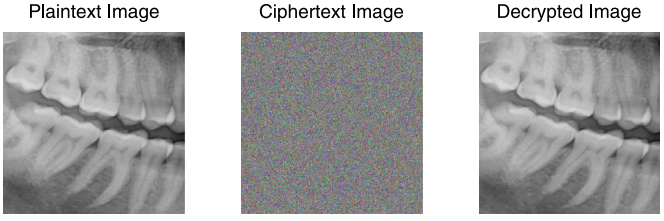


Fig. 6. Encryption and decryption of medical image.

3.1. Key space

The key space is basically defined as the total possible number of key combinations that is utilized in the encryption process. In the proposed cryptographic model a 280-bit long randomly generated secret key is used to generate initial condition and control parameters of coupled map lattice and intertwining logistic map. Here, a 280-bit long key is used, hence the key space is 2^{280}, which is good enough to withstand brute force attacks. For secure cryptographic systems, key space should be greater than 2^{100} [47].

3.2. Key sensitivity analysis

Key sensitivity is the most significant feature in each cryptographic model. It indicates the change in cipher image when plain image is encrypted with one-bit change in secret key. One-bit change should brought-out a significant change in the output cipher image. Here five secret keys (K_1, K_2, K_3, K_4, K_5) with one-bit difference are used to check the sensitivity of the model.

$K_1 = [7retwsywzxwer23456klhgyrte68789dgcdhjguipu7zmnbcadfghqwiuyt785];$
$K_2 = [7retwsywzxwer23456klhgyrte68789dgcdhjguipu7zmnbcadfghqwiuyt786];$
$K_3 = [7retwsywzxwer23456klhgyrte68789dgcdhjguipu7zmnbcadfghqwiuyt745];$
$K_4 = [7retwsywzxwer23456klhgyrte68789dgcdhjguipu7zmnbcadfghqwiuyt385];$
$K_5 = [7retwsywzxwer23456klhgyrte68789dgcdhjguipu7zmnbcadfghqwiuyu785];$

Fig 16(a)–(e) shows the encrypted image with one-bit difference in secret keys K_1, K_2, K_3, K_4 and K_5. Fig 16 (f)–(i) shows the difference images using keys K_1 and K_2, K_1 and K_3, K_1 and K_4, K_1 and K_5 respectively. One can notice that one-bit change in secret key results in completely different cipher image.

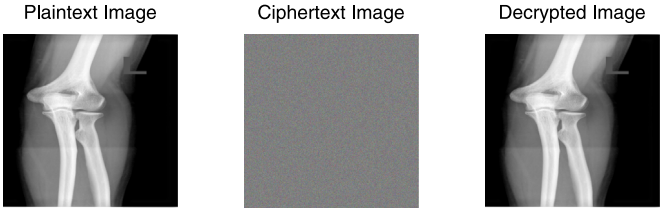


Fig. 7. Encryption and decryption of medical image.

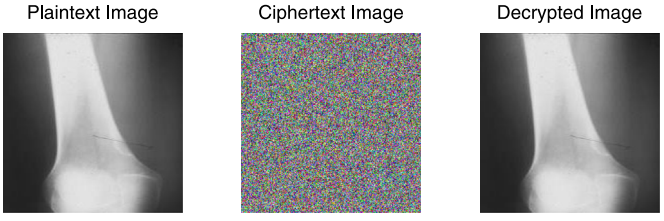


Fig. 8. Encryption and decryption of medical image.

Fig. 9. Encryption and decryption of medical image.

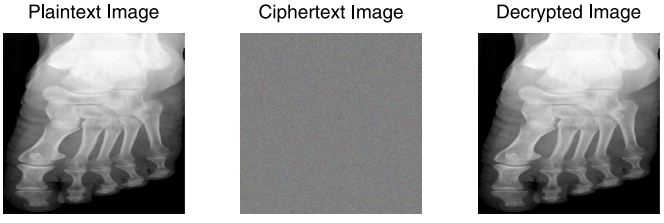


Fig. 10. Encryption and decryption of medical image.

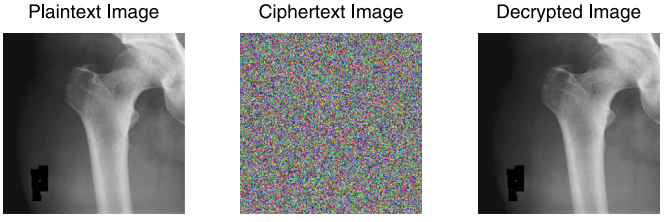


Fig. 11. Encryption and decryption of medical image.

3.3. Histogram analysis

A histogram plot indicates the distribution of pixel values of an image. A flat and uniform distribution of pixels resist the cipher

Table 1
Histogram uniformity assessment for different ciphertext images based on (χ^2) test.

Metrics	Fig. 17	Fig. 18	Fig. 19	Fig. 20	Fig. 21	Fig. 22	Fig. 23	Fig. 24
P value	0.3312	0.4438	0.5098	0.4157	0.4765	0.3890	0.4991	0.3689
($H = 0$ or 1)	0	0	0	0	0	0	0	0
Decision	A	A	A	A	A	A	A	A

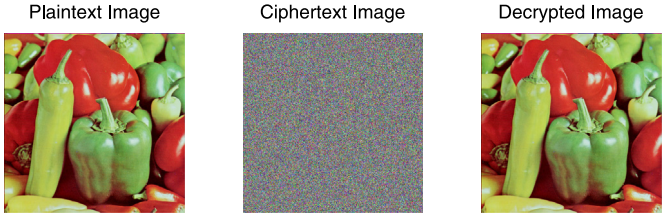


Fig. 12. Encryption and decryption of color image.

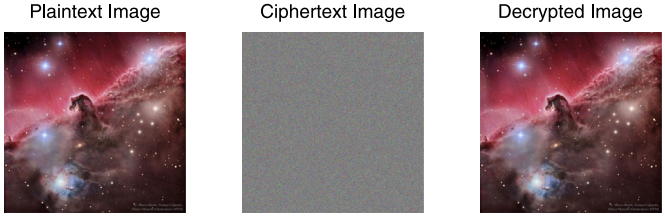


Fig. 13. Encryption and decryption of color image.

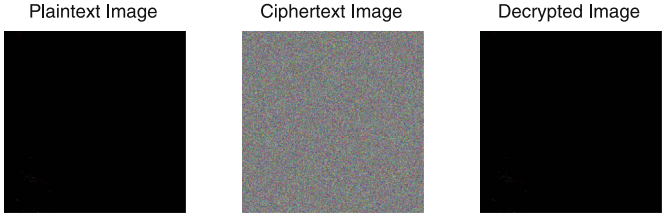


Fig. 14. Encryption and decryption of black image.

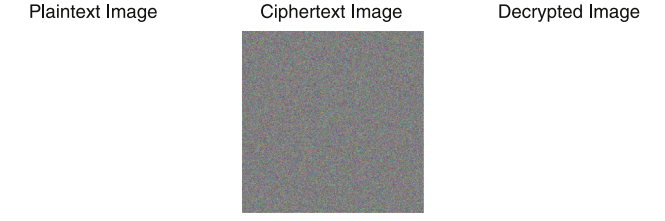


Fig. 15. Encryption and decryption of white image.

image against any frequency or statistical attack. A good cryptographic model must ensure to maintain a uniform distribution of pixels in a histogram.

Figs. 17–24 shows histograms of plaintext image, cipher image and decrypted image. One can clearly visualize that the histograms of cipher images are flat and uniformly distributed. It makes the proposed model resistive against statistical attacks.

Further, uniformity of the ciphertext image histogram is analyzed using chi-square (χ^2) test and summarized in Table 1. It is to be noted from the table that CML based diffusion model accept the null hypothesis and all value of $p > 0.05$ that prove the flat and uniform distribution of image pixels. Letter 'A' used in the table denotes Accepted.

3.4. Correlation analysis

Correlation analysis test is used to evaluate the resistance of cryptographic model against statistical attacks. In general, correlation among adjacent pixels in meaningful or original image is very high. A cryptographic model is employed to reduce the correlation among adjacent pixels in cipher or transmitted image and it should approach to 0 for better cryptosystems.

The correlation coefficient r_{xy} is calculated between two adjacent pixels of the image as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{18}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{19}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{20}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{21}$$

Here x and y represent gray level values of two adjoining pixels of the image. N represent total number of pixels, $E(x)$ and $E(y)$ represent mean values of x_i and y_i respectively. Fig. 25 and 26 shows the correlation coefficient in cipher image for different values of coupled map lattice parameter μ.

Tables 2–4 shows the correlation coefficients in cipher images for each channel separately for different values of CML control parameter μ. It can notice that the CML based diffusion model successfully reduce the correlation among adjacent of the cipher image that makes the model resistive against statistical attacks. O-HR, O-HB and O-HG represent correlation coefficients in original image for red, green and blue channel in horizontal direction, O-VR, O-VB and O-VG represent correlation coefficients in original image for red, green and blue channel in vertical direction, O-DR, O-DB and O-DG represent correlation coefficients in original image for red, green and blue channel in diagonal direction. 1.88, 1.89 and 1.90 are different values of control parameter μ.

3.5. Differential attack

To check the resistivity of the proposed CML based diffusion model against differential attacks, a small change is done in the plain or original image. Then original and modified image is encrypted using the proposed model. Both the encrypted image are compared to derive a relationship between them. NPCR (Number of pixel change rate) and UACI (Unified average change intensity) scores are calculated to analyze the differential attack. NPCR and UACI score are calculated to find-out the image difference as follows:

$$NPCR = \frac{\sum_{i,j} Diff(i,j)}{W \times H} \times 100\% \tag{22}$$

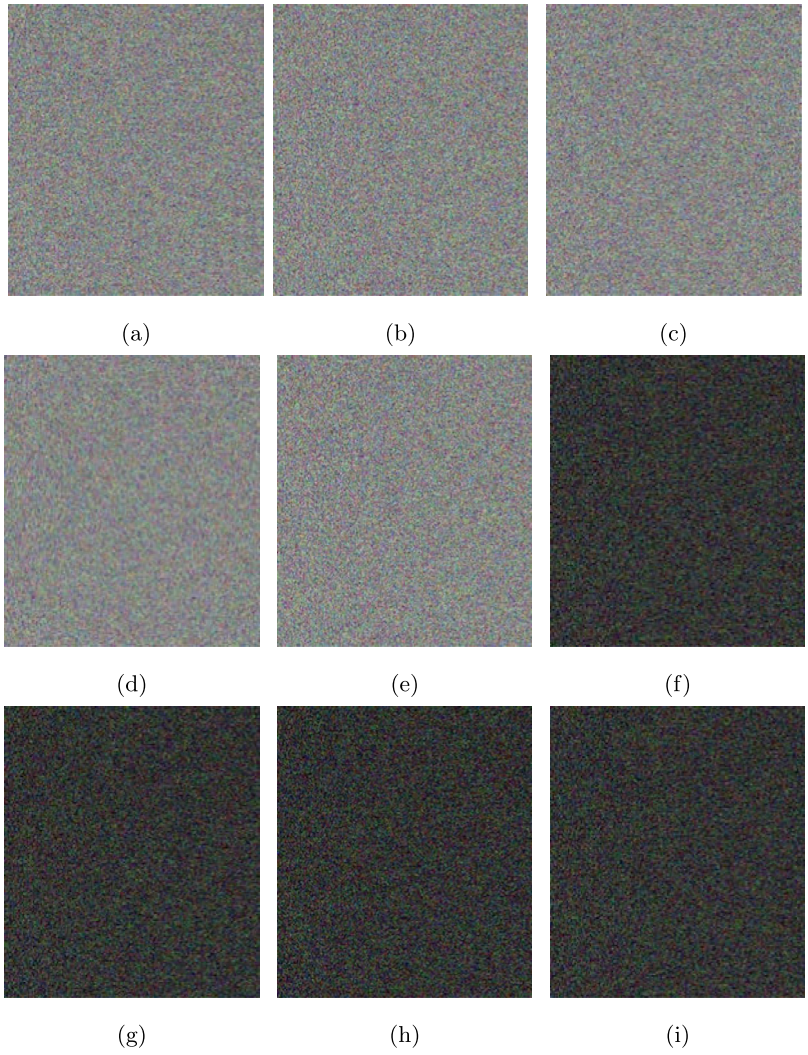


Fig. 16. Key sensitivity analysis for proposed cryptographic system. (a) C_1 using key K_1 (b) C_2 using key K_2 (c) C_3 using key K_3 (d) C_4 using key K_4 (e) C_5 using key K_5 (f) difference of $C_1 - C_2$ using key K_1 and K_2 (g) difference of $C_1 - C_3$ using key K_1 and K_3 (h) difference of $C_1 - C_4$ using key K_1 and K_4 (i) difference of $C_1 - C_5$ using key K_1 and K_5.

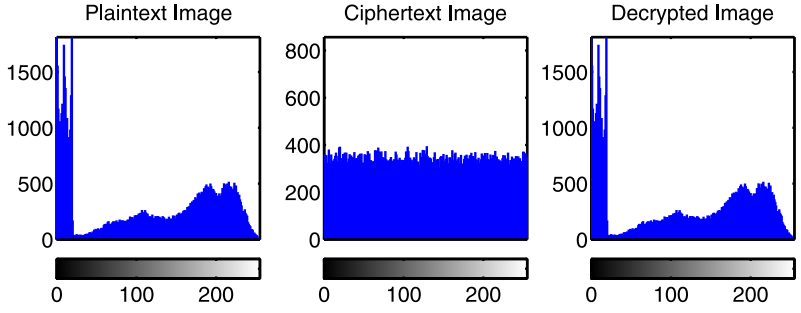


Fig. 17. Histogram of the medical image shown in Fig. 4.

$$UACI = \frac{\sum_{i,j} \frac{Cip(i,j) - Cip'(i,j)}{255}}{W \times H} \times 100\% \quad (23)$$

Here width and height of images are represented by W and H respectively. There is one pixel difference between Cip and Cip' image.

$Diff$ is defined as follows:

If $Cip(i, j) = Cip'(i, j)$ then $Diff(i, j) = 0$; else $Diff(i, j) = 1$.

Table 5, 6 shows the UACI and NPCR score for various images with a variation in CML control parameter μ.

3.6. Information entropy

The degree of uncertainity of an image is measured using information entropy which is described by Shannon 's theory in the euation given below:

$$H(s) = \sum_{i=0}^{2^N - 1} P(s_i)\ log_2 P(s_i) \quad (24)$$

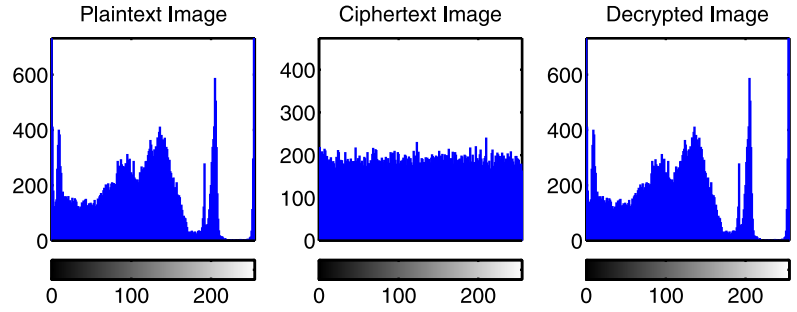


Fig. 18. Histogram of the medical image shown in Fig. 5.

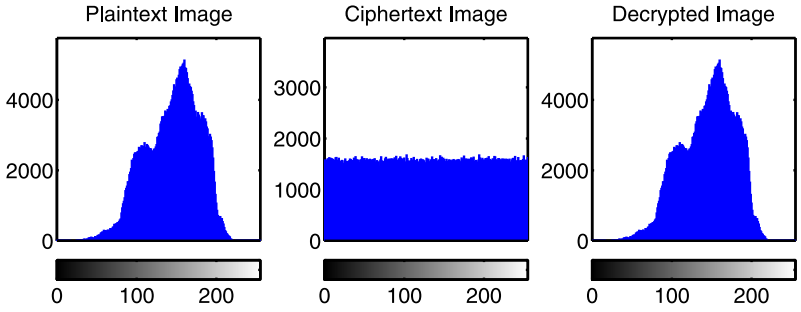


Fig. 19. Histogram of the medical image shown in Fig. 6.

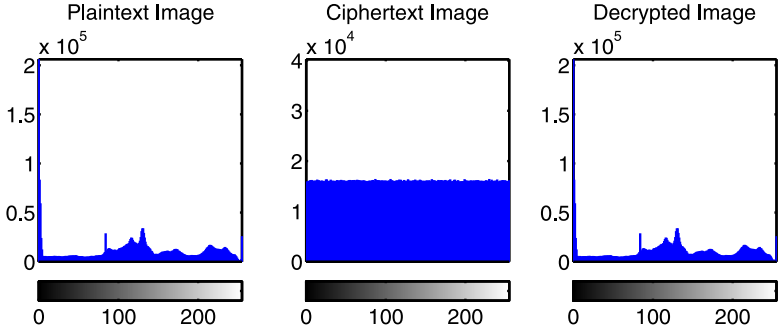


Fig. 20. Histogram of the medical image shown in Fig. 7.

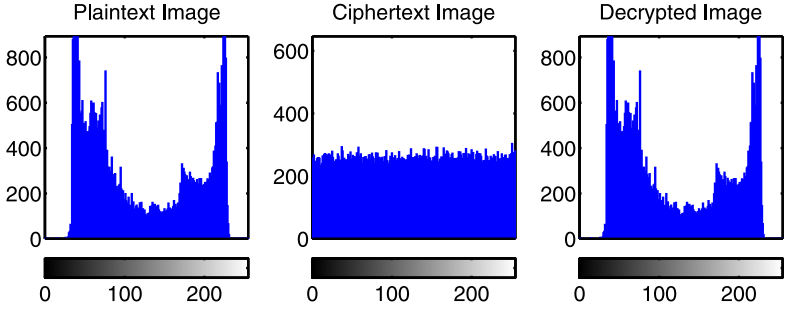


Fig. 21. Histogram of the medical image shown in Fig. 8.

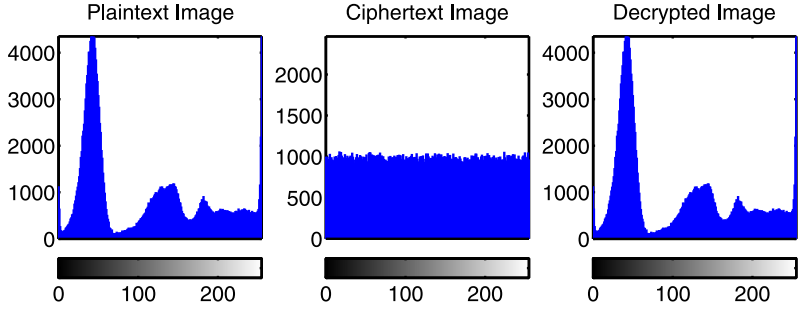


Fig. 22. Histogram of the medical image shown in Fig. 9.

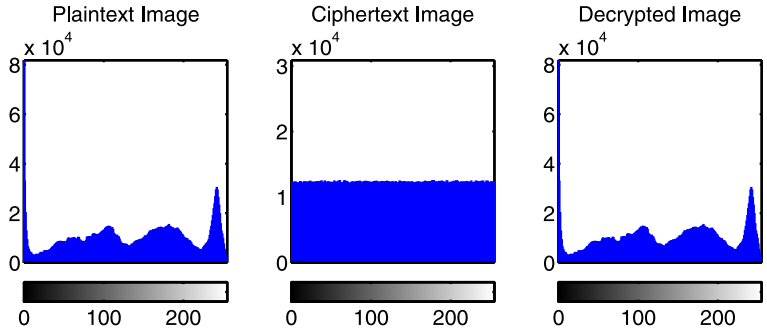


Fig. 23. Histogram of the medical medical image shown in Fig. 10.

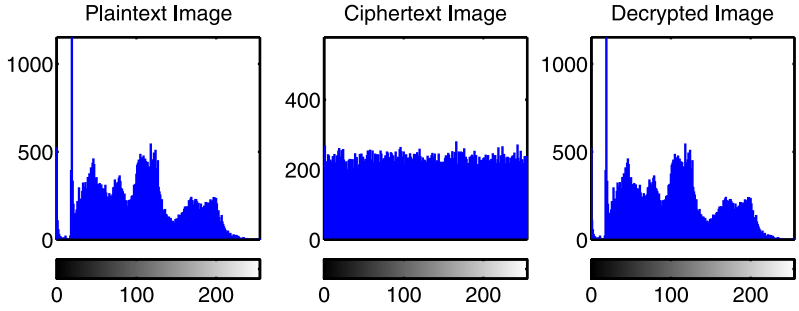


Fig. 24. Histogram of the medical image shown in Fig. 11.

Table 2
Correlation coefficients of adjoining pixels in original and cipher image using proposed cryptographic model for red channel at different value of CML parameter μ.

Direction	Fig. 17	Fig. 18	Fig. 19	Fig. 20	Fig. 21	Fig. 22	Fig. 23	Fig. 24
O-HR	0.9786	0.9761	0.9891	0.9599	0.9868	0.9562	0.9265	0.9345
1.88-HR	0.0013	0.0019	0.0008	−0.0013	−0.0041	−0.0032	0.0004	−0.0011
1.89-HR	0.0003	0.0021	−0.0007	−0.0015	−0.0038	−0.0041	−0.0021	0.0006
1.90-HR	0.0002	0.0025	0.0003	−0.0041	0.0008	−0.0043	0.0007	−0.0018
O-VR	0.9820	0.9567	0.9880	0.9567	0.9765	0.9890	0.9991	0.9689
1.88-VR	−0.0005	0.0001	0.0015	0.0011	−0.0012	0.0022	−0.0017	0.0004
1.89-VR	−0.0006	0.0004	0.0007	−0.0023	0.0002	−0.0044	−0.0015	0.0005
1.90-VR	−0.0008	−0.0002	0.0011	0.0007	−0.0022	−0.0033	−0.0028	0.0001
O-DR	0.9694	0.9438	0.9871	0.9157	0.9705	0.9810	0.9997	0.9739
1.88-DR	0.0021	0.0012	0.0011	0.0004	0.0005	0.0002	−0.0018	0.0016
1.89-DR	0.0017	−0.0005	−0041	0.0021	0.0013	−0.0041	−0.0000	0.0004
1.90-DR	0.0010	0.0003	−0.0032	−0.0023	0.0011	−0.0017	0.0000	−0.0021

Table 3
Correlation coefficients of adjoining pixels in original and cipher image using proposed cryptographic model for green channel at different value of CML parameter μ.

Direction	Fig. 17	Fig. 18	Fig. 19	Fig. 20	Fig. 21	Fig. 22	Fig. 23	Fig. 24
O-HG	0.9791	0.9750	0.9877	0.9899	0.9998	0.9652	0.9475	0.9715
1.88-HG	0.0010	0.0013	0.0011	−0.0010	−0.0031	−0.0012	0.0024	−0.0031
1.89-HG	0.0001	0.0011	−0.0027	−0.0035	−0.0018	−0.0021	−0.0033	0.0002
1.90-HG	0.0012	0.0020	0.0013	−0.0011	0.0003	−0.0013	0.0004	−0.0026
O-VG	0.9767	0.9987	0.9990	0.9689	0.9876	0.9910	0.9271	0.9376
1.88-VG	−0.0021	0.0003	0.0025	0.0001	−0.0019	0.0012	−0.0037	0.0001
1.89-VG	−0.0003	0.0014	0.0017	−0.0003	0.0004	−0.0014	−0.0010	0.0015
1.90-VG	−0.0001	−0.0007	0.0001	0.0000	−0.0020	−0.0003	−0.0018	0.0002
O-DG	0.9894	0.9932	0.9611	0.9555	0.9935	0.9615	0.9817	0.9919
1.88-DG	0.0011	0.0002	0.0001	0.0024	0.0012	0.0001	−0.0038	−0.0046
1.89-DG	−0.0007	0.0035	0.0001	−0.0031	−0.0023	0.0001	0.0010	−0.0014
1.90-DG	−0.0000	−0.0030	0.0002	0.0003	−0.0005	0.0010	−0.0020	0.0013

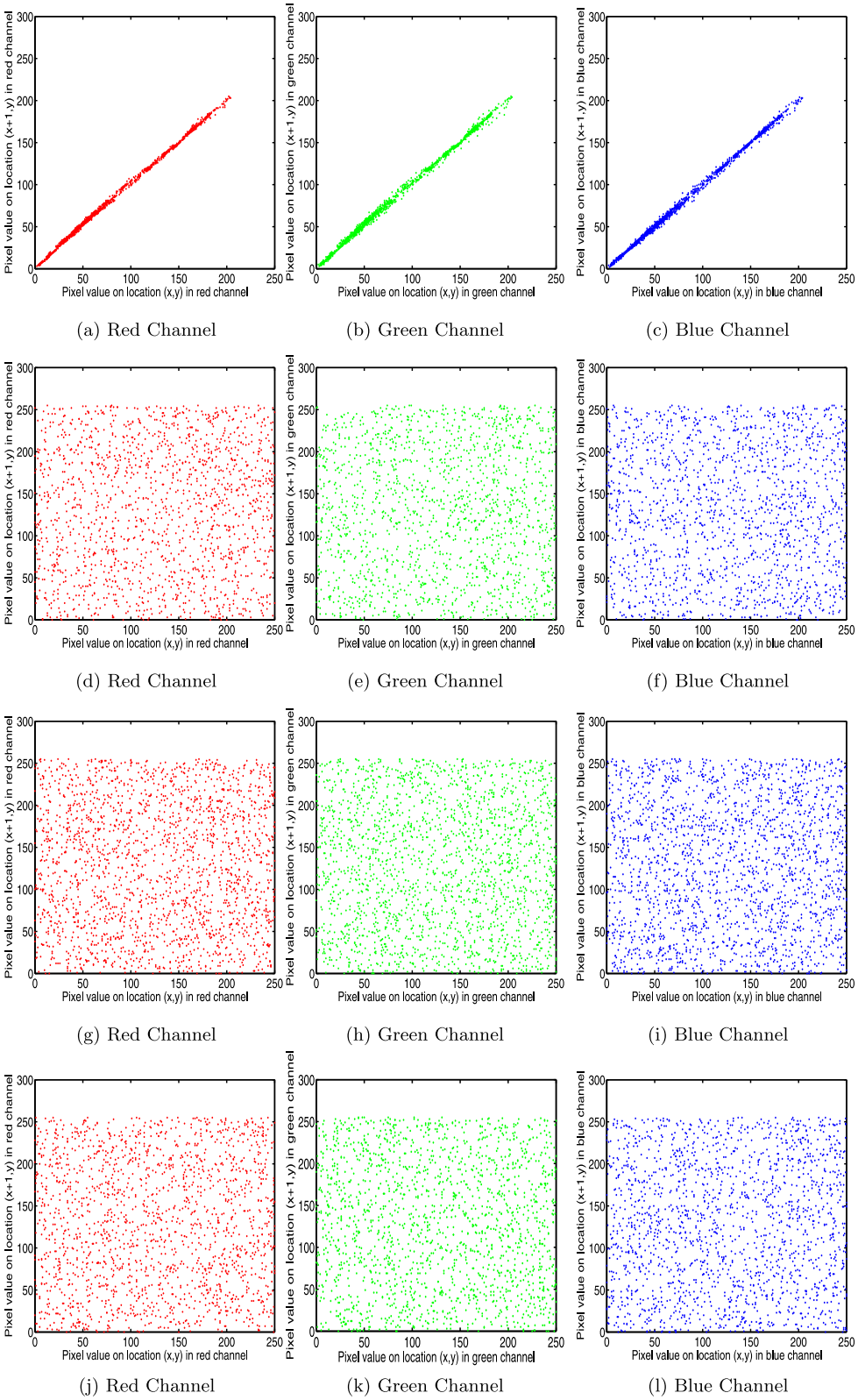
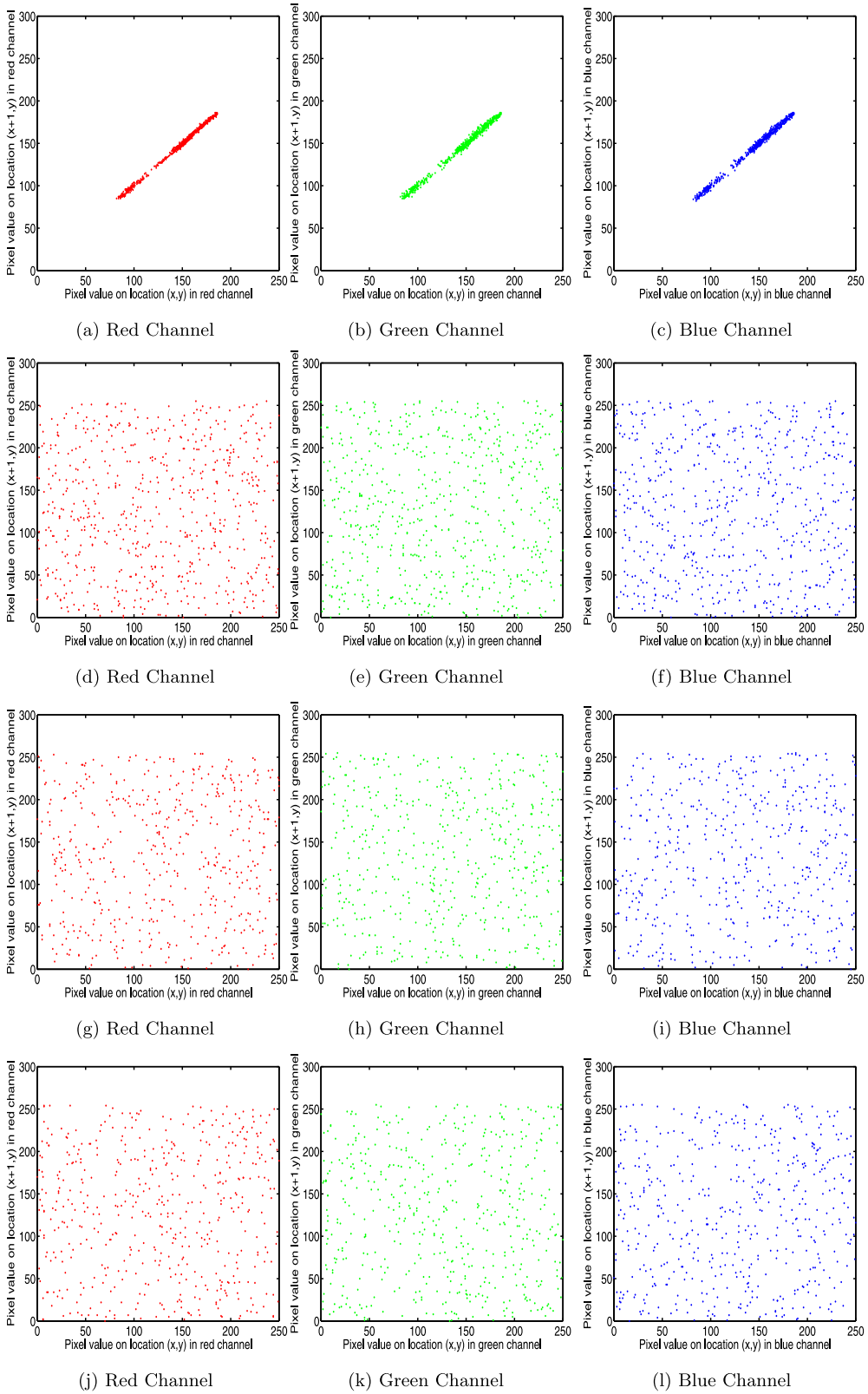


Fig. 25. Horizontal, vertical and diagonal direction correlations of two adjoining pixels for Plaintext Image shown in Fig. 12.



(a) Red Channel (b) Green Channel (c) Blue Channel

(d) Red Channel (e) Green Channel (f) Blue Channel

(g) Red Channel (h) Green Channel (i) Blue Channel

(j) Red Channel (k) Green Channel (l) Blue Channel

Fig. 26. Horizontal, vertical and diagonal direction correlations of two adjoining pixels for Plaintext Image shown in Fig. 13.

Where, Information entropy is denoted by $H(s)$, s represent the information source, N represent the total number of bits in a symbol and $P(s_i)$ represent the probability of finding s_i.

Table 7 shows the information entropy using the proposed cryptographic model for varying CML control parameter μ.

Local shannon entropy was introduced in [48] to evaluate the randomness of the images. Random Non-overlapping blocks are selected to compute the local shannon entropy test.

From the Table 8, one can notice that calculated local shannon entropy of the cipher images are close to 8 ($7.9996 \approx 8$). Hence, it

Table 4
Correlation coefficients of adjoining pixels in original and cipher image using proposed cryptographic model for blue channel at different value of CML parameter μ.

Direction	Fig. 17	Fig. 18	Fig. 19	Fig. 20	Fig. 21	Fig. 22	Fig. 23	Fig. 24
O-HB	0.9987	0.9972	0.9843	0.9313	0.9645	0.9899	0.9567	0.9768
1.88-HB	0.0010	0.0009	0.0022	0.0003	0.0001	0.0012	−0.0044	0.0004
1.89-HB	−0.0023	0.0002	−0.0017	0.0005	0.0008	0.0001	0.0034	0.0002
1.90-HB	0.0011	0.0005	−0.0001	0.0011	0.0018	0.0013	0.0003	0.0010
O-VB	0.9654	0.9987	0.99720	0.9874	0.9989	0.9961	0.9546	0.9432
1.88-VB	0.0015	−0.0011	0.0002	−0.0021	0.0001	−0.0002	0.0007	−0.0014
1.89-VB	0.0003	0.0011	−0.0017	0.0003	0.0022	0.0002	0.0010	−0.0015
1.90-VB	−0.0012	0.0003	0.0001	0.0017	−0.0012	0.0013	0.0008	−0.0031
O-DB	0.9987	0.9567	0.9921	0.9365	0.9874	0.9990	0.9797	0.9719
1.88-DB	0.0011	0.0000	−0.0000	0.0014	0.0015	0.0022	0.0002	−0.0036
1.89-DB	0.0007	−0.0025	−0001	0.0021	−0.0033	0.0011	−0.0023	0.0015
1.90-DB	0.0001	0.0007	0.0012	0.0003	0.0001	0.0001	−0.0030	−0.0011

Table 5
NPCR score for different images with varying CML control parameter μ.

Image	$\mu = 1.88$	$\mu = 1.89$	$\mu = 1.90$
Fig. 4	99.81	99.87	99.86
Fig. 5	99.85	99.70	99.83
Fig. 6	99.89	99.79	99.91
Fig. 7	99.93	99.92	99.89
Fig. 8	99.91	99.90	99.92
Fig. 9	99.80	99.82	99.94
Fig. 10	99.86	99.88	99.80
Fig. 11	99.90	99.81	99.82
Fig. 12	99.87	99.84	99.81
Fig. 13	99.91	99.86	99.89
Fig. 14	99.80	99.83	99.85
Fig. 15	99.92	99.84	99.87

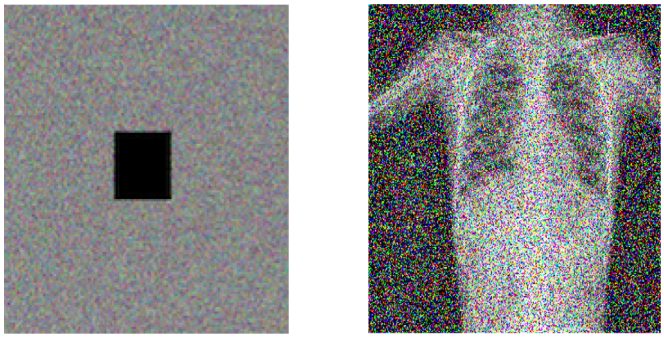
Table 6
UACI score for different images with varying CML control parameter μ.

Image	$\mu = 1.88$	$\mu = 1.89$	$\mu = 1.90$
Fig. 4	33.13	33.34	33.21
Fig. 5	33.29	33.14	33.38
Fig. 6	33.43	33.24	33.36
Fig. 7	33.25	33.27	33.29
Fig. 8	33.20	33.19	33.45
Fig. 9	33.53	33.18	33.27
Fig. 10	33.49	33.17	33.36
Fig. 11	33.41	33.31	33.20
Fig. 12	33.40	33.44	33.25
Fig. 13	33.38	33.33	33.40
Fig. 14	33.37	99.29	33.39
Fig. 15	33.46	33.42	33.38

can be concluded from the above table that information generated by the proposed model is highly random or unpredictable.

3.7. Cropping test

Robustness of the proposed coupled map lattice based diffusion model is examine using crop test where a block of cipher image is replaced with all zero pixels [49]. During the transfer of information over the communication network, crop attacks occurs. In this model cipher is cropped with a window size 125×125 during the transmission process. From Fig. 27 (a–b), it is to be notice that most of pixels of distorted image pixels are extracted and one can easily recognize the cipher image. The calculated PSNR (Peak Signal to Noise ratio) value is 31.9599 db (Fig. 28).



(a) (b)

Fig. 27. Crop test shows low-level distortion spread over cipher image.

3.8. Compression

In data transmission over the communication network, compression is most desired operation due to bandwidth limitation. Data is gone through encoding process to reduce the its size. In the proposed CML based diffusion model, JPEG lossless compression test is performed. It is to be visualize from the simulation results that, if image is compressed for compression ratio ≥ 4.7819, most of decrypted image pixels are distorted and decrypted image is completely lost for the compression ratio ≥ 28.8427. Finally, one can conclude from the above compression test that proposed CML based diffusion model is robust against lossless compression.

The proposed coupled map lattice based diffusion model for image encryption is compared with other existing algorithms. From the Table 9, one can notice that proposed model performs better as compared to models based on Genetic, Genetic-DNA, Genetic-CML and WDICA (weighted discrete imperialist competitive algorithm).

3.9. Time cost comparison

In Table 10 time cost comparison of different cryptographic algorithms with different image size for the same computing envi-

Table 7
Information entropy for different images with varying CML control parameter μ.

Image	Fig. 17	Fig. 18	Fig. 19	Fig. 20	Fig. 21	Fig. 22	Fig. 23	Fig. 24
Original image	7.7832	7.6586	7.7103	6.4812	7.7665	7.7798	7.6134	7.823
$\mu = 1.88$	7.9992	7.9988	7.9981	7.9979	7.9968	7.9992	7.9995	7.9991
$\mu = 1.89$	7.7993	7.9990	7.9984	7.9989	7.9980	7.9995	7.9991	7.9987
$\mu = 1.90$	7.7992	7.9994	7.9991	7.9998	7.9986	7.9993	7.9989	7.9996

Table 8
The Local Shanon entropy test of the ciphertext images generated using proposed cryptographic model. Number of pixels $Tb = 1936$.

Image	Fig. 17	Fig. 18	Fig. 19	Fig. 20	Fig. 21	Fig. 22	Fig. 23	Fig. 24
$K = 30$	7.9994	7.9998	7.9996	7.9997	7.9994	7.9998	7.9997	7.9993
$K = 40$	7.9993	7.9998	7.9991	7.9999	7.9998	7.9996	7.9995	7.9998

Table 9
Comparision of Proposed cryptographic model with other models for various parameters.

Algorithm	Correlation coefficient			Entropy	NPCR	UACI
	R	G	B			
Proposed model	0.0020	0.0012	0.0011	7.9992	0.998501	0.333401
Ref. [50]	0.0031	0.0029	0.0013	7.9992	0.992592	0.331834
Ref. [51]	0.0035	0.0002	−0.0013	7.9907	0.756256	0.348651
Ref. [52]	0.0039	0.0041	0.0008	7.9993	0.991074	0.331085
Ref. [53]	0.0062	0.0106	0.0015	7.9983	0.990383	0.329283
Ref. [54]	0.0149	0.0210	0.0062	7.9951	0.986273	0.316822

Table 10
Speed comparison for different image size on Matlab 7.0.

Image size	System characteristics	Ref. [14]	Ref. [55]	Ref. [56]	Proposed
(256 × 256)	Core (TM) CPU 2.30 GHz	0.03900	0.30420	0.07020	0.03300
(512 × 512)	Core (TM) CPU 2.30 GHz	0.15600	1.15441	0.25740	0.14100
(1024 × 1024)	Core (TM) CPU 2.30 GHz	0.56940	4.63323	0.99841	0.46660

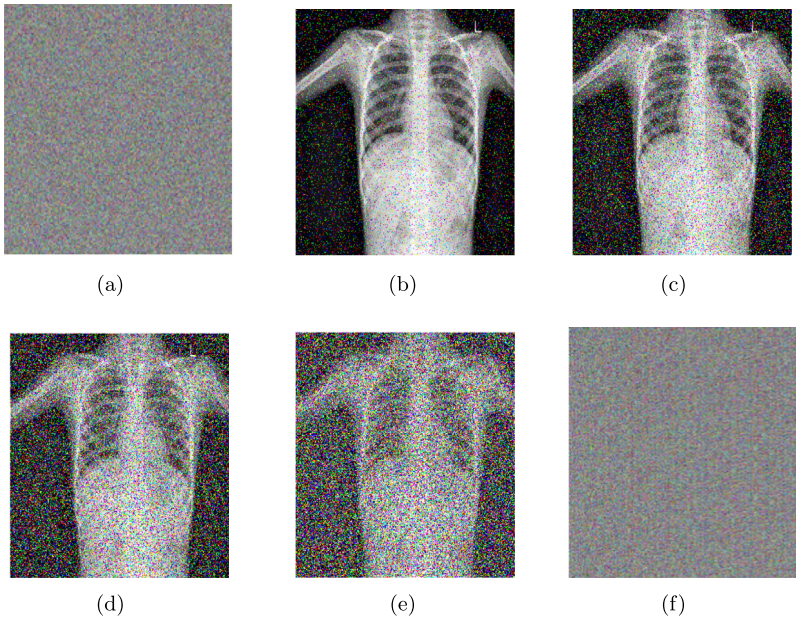


Fig. 28. JPEG lossless compression test. (a) Cipher image, (b) Resulted image for compression ratio ≥ 4.7819, (c) Resulted image for compression ratio ≥ 9.8826, (d) Resulted image for compression ratio ≥ 14.2889, (e) Resulted image for compression ratio ≥ 17.8025, (f) Resulted image for compression ratio ≥ 28.8427.

ronment is mentioned [14]. It is to be noted from the data given in Table 10 that proposed cryptographic model performs better as compared to other methods.

4. Conclusion

In this paper, Coupled map lattice based diffusion model is deduced to secure medical images. Multiple randomly generated secret key are used to analyze the proposed cryptographic model for various medical images. The proposed cryptographic model works effectively in different test cases like lossless compression, noise addition to the cipher image or wrong key etc. Performance and security analysis is carried out using key sensitivity, crop test, histogram analysis, keyspace analysis, correlation coefficient analysis and differential attacks. Robustness of the model against differential attacks is ensured based on zero or negligible correlation among cipher image pixels and an average NPCR 99.85 score. Further, the model is also analyzed for different control parameter value μ, with the higher value $\mu = 1.90$ is most appropriate in the diffusion model. It is to be noted from the obtained results that proposed coupled map lattice based diffusion model performs better as compared to other cryptosystems and can transfer image in more reliable and secured way over the communication network.

Acknowledgement

The author acknowledges the support provided by the Jamia Millia Islamia University for this research work. Subodh Kumar acknowledges with thanks to UGC for financial support under UGC-Ref.No: 3482/(SC)(NET-NOVEMBER 2017).

References

[1] Lacoste C, Lim JH, Chevallet JP, Le DTH. Medical-image retrieval based on knowledge-assisted text and image indexing. IEEE Trans Circuits Syst Video Technol 2007;17(7):889–900. doi:10.1109/TCSVT.2007.897114.

[2] Zinger S, Ruijters D, Do L, de With PHN. View interpolation for medical images on autostereoscopic displays. IEEE Trans Circuits Syst Video Technol 2012;22(1):128–37. doi:10.1109/TCSVT.2011.2158362.

[3] A secured cryptographic model using intertwining logistic map. Procedia Comput Sci 2018;143:804–11 8th International Conference on Advances in Computing Communications (ICACC-2018). doi:10.1016/j.procs.2018.10.386.

[4] Kumar S, Kumar M, Das MK, Singh S, Budhiraja R. Improved cryptographic model for better information security. In: 2017 International conference on information and communication technology convergence (ICTC); 2017. p. 406–10. doi:10.1109/ICTC.2017.8191013.

[5] Kumar M, Kumar S, Das MK, Singh S, Budhiraja R. Chaotic dynamical systems based image encryption model. In: 2017 International conference on information and communication technology convergence (ICTC); 2017. p. 93–8. doi:10.1109/ICTC.2017.8190949.

[6] Zanin M, Pisarchik AN. Gray code permutation algorithm for high-dimensional data encryption. Inf Sci 2014;270:288–97. doi:10.1016/j.ins.2014.02.131.

[7] L M, S MCV. A survey on protection of medical images. In: 2015 International conference on control, instrumentation, communication and computational technologies (ICCICCT); 2015. p. 503–6. doi:10.1109/ICCICCT.2015.7475331.

[8] Hua Z, Zhou Y. Design of image cipher using block-based scrambling and image filtering. Inf Sci 2017;396:97–113. doi:10.1016/j.ins.2017.02.036.

[9] Kumar C, Singh AK, Kumar P. A recent survey on image watermarking techniques and its application in e-governance. Multimed Tools Appl 2018;77(3):3597–622. doi:10.1007/s11042-017-5222-8.

[10] Liu J, Ma Y, Li S, Lian J, Zhang X. A new simple chaotic system and its application in medical image encryption. Multimed Tools Appl 2018. doi:10.1007/s11042-017-5534-8.

[11] Ravichandran D, Rajagopalan S, Upadhyay HN, Rayappan JBB, Amirtharajan R. Encrypted biography of biomedical image - a pentalayer cryptosystem on FPGA. J Signal Process Syst 2018. doi:10.1007/s11265-018-1337-z.

[12] Dixit P, Gupta AK, Trivedi MC, Yadav VK. Traditional and hybrid encryption techniques: asurvey. In: Perez GM, Mishra KK, Tiwari S, Trivedi MC, editors. Networking communication and data knowledge engineering. Singapore: Springer Singapore; 2018. p. 239–48. ISBN 978-981-10-4600-1.

[13] Özkaynak F. Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dyn 2018;92(2):305–13. doi:10.1007/s11071-018-4056-x.

[14] Huang X, Ye G. An efficient self-adaptive model for chaotic image encryption algorithm. Commun Nonlinear Sci Numer Simul 2014;19(12):4094–104. doi:10.1016/j.cnsns.2014.04.012.

[15] Huang X, Ye G. An image encryption algorithm based on hyper-chaos and dna sequence. Multimed Tools Appl 2014;72(1):57–70. doi:10.1007/s11042-012-1331-6.

[16] Ye G, Huang X. An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing 2017;251:45–53. doi:10.1016/j.neucom.2017.04.016.

[17] Kumar M, Kumar S, Budhiraja R, Das M, Singh S. A cryptographic model based on logistic map and a 3-d matrix. J Inf Secur Appl 2017;32(C):47–58. doi:10.1016/j.jisa.2016.09.002.

[18] Hua Z, Yi S, Zhou Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Processing 2018;144:134–44. doi:10.1016/j.sigpro.2017.10.004.

[19] Cao W, Zhou Y, Chen CP, Xia L. Medical image encryption using edge maps. Signal Process 2017;132:96–109. doi:10.1016/j.sigpro.2016.10.003.

[20] Laiphrakpam DS, Khumanthem MS. Medical image encryption based on improved Elgamal encryption technique. Optik 2017;147:88–102. doi:10.1016/j.ijleo.2017.08.028.

[21] Laiphrakpam DS, Khumanthem MS. Cryptanalysis of symmetric key image encryption using chaotic Rossler system. Optik 2017;135:200–9. doi:10.1016/j.ijleo.2017.01.062.

[22] Mandal MK, Madhumita K, Singh SK, Barnwal VK. Symmetric key image encryption using chaotic Rossler system. Secur Commun Netw 2014;7(11):2145–52. doi:10.1002/sec.927.

[23] Ravichandran D, Praveenkumar P, Rayappan JBB, Amirtharajan R. Chaos based crossover and mutation for securing DICOM image. Comput Biol Med 2016;72:170–84. doi:10.1016/j.compbiomed.2016.03.020.

[24] Ravichandran D, Praveenkumar P, Rayappan JBB, Amirtharajan R. Dna chaos blend to secure medical privacy. IEEE Trans NanoBioscience 2017;16(8):850–8. doi:10.1109/TNB.2017.2780881.

[25] Masuda N, Aihara K. Cryptosystems with discretized chaotic maps. IEEE Trans Circuits Syst I 2002;49(1):28–40. doi:10.1109/81.974872.

[26] Pisarchik A, Zanin M. Image encryption with chaotically coupled chaotic maps. Physica D 2008;237(20):2638–48. doi:10.1016/j.physd.2008.03.049.

[27] Pisarchik AN, Flores-Carmona NJ, Carpio-Valadez M. Encryption and decryption of images with chaotic map lattices. Chaos 2006;16(3):033118. doi:10.1063/1.2242052.

[28] Wu X, Li Y, Kurths J. A new color image encryption scheme using CML and a fractional-order chaotic system. PLoS ONE 2015;10(3):1–28. doi:10.1371/journal.pone.0119660.

[29] Wang X, Xu D. Image encryption using genetic operators and intertwining logistic map. Nonlinear Dyn 2014;78(4):2975–84. doi:10.1007/s11071-014-1639-z.

[30] Kumar M, Kumar S, Budhiraja R, Das MK, Singh S. Intertwining logistic map and cellular automata based color image encryption model. In: 2016 International conference on computational techniques in information and communication technologies (ICCTICT); 2016. p. 618–23. doi:10.1109/ICCTICT.2016.7514653.

[31] Kumar M, Kumar S, Budhiraja R, Das MK, Singh S. Lightweight data security model for Iot applications: a dynamic key approach. In: 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData); 2016. p. 424–8. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2016.100.

[32] Wang X-y, Bao X-m. A novel block cryptosystem based on the coupled chaotic map lattice. Nonlinear Dyn 2013;72(4):707–15. doi:10.1007/s11071-012-0747-x.

[33] Xiang T, wo Wong K, Liao X. Selective image encryption using a spatiotemporal chaotic system. Chaos 2007;17(2):023115. doi:10.1063/1.2728112.

[34] Arroyo D, Rhouma R, Alvarez G, Li S, Fernandez V. On the security of a new image encryption scheme based on chaotic map lattices. Chaos 2008;18(3):033112. doi:10.1063/1.2959102.

[35] Xing-Yuan W, Na Z, Xiao-Li R, Yong-Lei Z. Synchronization of spatiotemporal chaotic systems and application to secure communication of digital image. Chin Phys B 2011;20(2):020507.

[36] Wang Y, Liao X, Xiao D, Wong K-W. One-way hash function construction based on 2d coupled map lattices. Inf Sci 2008;178(5):1391–406. doi:10.1016/j.ins.2007.10.008.

[37] Solak E, Çokal C. Algebraic break of image ciphers based on discretized chaotic map lattices. Inf Sci 2011;181(1):227–33. doi:10.1016/j.ins.2010.09.009.

[38] Ge X, Liu F, Lu B, Wang W. Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem and its improved version. Phys Lett A 2011;375(5):908–13. doi:10.1016/j.physleta.2010.12.065.

[39] Rhouma R, Belghith S. Cryptanalysis of a spatiotemporal chaotic cryptosystem. Chaos Solitons Fractals 2009;41(4):1718–22. doi:10.1016/j.chaos.2008.07.016.

[40] Hao Z, Xing-yuan W, Si-wei W, Kang G, Xiao-hui L. Application of coupled map lattice with parameter q in image encryption. Opt Lasers Eng 2017;88:65–74. doi:10.1016/j.optlaseng.2016.07.004.

[41] A cryptographic model for better information security. J Inf Secur Appl 2018;43:123–38. doi:10.1016/j.jisa.2018.10.011.

[42] Hua Z, Zhou Y, Pun C-M, Chen CP. 2D sine logistic modulation map for image encryption. Inf Sci 2015;297:80–94. doi:10.1016/j.ins.2014.11.018.

[43] LOZI R. Un attracteur étrange (?) du type attracteur de hénon. J Phys Colloques 1978;39. C5–9–C5–10. 10.1051/jphyscol:1978505.

[44] Kumar M, Kumar S, Das M, Budhiraja R, Singh S. Securing images with a diffusion mechanism based on fractional Brownian motion. J Inf Secur Appl 2018;40:134–44. doi:10.1016/j.jisa.2018.03.007.

[45] Li C. Cracking a hierarchical chaotic image encryption algorithm based on permutation. CoRR 2015 arXiv:1505.00335.

[46] Xie EY, Li C, Yu S, Lü J. On the cryptanalysis of Fridrich's chaotic image encryption scheme. Signal Process 2017;132:150–4. doi:10.1016/j.sigpro.2016.10.002.

[47] Mills D. Review of cryptography: theory and practice by d. r. stinson. Cryptologia 2007;31(1):87–8. doi:10.1080/01611190600964785.

[48] Wu Y, Zhou Y, Saveriades G, Agaian S, Noonan JP, Natarajan P. Local Shannon entropy measure with statistical tests for image randomness. Inf Sci 2013;222:323–342. Including Special Section on New Trends in Ambient Intelligence and Bio-inspired Systems. 10.1016/j.ins.2012.07.049.

[49] Pak C, Huang L. A new color image encryption using combination of the 1d chaotic map. Signal Process 2017;138:129–37. doi:10.1016/j.sigpro.2017.03.011.

[50] Nematzadeh H, Enayatifar R, Motameni H, Guimarães FG, Coelho VN. Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. Opt Lasers Eng 2018;110:24–32. doi:10.1016/j.optlaseng.2018.05.009.

[51] Ismail SM, Said LA, Radwan AG, Madian AH, Abu-Elyazeed MF. Generalized double-humped logistic map-based medical image encryption. J Adv Res 2018;10:85–98. doi:10.1016/j.jare.2018.01.009.

[52] Enayatifar R, Abdullah AH, Isnin IF. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt Lasers Eng 2014;56:83–93. doi:10.1016/j.optlaseng.2013.12.003.

[53] Enayatifar R, Abdullah AH, Lee M. A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption. Opt Lasers Eng 2013;51(9):1066–77. doi:10.1016/j.optlaseng.2013.03.010.

[54] Abdullah AH, Enayatifar R, Lee M. A hybrid genetic algorithm and chaotic function model for image encryption. AEU 2012;66(10):806–16. doi:10.1016/j.aeue.2012.01.015.

[55] Norouzi B, Mirzakuchaki S, Seyedzadeh SM, Mosavi MR. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimed Tools Appl 2014;71(3):1469–97. doi:10.1007/s11042-012-1292-9.

[56] A designed image encryption algorithm based on chaotic systems. J Comput Theor Nanosci 2012;9(12).