International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

An Efficient Encryption System on 2D Sine Logistic Map based Diffusion

Akshay Chamoli
Dept. of Computer Science,
Jamia Hamdard New Delhi, India
akachamoli@gmail.com

Jawed Ahmed
Dept. of Computer Science,
Jamia Hamdard New Delhi, India
Jahmed2047@jamiahamdard.ac.in

Mohammad Afshar Alam
Vice-chancellor
Jamia Hamdard New Delhi, India
aalam@jamiahamdard.ac.in

Bhavya Alankar
Dept. of Computer Science,
Jamia Hamdard New Delhi, India
alankar.bhavya@jamiahamdard.ac.in

Abstract

An optimal cryptographic model is proposed, enabling the feature of 2D sine logistic map-based diffusion algorithm. The 2D sine logistic map process is merged with the algorithm as it has the ability to provide random number generator as well as to overcome blank. The previous existing models based on image encryption use to work on raw images but without alteration for the process of confusion and diffusion. The main disadvantage as the nearby pixel values for an image always remains similar. This issue is resolved by a Pseudo random generator process which is based on key stream that alters pixel value. Furthermore 2D sine logistic map based diffusion process has shown an improvement in the key sensitivity and the complex relationships that use to get developed between cipher and test image.2D sine logistic map with diffusion method used to keep pixels intact with each other to such an extent as even a single bit modification in the intensity value of an original image pixel will lead to a huge change in most of the pixels of the cipher and thus makes the model very sensitive to make any changes in the pixel value or secret key for an image. As seen and analyzed with a variety of test results that strategic model used for encryption can easily encrypt the plain image into a cipher of a random binary sequence.

Keywords: 2D Sine Logistic Map, Diffusion, Confusion, Encryption

Introduction

A lot has expanded in the area of communication technologies and a wide variety of information daily gets generated which is then stored as well as shared over communication network [1]. The main focus is always to prevent the critical information from any unauthorized users [2]. To resolve these issues the image encryption technology came into picture and is also an important process [3]. Some new analysis on chaos method for image encryption is shared [4]. Chaos based cryptosystems have features like behavior is dynamic in nature and they are sensitive to initial conditions with high complexity and quick implementation [5, 6]. Akhavan et al. [7], Dou et al. [8], Ubaidurrahman et al.[9] proposed a variety of cryptosystems using DNA computing having a variety of different encoding rules. A variety of others encryption processes that operates on the logic of discrete fractional wavelet transformation [10] as well as Fractional Fourier Transformation [11] with some other transformations also [12,13].Liu et al. [14], created an efficient symmetric algorithm that use to encrypt the images on the basis of 1-D coupled Sine map algorithm.In this paper the initial step is to analyze the actual structure of CCSM, generated in a digital computer with limited precision and proposing a 1-D coupled Sine map algorithm. In this the initial step is for analyzing the actual structure of CCSM which is generated in a digital computer with limited precision and in next step to choose a plain text attack for breaking CSMIE in respect with the number of blocks. The process which works on a 3D hyper-chaotic system and implements a hash value of a plain image using pre-modular, permutation and diffusion architecture. Mondal et al. [15], an efficient encryption algorithm on the concept of 2D sine–cosine cross-chaotic (SC3) map with high confusion and diffusion capability. The procedure utilizes chaotic maps to generate the secret keys that are used in the confusion process. In the last the process of diffusion is applied using RC4 stream cipher based on the concept of random sequence. Various other methods have also been proposed with the help of confusion-diffusion structure [16, 17].

1.1 Related work

The 2D logistic map is researched for its complicated behaviors of the evolution of basins and attractors [18]. It has greater complicated chaotic behaviors than one-dimensional Sine Logistic map. Because of the terrific residences of unpredictability, ergodicity and sensitivity to their parameters and initial values, chaotic maps are widely utilized in safety packages. Due to these homes, we introduce a selection based totally two-dimensional Sine Logistic map (2D-SLM) that is derived from the Logistic and Sine maps. Performance evaluation is furnished to show that 2D-SLM has the broader chaotic variety, better ergodicity and hyper chaotic properties than present chaotic maps. It has extraordinary chaotic overall performance and its outputs are hard to expect. In the closing decade, sine logistic map based totally diverse picture encryption algorithms have been developed. These algorithms have applied the 2D sine logistic map as key property to encrypt data.

Hua et al. [19], proposed an photo encryption model the usage of a brand new two-dimensional Sine Logistic map (2D-SLMM) that is derived from the Logistic and Sine maps. Zhu et al. [20] proposes a new 2D chaotic map, called the 2D Logistic-adjusted-Sine map (2D-LASM). It uses the Logistic map to regulate the entry of the Sine map and then extends its phase plane from 1D to 2D. Subodhet. Al. [21] proposed method confusion and diffusion each operations are performed, similarly to enhance the security level random values are added to the authentic picture. With the help of simulation effects and analysis of protection, it can be proved that modified two dimensional sine logistic map can encrypt numerous styles of snap shots. Further, a new cryptographic model the usage of 2D chaotic map which is derived from the idea of giving the 2 outputs of a 2D logistic map to two separate 1-dimensional logistic maps is advanced by means of madhu et al. [22]. 2D-SLM is applied to permute the positions of photo pixels. Similarly, Zhang et al. [23], advanced a brand new chaotic map mixed with put off and cascade, referred to as tent postpone-sine cascade with logistic map (TDSCL). It has pseudo-randomness and is suitable for picture encryption. In preferred, at the confusion level photo pixels are permuted, preserving pixel values unchanged using transformation method i.E. Baker map, Arnold map, Magic rectangular. Hence, it makes the confusion algorithm more vulnerable to statistical attacks [24]. While, at the diffusion stage Friedrich's diffusion mechanism is used where a small amendment in pixels impacts most of the pixels of the image. The mystery key may be revealed the use of chosen and acknowledged plaintext attacks[40-43] in Friedrich's diffusion mechanism [24, 25] the usage of DEA (distinction equation of the modulo addition) approach [26].

In proposed cryptographic models sine logistic map and two dimensional sine logistic map are used in confusion and diffusion fashions respectively. Due to 2 dimensional sine logistic map, the proposed map not most effective improves the restrictions of logistic map i.e. Solid and blank home windows, uneven distribution of sequences [21] but decreases the differential and statistical assaults risk [13]. Diffusion with two dimensional sine map further improve the performance of the encryption process and make it extra comfortable.

In the model, random numbers are introduced to the surroundings of the picture and similarly pics are represented converted into crimson, green and blue channels. Each channel is then subjected to pre-process operation to adjust pixels in it. Subsequently every channel of the image is shuffled the usage of the shuffling method to randomize all of the pixels. In order to growth the degree of bewilderment, each channel is subjected to a sine logistic map. Finally, pixels are subtle the use of a two dimensional

***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

sine logistic map primarily based diffusion method. This may be noticed that a two dimensional sine logistic map applied within the diffusion manner binds the prevailing, previous and next pixels [27].

The predominant work is outline as:

(1) A new composition of random records addition, pre-processing of pixels, shuffling followed by confusion and diffusion shape for cryptographic construction is proposed and evaluated.

(2) Secret Key utilized in every level of the cryptographic production, are made unique photograph dependent [28].

The rest of the object is prepared as: In Section 2 the preliminary situations and manage parameters are generated and utilized inside the two dimensional sine logistic map. Sub-section 2.10 details the two dimensional sine logistic map. In Section four random facts addition, pre-technique and shuffling process are defined. Section 5 details the confusion procedure used and similarly explains the diffusion model. A quick dialogue about the proposed encryption set of rules is described in Section 6. Detailed simulation is accomplished to affirm the cryptographic version against diverse styles of assaults and their consequences are given in Sections 7 and eight. Conclusion is outlined after sub-segment 3.10.

2. Initial conditions and parameters

A color image I = M*N is considered as a test image where M & N represent width and height respectively. The color image is represented into Red, Green and Blue components. Here parameter PT_s is plaintext image pixel submission, P_a, P_b, P_a are derived from PT_s in a way that any change in input image will affect all the parameters. A PRNG is used to generate a secret key L of 280-bit. Secret key is divided into sub keys L_1 to L_{35} of 8-bits each. Parameters x_0 to z_0, x_1 to z_1, x_2 to z_2 are chosen between 0 and 1 because these are the initial values for a two dimensional sine logistic map and the lyapunov exponent is positive in the given range [7].

$I = M*N$
$PTs = I$
$i=1$
$P_a = ((PT_s + MN) \times 255)/(1 + MN)$
$P_b = ((PT_s + 2 \times MN) \times 255)/(2 + MN)$ $PT_S = ((PT_s + 3 \times MN) \times 255)/(3 + MN)$
$L = L_1 L_2 L_3 L_4 L_{35}$
$x_0 = (((L_1 \oplus L_3 + L_5 + L_7 + Pa) \oplus (L_9 \oplus L_{11} \oplus L_{14}))/(1 + L_2 \times L_4)) \bmod 1$
$y_0 = (((L_2 \oplus L_4 + L_6 + L_{31} + Pb) \oplus (L_{10} \oplus L_{12} \oplus L_{14}))/(1 + L_{25} \times L_{30})) \bmod 1$
$z_0 = (((L_7 \oplus L_{20} + L_{31} + Pc) \oplus (L_{19} \oplus L_{22} \oplus L_{34}))/(1 + L_{33} + L_{35})) \bmod 1$
$x1 = (((L_{15} \oplus L_{29} + L_{18}) \oplus (L_{17} \oplus L_{20} \oplus L_{26}))/(1 + Ps + L_{21} + L_{27})) \bmod 1$
$y1 = (((L_{16} \oplus (L_{28} \oplus L_{23} \oplus L_{12}))/(1 + (Pa \times PTs) + L_{16} + L_{19})) \bmod 1$
$z1 = (((L_{22} \oplus L_{17} + L_{25} + L_{22}) \oplus (L_9 \oplus L_7 \oplus L_{31}))/(1 + (Pb \times Pc) + L_{23})) \bmod 1$
$x2 = (((L_{25} \oplus L_{19} + L_8) \oplus (L_7 \oplus L_2 \oplus L_6))/(1 + Pb \times L9)) \bmod 1$
$y2 = (((L_3 \oplus (L_8 \oplus L_{13} \oplus L_{30}))/(1 + PTs \times L_{34})) \bmod 1$
$z2 = (((L_{32} \oplus Pa + L_{15}) \oplus (L_{30} \oplus L_{11} \oplus L_{21}))/(1 + L_{33} + L_{22})) \bmod 1$

Here denotes bit-wise XOR operation, L_1, L_2, L_{35} are key dependent control parameters and sub keys. These are further used to derive the key-streams for 2D sine Logistic Map [13].

2.1 Sine logistic map and 2D sine logistic map

One-dimensional chaotic maps have been widely used in cryptographic models due to desirable chaotic properties with simple structure. But a one-dimensional logistic map contains one control parameter and one initial parameter [29]. It has a problem of blank and stable windows, small key space and unevenly distributed output sequence. An attacker can use these defects to reveal the secret key. To attain better chaotic behavior, large key space and to overcome the defects in the logistic map, 2D SLM as a diffusion is developed.

2.2 Sine logistic map

Mathematically sine logistic map is defined as below:

$$x_{i+1} = \alpha(\sin(\pi y_i) + \beta)x_i(1 - x_i),$$

$$y_{i+1} = \alpha(\sin(\pi x_{i+1}) + \beta)y_i(1 - y_i)$$

(1)

Here the value of α is within the range of [0, 1] and the value of β is fixed as 3. This two dimensional logistic map is formed using Sine and Logistic maps. Logistic equation is scaled by using α and then output is given to the input of the sine logistic map.

2.3 Two dimensional Sine Logistic Sine map

Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

Mathematically two dimensional modified logistic sine map is defined as below:

$x_{i+1}= \sin(\pi\ \alpha(y_i+x_{i\ +}\ \beta)x_i(1-x_i)),$
$y_{i+1}=\sin(\pi\alpha(x_{i+1}+y_i+\beta)y_i(1-y_i))$ (2)

Here the value of α is within the range of [0, 1] and the value of β is fixed as 3. This modified two dimensional logistic map is formed using Sine and Logistic maps. Logistic equation is scaled by using α and then output is given to the input of the sine logistic map. Two dimensional sine logistic map has more complicated output in comparison to the logistic map and sine map and the value of the lyapunov exponent is positive and accomplishes the chaotic property. In all trajectories the initial values are set as (0.1, 0.2) and parameters are set in such a way that chaotic map could be distributed in a larger area. It can be seen from figures 1.1 and figure 1.2 Two Dimensional sine logistic map distributed in complete range. It also has a larger area in comparison to other maps. so it can be concluded that a two dimensional modified sine map has better ergodicity and is more random.

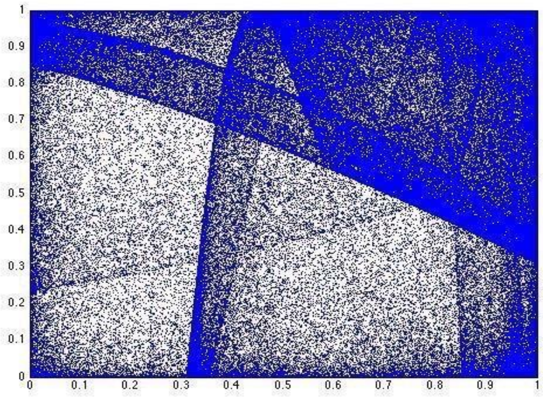


Fig. 1.1: Sine logistic map

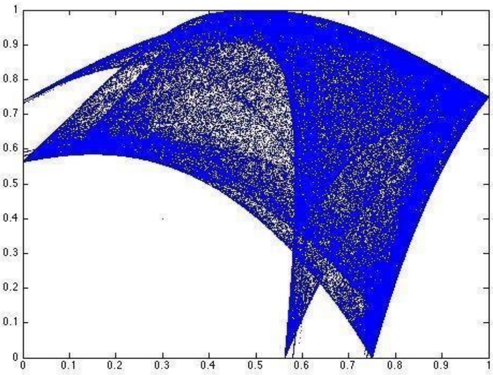


Fig. 1.2: 2D sine logistic map

2.4 Lyapunov exponent

Lyapunov exponent quantifies the chaotic behavior for the dynamical systems. If the value of the Lyapunov exponent is positive then one can state that the dynamical system is chaotic [32]. Figure 2.1 and 2.2. shows the lyapunov exponent for sine logistic map (r =3.998) and 2D sine logistic map (μ = 3.999) respectively.

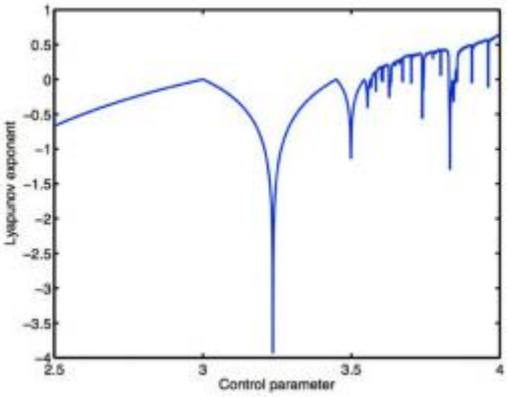


Fig. 2.1: Lyapunov exponent for sine map

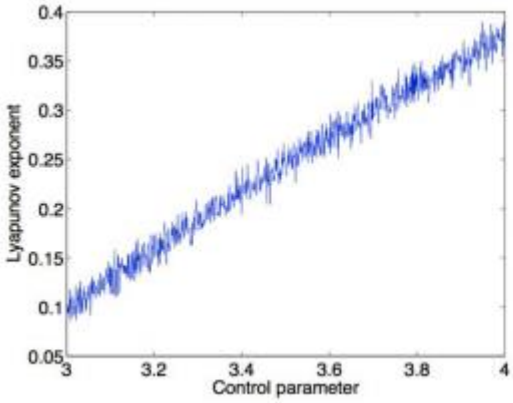


Fig. 2.2 :lyapunov exponent for 2D sine map

From the ongoing analysis, it is to be noted here that a two dimensional sine logistic map is more complex and more random in nature. It makes the map suitable to be used in encryption.

2.5 Key generation

A 128-bit long random binary secret key (K) is used to generate control parameters and initial conditions that are used in sine logistic map and in 2D sine logistic map. Secret key is further divided into 16 blocks ($K_1$to K_{16}). From the Eq. (3), it can be concluded that the primary conditions and control parameters of 2D sine logistic map logistic map and are key dependent and more sensitive to changes in even a single bit of the 128-bit long external secret key. Hence, the proposed encryption model with a key space of 2^{128} can resist any brute-force attack.

$K = K_1\ K_2\ K_3\ K_4 \ldots.\ K_{16}$,

$\mu = 3.9 + [(K_2 + K_5) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{16})) \bmod 2]/100$,

$x_1 = [((K_{15} + K_{11}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{16}))/(K_{13} + K_{12})] \bmod 1$,

$x_2 = [((K_{13}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{16}))/(K_{10} + K_{14})] \bmod 1$,

$x_3 = [((K_{11} + K_{12}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{16}))/(1 + K_{16})] \bmod 1$,

$y_1 = [((K_3 + K_2) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{16}))/(K_{14} + K_{16})] \bmod 2$,

$y_2 = [((K_9 + K_{12}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{16}))/(K_{15} + K_{16})] \bmod 2$,

$y_3 = [((K_{14} + K_{13}) \oplus (K_1 \oplus K_2 \oplus \ldots\ldots\ldots K_{16}))/(1 + K_{28})] \bmod 2$,

$SF = K_1 \times K_8 + (K_7 \times K_6) \oplus K_9 + 111 \qquad (3)$

Here $\oplus$ denotes bitwise XOR operation, x1, x2, x3, y1, y_2, y_3, K_1, K_2, … K_{16} are initial parameters and keys.

2.6 Mixing process

Chaotic Mixing makes a complex relationship between plain image and 2D Sine logistic map based chaotic sequence. Plain image pixel values are modified by 2D Sine logistic map based chaotic sequences. Further, these sequences are converted into a one dimensional array. Then the first pixel is XOR-ed with first chaotic sequence value, similarity second pixel with second chaotic sequence value and so on. This process is applied for the complete array. Mathematically, the process of mixing is represented as:

$I' = I \oplus R$.

Here, I and I ′ represents a plain image and the corresponding image generated after the mixing process. Term R represents 2D sine logistic map based chaotic sequences.

2.7 Shuffling engine

The shuffling engine helps in reducing the correlation among the image pixels placed adjacent to each other. Following steps are used to implement the shuffling process.

Step 1: At first, 2D - SLM map based chaotic matrix is generated and sorted in increasing order.

Step 2: Sorted pixel positions are retained and the matrix is indexed column-wise.

Step 3: Plain image is shuffled based on the indexed matrix obtained in step 2.

Step 4: Further, row-wise sorted matrix is again sorted column-wise and adjusted in increasing order.

Step 5: Now the sorted positions are indexed row-wise.

Step 6: Finally, the shuffled matrix obtained in step 3 is shuffled again based on a row-wise indexed matrix.

This shuffling process is repeated for the entire image pixels. It is to be noted that a two tier shuffling process is used to minimize correlation and to ensure the maximum confusion among pixels. This two tier shuffling mechanism makes the system resistive against differential attacks.

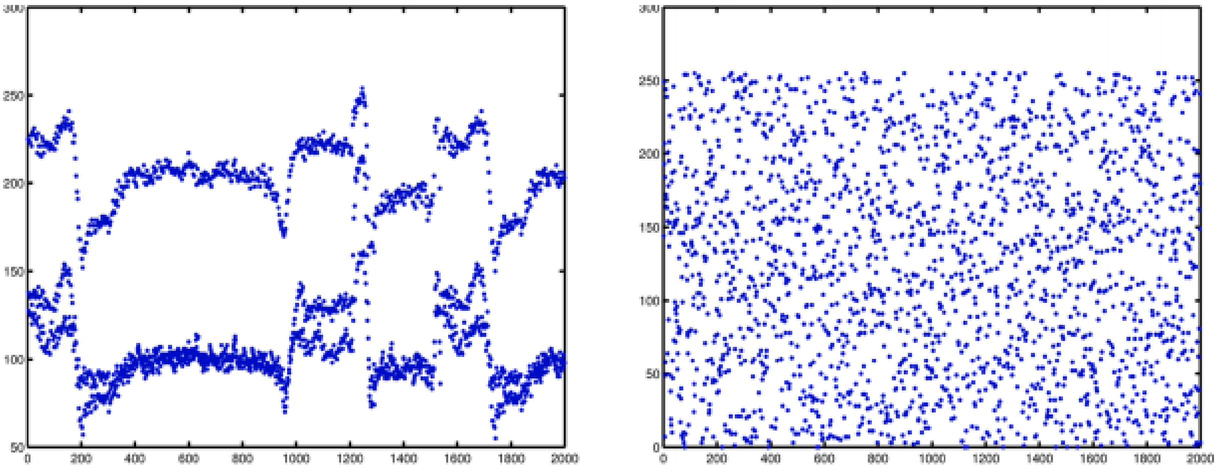


Fig. 3: Result of shuffling process is shown for the numbers ranging from 0 to 2000. Fig. (a) shows the pixels before shuffling and shuffled values are shown in Fig. (b). y-axis represents the Pixel values and x-axis shows the pixel positions.

2.8 Confusion

It is the process that makes the complex relationship among plaintext, cipher-text and secret key. Hence attackers would not be able to find-out any clue whether a change is made plain-text/ cipher-text or key. Many existing cryptographic systems use initial condition and control parameters to generate the cipher. As a result, differential attacks can be used to reveal information.

Following mathematical relation represents the confusion process:

$$C_{i+1} = C_{i-1} \oplus Key_i \oplus C_i \oplus SM_i. \quad (4)$$

where, $1 \leq i \leq$ size of image. Confusion operation is applied for all the pixels of the image using Eq. (4).

2.9. Diffusion

Diffusion model is used to bind image pixels in a way that one-bit change will affect most of the cipher image pixels. In plain images, adjacent pixels pose high correlation and diffusion is applied to reduce the correlation among adjacent pixels. 2D Sine Logistic map uses initial conditions x_1, x_2, x_3 and the parameters μ, k_1, k_1 and k_3 to be used in the proposed diffusion model. The generated key stream is first scaled up using factor SF. This operation is defined as [25]:

$$C_i = [\ (C_i \oplus C_{i-1}) + [\ SM_i \times SF \bmod 256\ ] \oplus C_{i+1}\ ] \bmod 256. \quad (5)$$

where $1 \leq i \leq M \times N$, C_i, C_{i-1} and C_{i+1} represent the current pixel, previous and next pixel of the image respectively. SM_i represents the key stream generated using 2D Sine logistic map and scaled up by factor SF.

2.10. 2D Sine logistic map 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, the test image is transformed into a linear array.
Step 2: PRNG (Pseudo random number generator) based 128-bit external random key is generated and further used to generate initial conditions and control parameters to the sequence 2D Sine logistic map.
Step 3: Transformed Test image (Obtained in Step 1) is XOR-ed with the sequence generated by 2D Sine logistic map.
Step 4: Output obtained in step 3 is represented into a matrix and shuffled based on the shuffling engine in subsection 3.3. As a result pixels of the test image are shuffled with approximately zero or no correlation.
Step 5: To attain higher degree of confusion among the test image pixels, Sine map-based confusion with secret key is deduced.
Step 6: Finally, 2D Sine logistic map-based diffusion model is applied. It binds the pixels in a way that a change in one pixel will affect most of the test image pixels and the cipher image is obtained as shown in Fig. 4 and 5.

Fig. 4. Lena image and its encrypted and decrypted images.

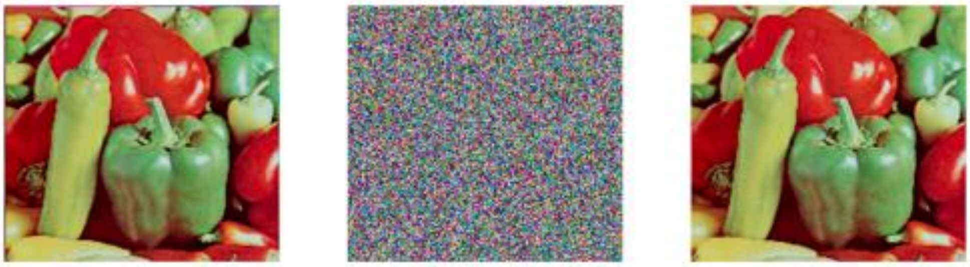


Fig. 5. Pepper image and its encrypted and decrypted images.

3. Simulation result and discussion

Over an unsecured channel, to improve the security aspect 2D Sine logistic map-based diffusion models help the system to share images. The proposed model should be resistive against differential and statistical attacks [26, 30, 27, 31] and to do so each procedure used in the model should enhance the features of the cipher. To improve the robustness of 2D Sine logistic map-based diffusion model, the cipher and secret key were analyzed with various security analysis techniques and the results are discussed in the rest of the paper.

3.1. Key space

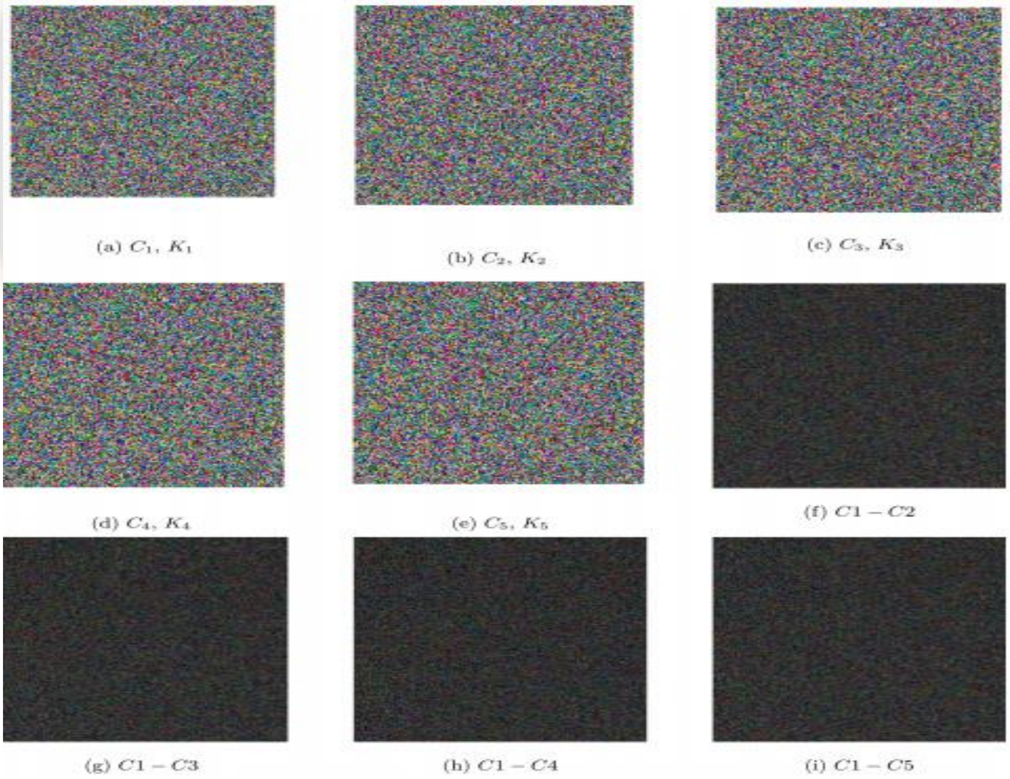
It simply represents the key combinations. In this paper, the proposed model uses a 128-bit key to compute initial conditions as well as the control parameters. The key space taken is 2^{128}. Since the key space is large it is also helpful against brute force attacks and technically the analysis says that a secure key-space should be $\geq 2^{100}$ [33].

3.2 Key sensitivity analysis

The most relevant feature for any encryption scheme. Shows a massive change in cipher as a one-bit change in secret key.

For example, five secret keys:

K_1 = [7retwsywzxwer234], K_2 = [7retwsywzxwer235], K_3 = [7retwsywzxwer234], K_4 = [7retwsywzxwer234], K_5 = [7retwsywzxwer234] each differ by one-bit, are used to check the sensitivity of the proposed encryption model. We have used Lena images for the key sensitivity test. In Fig. 6, cipher images are generated from the Lena image. Fig. 7(a)–(e) shows the cipher images with one-bit change in secret key $K_1 - K_5$. Fig. 6(f)–(i) shows the difference in cipher image using K_1&K_2 , K_1& K_3 , K_1& K_4 and K_1& K_5 . It is to be noted from key sensitivity test results that different ciphers are generated in each run. Hence key sensitivity tests enhance the security level of the proposed model.



(a) C_1, K_1 (b) C_2, K_2 (c) C_3, K_3

(d) C_4, K_4 (e) C_5, K_5 (f) $C1 - C2$

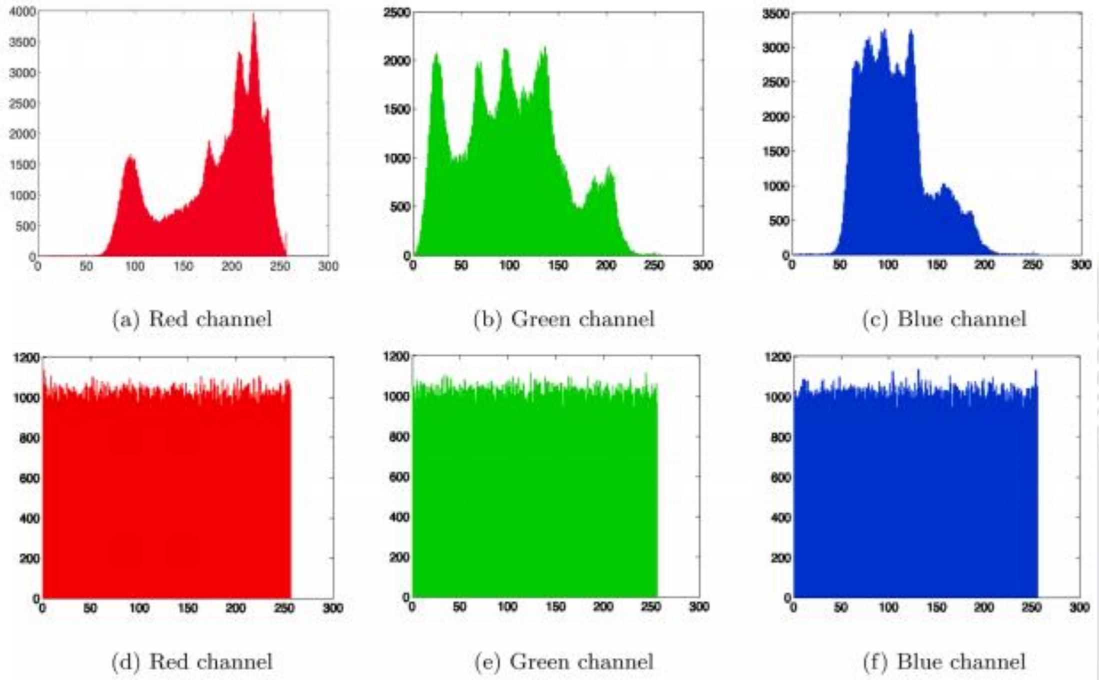
(g) $C1 - C3$ (h) $C1 - C4$ (i) $C1 - C5$

Fig. 6. Key sensitivity analysis for proposed 2D-SLM diffusion model for Lena image (Fig. 5 (Plain text)). (a) C_1, K_1 (b) C_2, K_2 (c) C_3, K_3 (d) C_4, K_4 (e) C_5, K_5 (f) C_1 - C_2 using K_1, K_2 (g) C_1 - C_3 using K_1, K_3 (h) C_1 - C_4 using K_1, K_4 (i) C_1 - C_5 using K_1, K_5.

Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

3.3 Histogram analysis

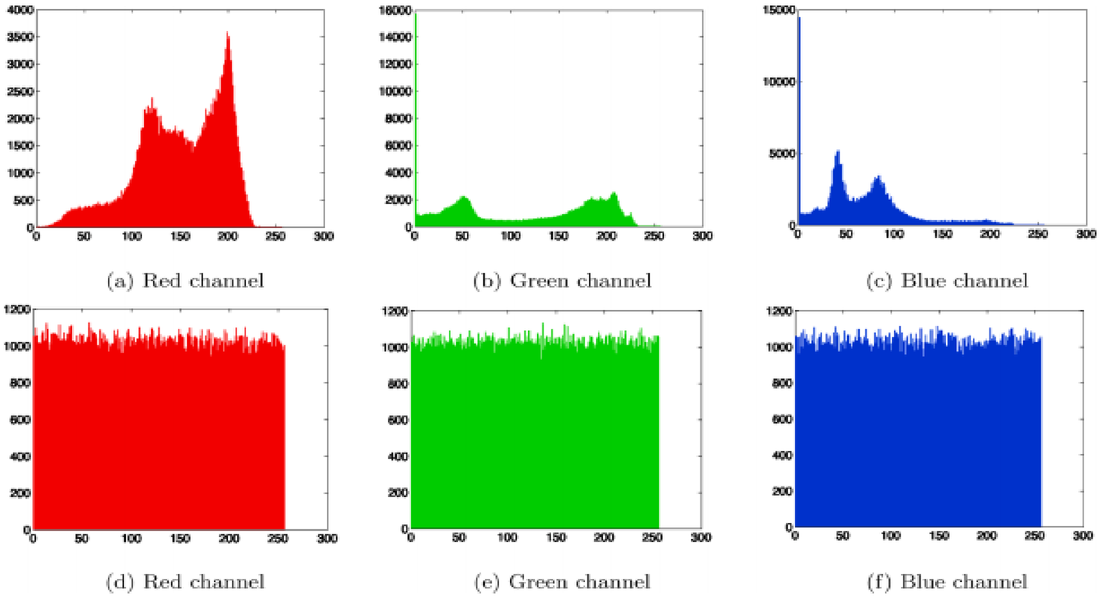
The pixel distribution in an image is represented by Histogram analysis. Uniformity plays a major role to compete against any kind of statistical or frequency attack if the pixels distribution for any cipher is uniform. Figs. 7 (a–f) (Lena) and 8 (a–f) (Pepper) are histograms for plain and cipher images respectively. It is to be noted from the histograms that red, green and blue channels of cipher image are flat and uniform. Further, the chi-square (χ2) test was analysed on a cipher image and the outcome is mentioned in Table 2. One can notice from Table 2, p values are > 0.05 which shows that the cipher pixels are uniform in nature and accept the null hypothesis. 'A' denotes null hypothesis acceptance.



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

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

Fig. 7. Plain image (Lena) Histogram for (a) Red, (b) Green and (c) Blue channel & Cipher image Histogram for (a) Red, (b) Green and (c) Blue channel



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

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

Fig. 8. Plain image (Pepper) Histogram for (a) Red, (b) Green and (c) Blue channel & Cipher image Histogram for (a) Red, (b) Green and (c) Blue channel.

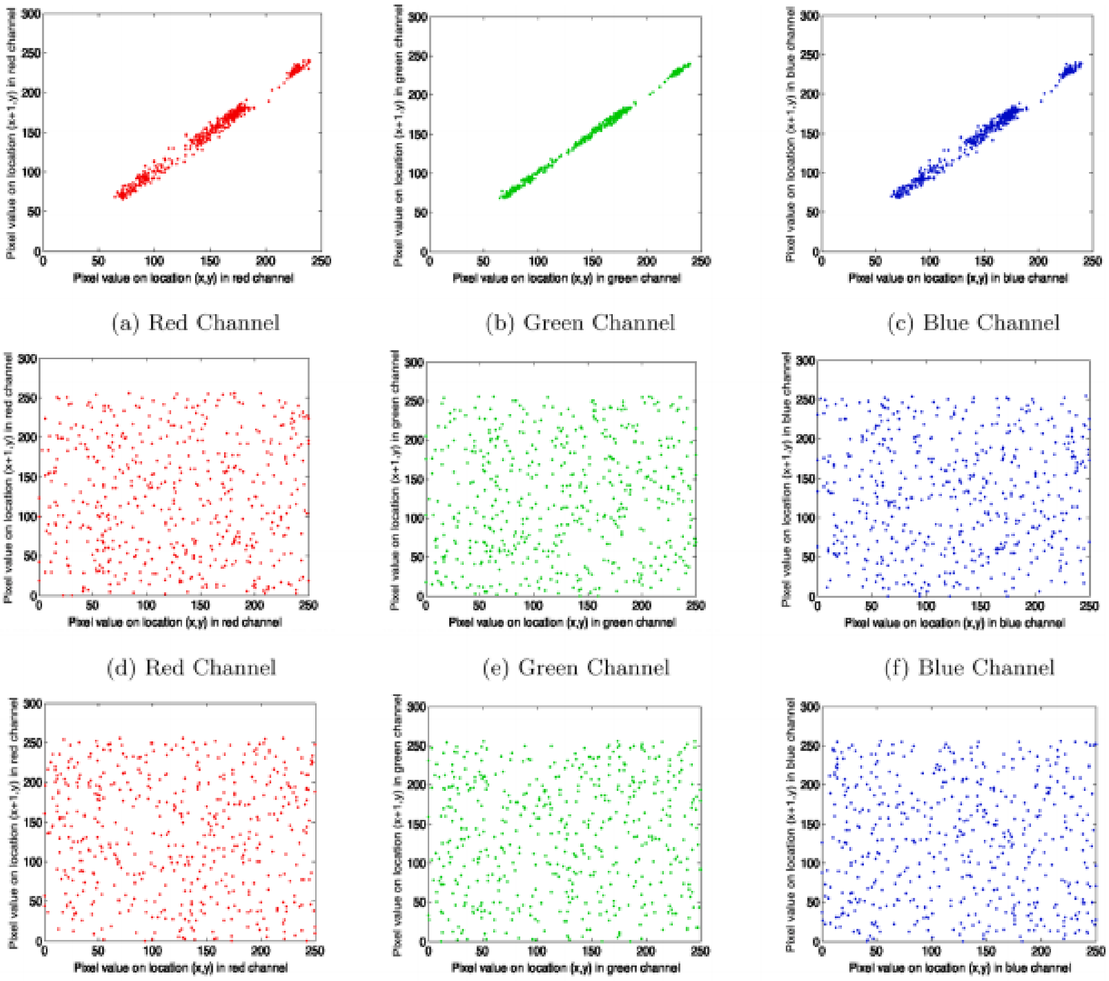
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

3.4 Correlation analysis

Correlation analysis evaluates the resistance of 2D Sine logistic map based diffusion models. For a secure image correlation coefficient between adjacent pixels should be approximately 0. Correlation coefficient is defined as r_{XY}:

$$\begin{aligned}
r_{xy} &= \frac{Cov(x,y)}{\sqrt{D(x)D(y)}} \\
E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i \\
D(x) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \\
cov(x,y) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))
\end{aligned}$$

Here, N represents the total number of pixels. E(x) and E(y) represent the mean for x_i and y_I respectively. Fig. 9 (a–c) and (d–i) show the correlation for test and cipher images.



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

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

Fig: 9: Horizontal, vertical and diagonal direction correlations of two adjoining pixels for Lena image.

3.5 Differential attack

NPCR and UACI scores are used to check the resistivity of the proposed model against differential attacks. These are computed based on a minor change in test image and corresponding cipher. NPCR and UACI scores are calculated as:

$$\text{NPCR} = -\frac{\sum_{i,j} DI(i,j)}{M*N} * 100\%$$

$$\text{UACI} = \frac{\sum_{i,j} \frac{CI(i,j) - CI'(I,J)}{255}}{M*N} * 100\%$$

CI and CI' are cipher images with one bit pixel difference.
if CI (i; j) = CI'(i; j) DI (i; j) = 0OtherwiseDI (i; j) = 1

The Tables 6 and 7 below shows NPCR and UACI values for a range of control parameter values µ. One can notice from the tables 6 and 7 that the proposed model achieves higher NPCR and UACI score which makes the model resistive against differential attacks.

Table 6: NPCR score comparison for different 2D Sine map control parameter µ.

Image	**µ** = 3.88	**µ** = 3.89	**µ** = 3.90
Lena	99.76	99.74	99.80
Pepper	99.80	99.78	99.83
Boat	99.81	99.74	99.81
Baboon	99.90	99.82	99.69

Table 7: UACI score comparison for different 2D SLM control parameter µ.

Image	**µ** = 3.88	**µ** = 3.89	**µ** = 3.90
Lena	33.39	33.37	33.41
Pepper	33.49	33.44	33.48
Boat	33.47	33.44	38.46
Baboon	33.45	33.47	33.49

3.6 Information entropy

The degree of uncertainty is measured by Information entropy and the parameter used is s:

$$H_e(s) = -\sum_{i=0}^{2^n-1} I(s_i) - log_2\ (s_i)$$

The variable N represents total bits per symbol and the parameter $I(S_i)$ represents probability of symbol s_i. $H_e(s)$ gives the value for information entropy and for an efficient cryptographic model the approximate value should be near to 8. The below mentioned Table 8 signifies comparison among information entropy with different values of control parameter µ. The noticeable information is when information entropy is taken as 8 then it confirms no information leakage.

Table 8: Information entropy comparison for different 2D sine map control parameters µ.

Image	**Lena**	**Pepper**	**Boat**	**Baboon**
Original Image	7.4541	7.5132	7.6751	6.4287
µ = 3.88	7.9989	7.9990	7.9991	7.9999
µ = 3.89	7.7991	7.9992	7.9997	7.9990
µ = 3.90	7.7998	7.9991	7.9993	7.9995

Table 9: Comparison With Existing model for encryption

Algorithm	**Entropy**	**NPCR**	**UACI**
Proposed Model	7.9998	0.997513	0.3344
Ref.[34]	7.9983	0.990383	0.329283
Ref.[35]	7.9992	0.998501	0.333401

Ref.[36]	7.9993	0.991074	0.331085
Ref.[37]	7.9951	0.986273	0.316882
Ref.[38]	7.9992	0.992592	0.331834
Ref.[39]	7.9974	0.996094	0.286345
Ref.[40]	7.9991	0.995789	0.334549
Ref.[41]	7.9978	0.9959	0.3350
Ref.[42]	7.9942	0.9930	0.3334
Ref.[43]	7.9030	0.9957	0.3346
Ref.[44]	7.9938	0.9960	0.4363

Table 10: Comparison of Correlation Coefficient with Existing model for encryption

Algorithm	R	G	B
Proposed Model	0.0011	0.0014	0.0010
Ref.[34]	0.0062	0.0106	0.0015
Ref.[35]	0.0020	0.0012	0.0011
Ref.[36]	0.0039	0.0041	0.0008
Ref.[37]	0.0149	0.0210	0.0062
Ref.[38]	0.0031	0.0029	0.0013
Ref.[39]	-0.0223	-0.0084	0.286345
Ref.[40]	0.0693	-0.0610	-0.0242
Ref.[41]	0.0004	0.0013	-0.0023
Ref.[42]	0.0063	0.0124	0.0179
Ref.[43]	-0.0294	-0.0014	-0.0180
Ref.[44]	0.0059	0.0027	0.0000

3.7 Compression

To transfer large amount of data the best technique is compression. The technique to compress data is known as encoding. In the proposed model the test used is jpeg lossless compression. The simulation results are shown below Fig. 10 that cipher image (a) is compressed for different compression ratio (CR) Fig. 10(b) CR ≥ 5.9853, Fig. 10(c) CR ≥ 9.7653, Fig. 10(d) CR ≥ 13.4589, Fig. 10(e) CR ≥ 16.9065 and Fig. 10(f) CR ≥ 29.9781. The final image obtained after the involvement of compression ratio ≥

***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

29.9781 is fully distorted. It concludes that the technique of 2D Sine logistic map-based diffusion model makes the model robust for the technique of lossless compression. The analysis from Table 10 is that firstly the correlation coefficient is negligible, Information entropy is at maximum (approximately 8), NPCR and UACI score are higher (≥ 99.60 and ≥ 33.43) and suitable for each channel that support resistivity of the model against various known attacks. The results shown below states that the proposed model when compared to the other existing models have performed better in the security aspect and is mentioned below in Table 10.

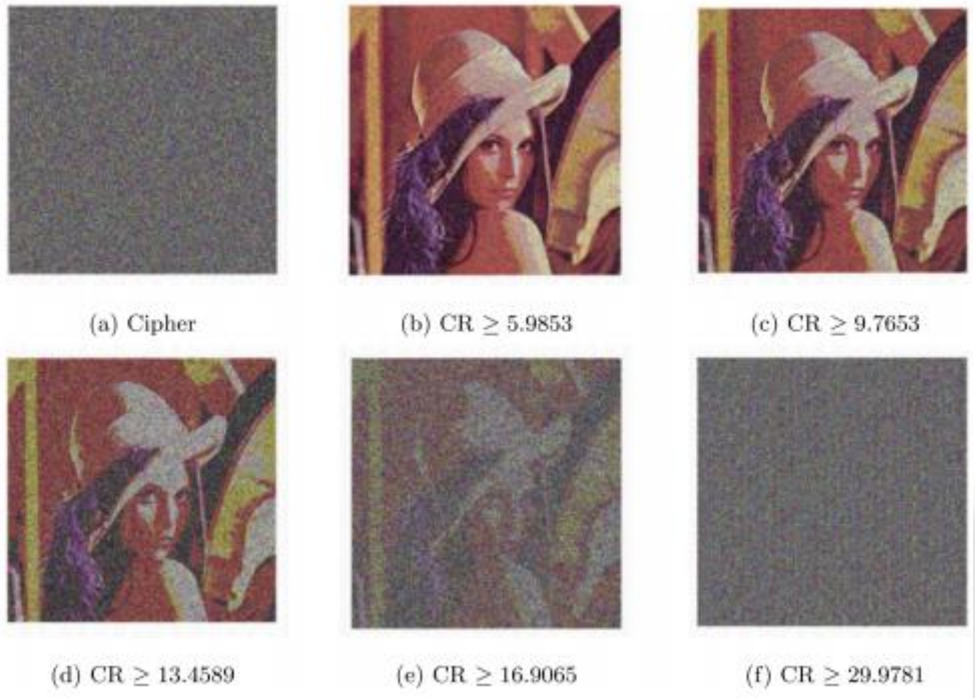


Fig. 10. Compression Ratio (CR) test (Lossless). (a) Cipher image, (b) CR ≥ 5.9853, (c) CR ≥ 9.7653, (d) CR ≥ 13.4589, (e) CR ≥ 16.9065, (f) CR ≥ 29.9781.

4. Conclusion

Improvement in the area of security in respect of images can be positively done with the help of diffusion technique. The diffusion technique is successful with the help of statistical trials. The 2D Sine Logistic map has better results when compared with the simple Logistic map technique. In this paper the model is observed with various test images as well as secret keys. The technique such as shuffling, diffusion and key search mechanism have given better results for the proposed algorithm. It has been shown that our proposed algorithm has given better outputs when compared with various existing algorithms.

References

1. Bansal, R., Gupta, S., & Sharma, G. (2017). An innovative image encryption scheme based on chaotic map and Vigenère scheme. *Multimedia Tools and Applications*, *76*(15), 16529-16562.
2. Ariatmanto, D., &Ernawan, F. (2020). An improved robust image watermarking by using different embedding strengths. *Multimedia Tools and Applications*, 1-27.
3. Abdelfatah, R. I., Nasr, M. E., &Alsharqawi, M. A. (2020). Encryption for multimedia based on chaotic map: Several scenarios. *Multimedia Tools and Applications*, *79*(27), 19717-19738.
4. Özkaynak, F. (2018). Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dynamics*, *92*(2), 305-313.
5. Guan, Z. H., Huang, F., & Guan, W. (2005). Chaos-based image encryption algorithm. *Physics letters A*, *346*(1-3), 153-157.
6. Kumar, M., Kumar, S., Budhiraja, R., Das, M. K., & Singh, S. (2016, March). Intertwining logistic map and Cellular Automata based color image encryption model. In *2016 international conference on computational techniques in information and communication technologies (ICCTICT)* (pp. 618-623). IEEE.
7. Akhavan, A., Samsudin, A., &Akhshani, A. (2017). Cryptanalysis of an image encryption algorithm

***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

based on DNA encoding. *Optics & Laser Technology*, *95*, 94-99.

8. Dou, Y., Liu, X., Fan, H., & Li, M. (2017). Cryptanalysis of a DNA and chaos based image encryption algorithm. *Optik*, *145*, 456-464.
9. UbaidurRahman, N. H., Balamurugan, C., &Mariappan, R. (2015). A novel DNA computing based encryption and decryption algorithm. *Procedia Computer Science*, *46*, 463-475.
10. Bhatnagar, G., Wu, Q. J., & Raman, B. (2013). Discrete fractional wavelet transform and its application to multiple encryption. *Information Sciences*, *223*, 297-316.
11. Zhao, T., Ran, Q., Yuan, L., Chi, Y., & Ma, J. (2016). Security of image encryption scheme based on multi-parameter fractional Fourier transform. *Optics Communications*, *376*, 47-51.
12. Kumar, M., Kumar, S., Budhiraja, R., Das, M. K., & Singh, S. (2017). A cryptographic model based on a logistic map and a 3-D matrix. *journal of information security and applications*, *32*, 47-58.
13. Kumar, S., Kumar, M., Budhiraja, R., Das, M. K., & Singh, S. (2018). A cryptographic model for better information security. *Journal of information security and applications*, *43*, 123-138.
14. Liu, Y., Qin, Z., Liao, X., & Wu, J. (2020). Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled Sine map. Nonlinear Dynamics, 100(3), 2917-2931.
15. Mondal, B., Behera, P. K., &Gangopadhyay, S. (2020). A secure image encryption scheme based on a novel 2D sine–cosine cross-chaotic (SC3) map. Journal of Real-Time Image Processing, 1-18.
16. Li, Y., Wang, C., & Chen, H. (2017). A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering*, *90*, 238-246.
17. Patidar, V., Pareek, N. K., &Sud, K. K. (2009). A new substitution–diffusion based image cipher using chaotic standard and logistic maps. *Communications in Nonlinear Science and Numerical Simulation*, *14*(7), 3056-3075.
18. Wu, Y., Noonan, J. P., Yang, G., & Jin, H. (2012). Image encryption using the two-dimensional logistic chaotic map. Journal of Electronic Imaging, 21(1), 013014.
19. Hua, Z., Zhou, Y., Pun, C. M., & Chen, C. P. (2015). 2D Sine Logistic modulation map for image encryption. Information Sciences, 297, 80-94.
20. Hua, Z., & Zhou, Y. (2016). Image encryption using 2D Logistic-adjusted-Sine map. Information Sciences, 339, 237-253.
21. Subodh Kumar, Rajendra Kumar, (2019). A Modified Image Encryption Technique Using Two Dimensional Sine Logistic Map. *International Journal of Computer Sciences and Engineering*, 7(3), 1110-1115.
22. Sharma, M. (2020). Image encryption based on a new 2D logistic adjusted logistic map. Multimedia Tools and Applications, 79(1), 355-374.
23. Zhang, G., Ding, W., & Li, L. (2020). Image encryption algorithm based on tent delay-sine cascade with logistic map. Symmetry, 12(3), 355.
24. Fu, C., Meng, W. H., Zhan, Y. F., Zhu, Z. L., Lau, F. C., Chi, K. T., & Ma, H. F. (2013). An efficient and secure medical image protection scheme based on chaotic maps. *Computers in biology and medicine*, *43*(8), 1000-1010.
25. Chen, J. X., Zhu, Z. L., Fu, C., & Yu, H. (2014). A fast image encryption scheme with a novel pixel swapping-based confusion approach. *Nonlinear Dynamics*, *77*(4), 1191-1207.
26. Zhang, L. Y., Zhang, Y., Liu, Y., Yang, A., & Chen, G. (2017). Security analysis of some diffusion mechanisms used in chaotic ciphers. *International Journal of Bifurcation and Chaos*, *27*(10), 1750155.
27. Wang, X., Li, B., Wang, Y., Lei, J., &Xue, J. (2021). An efficient batch images encryption method based on DNA encoding and PWLCM. *Multimedia Tools and Applications*, *80*(1), 943-971.
28. Liu, Y., Jiang, Z., Xu, X., Zhang, F., &Xu, J. (2020). Optical image encryption algorithm based on hyper-chaos and public-key cryptography. *Optics & Laser Technology*, *127*, 106171.
29. Amani, H. R., &Yaghoobi, M. (2019). A new approach in adaptive encryption algorithm for color images based on DNA sequence operation and hyper-chaotic system. *Multimedia Tools and Applications*, *78*(15), 21537-21556.
30. Soltanzadeh, P., &Hashemzadeh, M. (2021). RCSMOTE: range-controlled synthetic minority over-sampling technique for handling the class imbalance problem. *Information Sciences, 542,* 92-111.
31. Huang, X. (2012). Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dynamics*, *67*(4), 2411-2417.

32. Young, L. S. (1982). Dimension, entropy and Lyapunov exponents. *Ergodic theory and dynamical systems*, *2*(1), 109-124.
33. Huang, C. K., &Nien, H. H. (2009). Multi chaotic systems based pixel shuffle for image encryption. *Optics communications*, *282*(11), 2123-2127.
34. Kadir, A., Hamdulla, A., &Guo, W. Q. (2014). Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Optik*, *125*(5), 1671-1675.
35. Biswas, P., Kandar, S., &Dhara, B. C. (2020). An image encryption scheme using sequence generated by interval bisection of polynomial function. *Multimedia Tools and Applications*, *79*(43), 31715-31738.
36. Karmouni, H., Sayyouri, M., &Qjidaa, H. (2021). A novel image encryption method based on fractional discrete Meixner moments. *Optics and Lasers in Engineering*, *137*, 106346.
37. Kaur, M., & Kumar, V. (2018). Fourier–Mellin moment-based intertwining map for image encryption. *Modern Physics Letters B*, *32*(09), 1850115.
38. Nematzadeh, H., Enayatifar, R., Motameni, H., Guimarães, F. G., & Coelho, V. N. (2018). Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. *Optics and Lasers in Engineering*, *110*, 24-32.
39. Zhang, Y. (2020). The fast image encryption algorithm based on lifting scheme and chaos. *Information Sciences*, *520*, 177-194.
40. Kumar, V. and Kumar, R., 2015. An adaptive approach for detection of blackhole attack in mobile ad hoc network. Procedia Computer Science, 48, pp.472-479.
41. Kumar, V. and Kumar, R., 2015. An optimal authentication protocol using certificateless ID-based signature in MANET. In Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3 (pp. 110-121). Springer International Publishing.
42. Kumar, V. and Kumar, R., 2015, April. Detection of phishing attack using visual cryptography in ad hoc network. In 2015 International Conference on Communications and Signal Processing (ICCSP) (pp. 1021-1025). IEEE.
43. Kumar, V., Shankar, M., Tripathi, A.M., Yadav, V., Rai, A.K., Khan, U. and Rahul, M., 2022. Prevention of Blackhole Attack in MANET using Certificateless Signature Scheme. Journal of Scientific & Industrial Research, 81(10), pp.1061-1072.
44. Farah, M. B., Guesmi, R., Kachouri, A., &Samet, M. (2020). A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. *Optics & Laser Technology*, *121*, 105777.
45. Wang, S., Wang, C., &Xu, C. (2020). An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm. *Optics and Lasers in Engineering*, *128*, 105995.
46. Liu, Y., Jiang, Z., Xu, X., Zhang, F., &Xu, J. (2020). Optical image encryption algorithm based on hyper-chaos and public-key cryptography. *Optics & Laser Technology*, *127*, 106171.
47. Belazi, A., Abd El-Latif, A. A., Diaconu, A. V., Rhouma, R., &Belghith, S. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Optics and Lasers in Engineering*, *88*, 37-50.
48. Kaur, G., Agarwal, R., &Patidar, V. (2020). Chaos based multiple order optical transform for 2D image encryption. *Engineering Science and Technology, an International Journal*, *23*(5), 998-1014.