AMCSFFT-CIE: Alternate Multi-dimensional Chaotic Structure and Fast Fourier Transform based Novel Approach to Color Image Encryption

Mohit Dua[1*], Shelza Dua[2], Priyanka Jaroli[3]

[1]Department of computer Engineering, NIT Kurukshetra, Haryana, India
[2]Department of Electronics and Communication Engineering, NIT Kurukshetra, India
[3]Department of Computer Science, Banasthali University, Newai, India
er.mohitdua@nitkkr.ac.in, shelza_ecn@yahoo.com, Priyanka.jaroli@gmail.com
Corresponding Author: *Mohit Dua

Abstract: Low-dimensional chaotic maps are used for encrypting images because of their simplicity and low implementation cost. However, such chaotic systems are less secure and are slow in encryption speed as compared to multi-dimensional chaotic systems. This paper proposes the combination of spatial domain and frequency domain for image encryption. The proposed combination uses Four-dimensional chaotic map Lorenz System (LS) for key generation and alternate logistic structure for permutation-diffusion process. Initially, Lorenz System (LS) generates the security key using matrices color image's R, G, and B components. Secondly, one dimensional and two dimensional chaotic structures are used to generate a chaos matrix i.e. the two logistic maps are iterated alternately for diffusing the matrix. Finally, the diffused plain image matrix is encoded into the phase and amplitude of the composite function which is encrypted with white noise distribution by using the fast Fourier transform. The simulated outcomes describe that the proposed approach increases the key space value, encryption speed and resists brute force attacks.
Keywords: Image encryption, LS, Alternate logistic structure, LM, MDCS, FFT.

1. Introduction

Nowadays, anyone can be connected to the networks and devices that are present at different locations. The frequent use of internet has increased the requirement of the digital information security [1]. The digital information can be exchanged in different forms such text, image, audio, video etc. [2]. Unlike textual data, the digital image information has more peculiar features like size variability, highly redundant and strongly correlated pixels [3]. Also, transmissions of digital images over networks require the strong real-time property. Hence, a fast and secure encryption algorithm is an important area of research [4]. Traditional encryption algorithms like Data Encryption Standard (DES) [5], Two Fish cipher, International Data Encryption Algorithm (IDEA) [6] and Advanced Encryption Standard (AES) [7,8] are no more considered convenient and secure to encrypt digital image data. During the last two decades, a number of techniques had been suggested by researchers to secure the image information using conventional chaotic maps, multidimensional chaos and chaos based hybrid approaches [9,10].

Chaos is a nonlinear dynamics encryption technique and was discovered by Edward Lorenz in 1970. Lorenz used chaos theory to work on the weather prediction problem [10]. The chaos theory has a lot of attributes like ergodicity, sensitive to the initial condition, behavior dynamicity, Lyapunov exponent, nature unpredictability and strong computing ability [11]. Chaotic systems are based on two basic principles i.e. confusion and diffusion. A highly secure image encryption algorithm is obtained using these two stages [12]. The two-stage chaos based image encryption scheme is implemented by generating a security key and using this secure key to perform alternative element encryption. The encryption algorithm uses random bit sequences to create confusion-diffusion in image pixels. One-dimensional (1D), two-dimensional (2D) and three-dimensional (3D) are the commonly used chaotic maps, that are used to generate the secret key.

Received: November 20th, 2020. Accepted: December 24th, 2021
DOI: 10.15676/ijeei.2021.13.4.9

The encryption structure of the one-dimensional chaotic system is simple to implement. However, techniques like non-linear prediction or phase regression can easily be applied to cryptanalyze these maps. Therefore, the multi-dimensional technologies have emerged. In recent years, many advance researches of generating a random bit sequence and multi-dimensional chaotic system have been proposed [13-16]. The multi-dimensional chaotic maps are considered more safe and efficient than one-dimension chaos maps for information encryption [17]. These maps provide better performance and the large chaotic range in comparison to previously proposed chaotic maps. Multi-dimensional maps that use four dimensional differential equations endures chaotic state in large range [18]. The classic three-dimensional differential equation forms the basis of four-dimensional differential non-linear equations. The random bit sequence produced by the four-dimensional equations is more complex, secure and has an impact on efficiency of image encryption technique [19].

In [20], an improved technique based on multi-dimensional chaotic structure has been proposed to secure images from different attacks. The algorithm uses four-dimensional differential equation to produce a random bit sequence that iterates the chaotic equation $(3 * M * N)/4$ times. This iteration is used for diffusion of a color image in single round. Fast Fourier transform is an efficient processing method for converting spatial domain to frequency domain [21]. The numbers of pixels in spatial domain are used to denote number of frequencies in the frequency domain [22] and the algorithm claims to have large key space and security key, that is enough to resist attacks.

The work proposed in this paper uses Alternate Multi-dimensional Chaos Structure (AMCS) and Fast Fourier Transform (FFT) to encrypt color images. Lorenz System (LS) based Four-dimensional equations, and Alternate of one and two-dimensional Logistic map (LM) structures have been exploited to develop the encryption scheme. Initially, Lorenz System (LS) generates the security key using matrices of R, G, and B components of color image. Secondly, one-dimensional and two-dimensional chaotic structures are used to generate a chaos matrix i.e. two logistic maps are iterated alternately for diffusing the matrix. Finally, the diffused plain image matrix is encoded into the phase and amplitude of the composite function which is encrypted with white noise distribution by using the fast Fourier transform. It reduces the correlation between components, enhances security and encryption performance.

Rest of the paper is structured as: the next section of the paper describes the preliminaries of logistic chaotic mapping structure, four dimensional differential chaotic equations and Fast Fourier Transform. The proposed encryption framework is given in Section 3. Section 4 outlines the experimental details and results, and Section 5 discusses the conclusion.

2. Preliminaries

The section provides the basic details of the various approaches that have been applied to develop the proposed image cryptosystem.

A. One-dimensional LM

Since the introduction of chaos based cryptography, many chaotic maps have been proposed [23]. However, out of all these proposed chaos maps, Logistic map (LM) is considered to be the simplest and extensively accepted chaos map for developing information hiding algorithms. This map is easy to implement, is more stable and has less computation overhead, which is good for representing intricate dynamic behavior [24]. It can be mathematically expressed as:

$$z_{j+1} = v z_j (1 - z_j) \quad (1)$$

where, z_j ranges from 0 to 1 and the dynamicity of z_j is decided by the value of the parameter v. The range of $3.56 < v \leq 4$ makes the LM show complete dynamic behavior. For the implemented work v is taken as 3.9989 [25].

B. Two-dimensional LM

Dynamic cryptosystem mostly employs the chaotic function with more than one dimension, as such type of function provides larger and more random secret key space than one-dimensional chaos function [21]. This paper adopts the two dimensional logistic map that is an extension of one dimensional logistic map [26]. It provides better key space, provides better dependency on the control parameter. However, it is more complex than the one dimensional logistic map [27]. A 2D LM has a huge Lyapunov exponent value as compared to the 1D LM, which represents that the 2D logistic map shows more dynamic behavior. Hence, it becomes difficult for the intruder to guess the secret information [25]. Two dimensional LM, as described by equation (2), has less periodic windows. Thus, it is a more convenient and secure method for encryption [28].

$$\begin{cases} x_{j+1} = x_j v_1\left(1 - x_j\right) + L_1 {y^2}_j \\ y_{j+1} = y_j v_2\left(1 - y_j\right) + L_2\left({x^2}_j + x_j y_j\right) \end{cases} \tag{2}$$

where $2.75 < v_1 \leq 3.4$, $2.75 < \mathrm{v}_2 \leq 3.45$, $0.15 < \mathrm{L}_1 \leq 0.21$ and $0.13 < \mathrm{L}_2 \leq 0.15$. In this equation (0,1) interval are used for the *x, y* and *z*. The secret key provides the initial values of the x_0, y_0 and the values for the v_1,v_2, L_1 , L_2 [25][28].

Lorenz System

In last two decades, researchers have proposed many novel chaos functions by extending the already existing chaos functions [29]. Likewise, three-dimensional differential equations given in equation (3) forms the basis of Four-dimensional chaotic equations of Lorenz System (LS) [30-31]:

$$\begin{cases} \dfrac{dx_1}{dt} = a\,(x_2 - x_1) \\ \dfrac{dx_2}{dt} = bx_1 + cx_2 + x_1 x_3 \\ \dfrac{dx_3}{dt} = dx_3 + x_1 x_2 \end{cases} \tag{3}$$

As given in equation (4), using system (3) and adding a first-order differential state equation with respect to $\frac{dx_4}{dt}$ results in a new 4D chaotic system of Lorenz System [19].

$$\begin{cases} \frac{dx_1}{dt} = a\,(x_2 - x_1) \\ \frac{dx_2}{dt} = bx_4 + cx_2 + dx_1 - x_1 x_3 - x_3 x_4 \\ \frac{dx_3}{dt} = fx_3 + x_2 x_4 + x_1 x_2 \\ \frac{dx_4}{dt} = gx_2 - ex_4 - 0.05 x_1 x_3 \end{cases} \tag{4}$$

Here, state variables are denoted by x_1, x_2, x_3, x_4 and constant parameters are denoted by a, b, c, d, e, f, g [20]. For the implemented system, $a = 16$, $b = 45$, $c = -2$, $d = 45$, $e = 16$, $f = -4$, $g = 16$ have been used and the initial condition are $(1, 1, 1, 1)$ for x_1, x_2, x_3, x_4. The 0.000001 steps size is used to implement the system. The equation (4) is combined by Two Lorenz Systems and the four exponents used, have the values 2.10, 0, -15.21, and-24.74. The complexity of the multi-dimensional chaotic system (MDCS) is higher than the traditional MDCS [20].

D. Fast Fourier Transform

In 1965, Fast Fourier transform was first considered by Cooley and Tukey [32]. FFT reduces the computational complexity and increase the potential of the algorithm. It works on each pixel of the image and transform into frequency domain, the significant computation cost of the procedure is saved [33]. Fast Fourier transform can be represented by using the equation (5).

$$P[m] = \sum_{s=0}^{S-1} p[s] e^{-i(2\pi mn/N)} \quad (5)$$

3. Proposed Algorithm

The architectural framework of the proposed color image cryptosystem is discussed in detail in this section of the paper. Figure 1 gives the diagrammatical representation of the proposed architecture. Firstly, the developed method splits the given input image into R, G, and B components, and applies Lorenz System (LS) to generate the security key for R, G, and B components of color image. Secondly, one dimensional and two dimensional chaotic structures are used to generate a chaos matrix by iterating the two Logistic maps alternately for diffusing the matrix. Finally, the diffused plain image matrix is encoded into the phase and amplitude of the composite function which is encrypted with white noise distribution by using the Fast Fourier Transform (FFT).

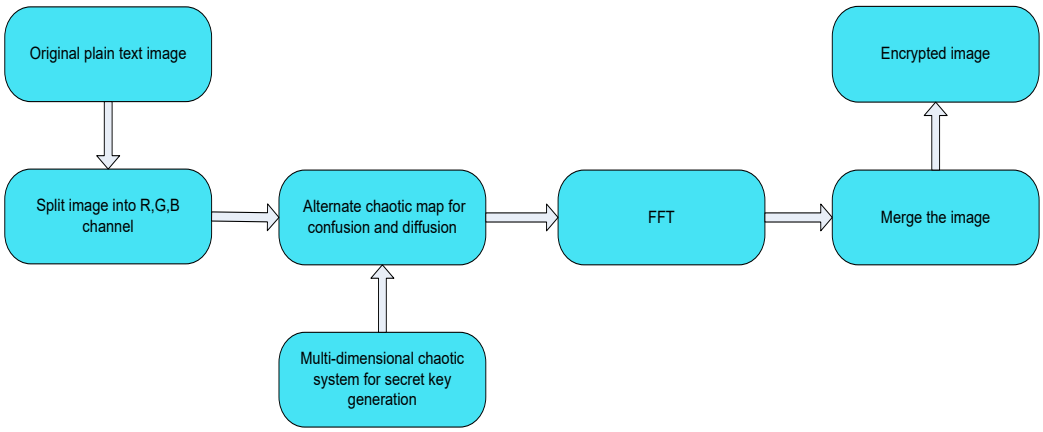


Figure 1: Proposed Approach to Image Encryption

A. Deterministic Random Bits Generator

The size of the input image is the deciding factor for the length of the key stream, in the proposed approach of image encryption. For a color image sizing $M \times N$, it generates $M \times N \times 3$ binary key streams. It reduces the time of encryption by using 4D equations to generate the key stream. Figure 2 gives the framework for the random bit generator, and Algorithm 1 describes the steps to generate it. The random bit sequences key1, key2 and key3 of length ($M \times N$ /3) are obtained. This sequence is used to encrypt $M \times N$ sized color image. For four dimensional differential chaotic systems, the Runga-Kutta method is used to generate a multi-dimensional chaotic sequence value.

Algorithm 1: Deterministic random bit generator
Step 1: Generate multi-dimensional chaotic sequence by using initial value ($x10$, $x20$, $x30$, $x40$) of chaotic system to iterate the equation (4) ($(M \times N)/3$+10) times and to obtain the random bit sequences, eliminate the first 10 group values. These initial values remove the transient effect of the bit generator.
Step 2: Quantize sequence obtained from step 1 by using every value of x_{j_i}, where $j = 1,2,3,4$ and $i = 1,2,3 \ldots . (M \times N)/3$. Use equation (6) and equation (7) to obtain the decimal part and integer part, respectively, of multi-dimensional chaos function.
$\emptyset x_{ji} = x_{j_i} - floor(x_{j_i})$ (6)
$x_{j_i} = mod(floor(\emptyset x_{j_i} \times 10^{14}), 65536)$ (7)

Step 3: Generate Key sequence, where x_{j_i} is given as:

$$x_{j_i} = s_{j_{i15}} * 2^{15} + s_{j_{i14}} * 2^{14} + s_{j_{i13}} * 2^{13} + \ldots\ldots + s_{j_{i1}} * 2^{1} + s_{j_{i0}} \quad (8)$$

Key1 is obtained from 1st to 8th bits of x_{1_i} , x_{2_i}, x_{3_i} is shown in equation (9).

$$\begin{cases} key1(k) = s_{1i_7} \times 2^7 + s_{1i_6} \times 2^6 + s_{1i_5} \times 2^5 + s_{1i_4} \times 2^4 + s_{1i_3} \times 2^3 + s_{1i_2} \times 2^2 + s_{1i_1} \times 2^1 + s_{1i_0} \\ key1(k+1) = s_{2i_7} \times 2^7 + s_{2i_6} \times 2^6 + s_{2i_5} \times 2^5 + s_{2i_4} \times 2^4 + s_{2i_3} \times 2^3 + s_{2i_2} \times 2^2 + s_{2i_1} \times 2^1 + s_{2i_0} \end{cases} \quad (9)$$

Key 2 obtained from 5th to 12th bits of x_{3_i} , x_{4_i}, x_{1_i} is shown in equation (10).

$$\begin{cases} key2(k) = s_{3i_{11}} \times 2^7 + s_{3i_{10}} \times 2^6 + s_{3i_9} \times 2^5 + s_{3i_8} \times 2^4 + s_{3i_7} \times 2^3 + s_{3i_6} \times 2^2 + s_{3i_5} \times 2^1 + s_{3i_4} \\ key2(k+1) = s_{4i_{11}} \times 2^7 + s_{4i_{10}} \times 2^6 + s_{4i_9} \times 2^5 + s_{4i_8} \times 2^4 + s_{4i_7} \times 2^3 + s_{4i_6} \times 2^2 + s_{4i_5} \times 2^1 + s_{4i_4} \end{cases} \quad (10)$$

Key 3 is obtained from 9th to 16th bits of x_{2_i} , x_{3_i}, x_{4_i} is shown in equation (11).

$$\begin{cases} key3(k) = s_{2i_{15}} \times 2^7 + s_{2i_{14}} \times 2^6 + s_{2i_{13}} \times 2^5 + s_{2i_{12}} \times 2^4 + s_{2i_{11}} \times 2^3 + s_{2i_{10}} \times 2^2 + s_{2j_9} \times 2^1 + s_{2i_8} \\ key3(k+1) = s_{3i_{15}} \times 2^7 + s_{3i_{14}} \times 2^6 + s_{3i_{13}} \times 2^5 + s_{3i_{12}} \times 2^4 + s_{3i_{11}} \times 2^3 + s_{3i_{10}} \times 2^2 + s_{3j_{\cdot}} \times 2^1 + s_{3i} \end{cases} \quad (11)$$

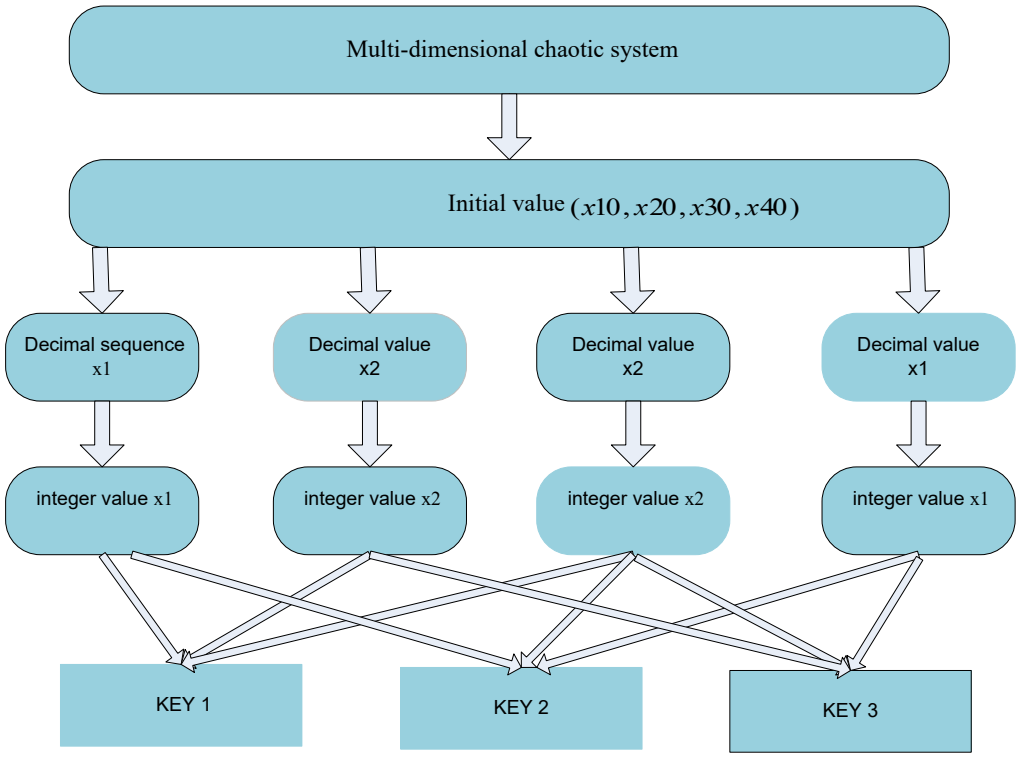


Figure 2. Proposed Random Bit Generator

B. Encryption

The color image (h) of size $M \times N$ is taken as input. The input color image is split into three pixel matrices h^r, h^g and h^b for R, G and B channels, respectively. The size of each pixel matrix is $M \times N$ and the range of pixels is from 0 to 255. The Rth pixel value of R, G and B matrix is denoted by h_R^r, h_R^g *and* h_R^b ($where\ R \in [0, M \times N - 1]$), respectively. Algorithm 2 gives the stepwise description of the proposed encryption technique.

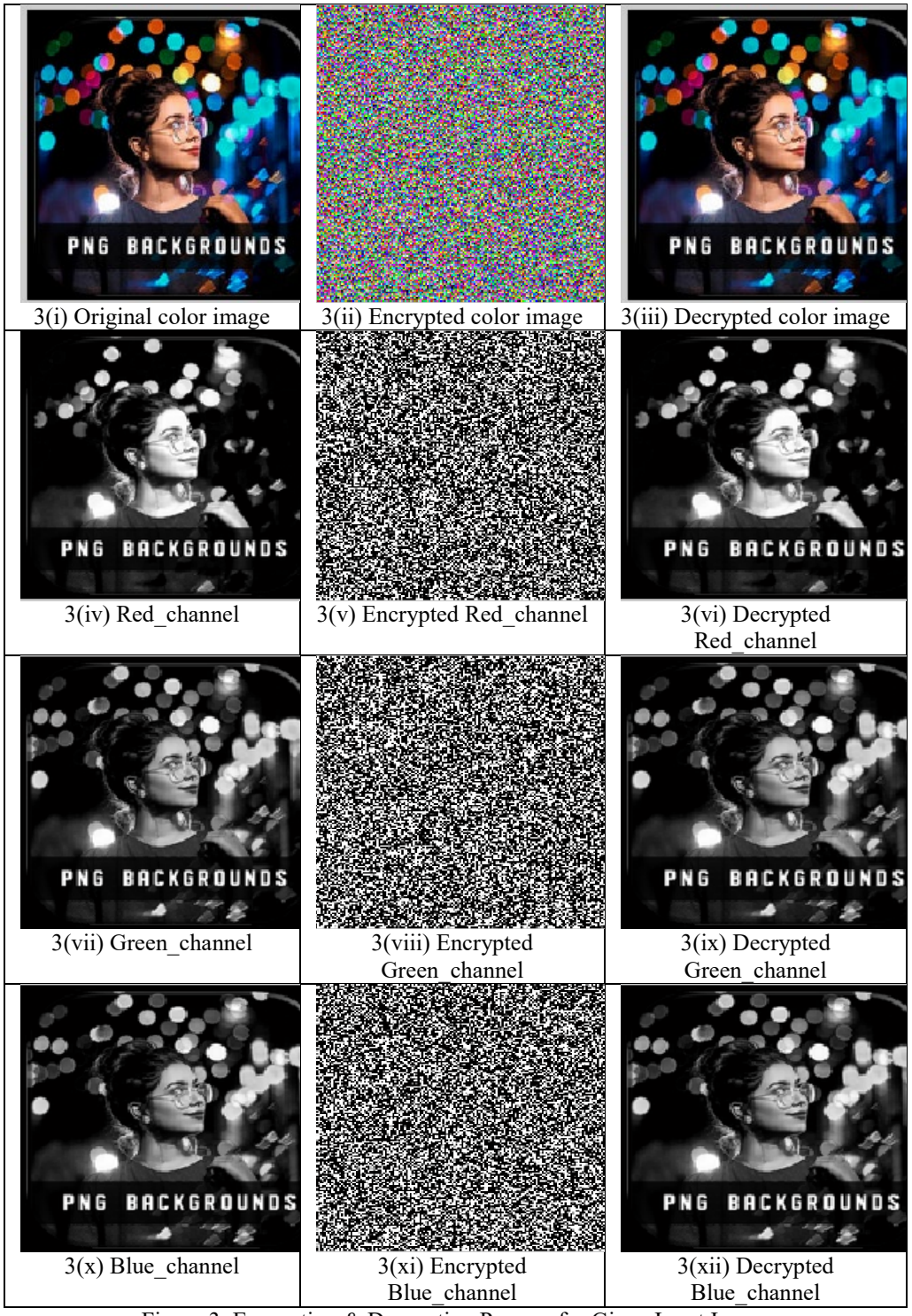
Algorithm 2: Proposed Encryption Algorithm
Step 1: Obtain matrix B by splitting the original plain image into R, G and B channels matrix h^r, h^g and h^b, respectively. Step 2:E_1, E_2, E_3 are determined for the all three channel of original color image h by using equations (12) to (14). After then transformed E_1, E_2, E_3 are obtained using equations (15) to (17) respectively. $E_1 = \sum_{j\epsilon[1-255]} h_j^r /(M \times N \times 255)$ (12) $E_2 = \sum_{j\epsilon[1-255]} h_j^g /(M \times N \times 255)$ (13) $E_3 = \sum_{j\epsilon[1-255]} h_j^b /(M \times N \times 255)$ (14) $\alpha = floor(mod((E_1 + E_2 + E_3) \times 10^{12}, 256))$ (15) $\beta = floor(mod(\frac{E_1+E_2+E_3}{2} \times 10^{12}, 256))$ (16) $\gamma = floor(mod(\frac{E_1+E_2+E_3}{3} \times 10^{12}, 256))$ (17) Step 3.Iterate Equation (2) and (1) using v, v_1,v_2, L_1, and L_2 the initial values of the x_0, y_0, and z_0 are used. In each iteration the new values x_j, y_j, z_j is obtained. Step 4. Continue iterating two-dimensional and one-dimensional equation alternately by using following sub-steps. Firstly, iterate equation (2) to obtain the values. Secondly, transform matrix to obtain the circular shift values. Thirdly, perform XOR operation between matrix B and transform matrix. Finally, continuously iterate equation (1). Step 5: Obtain the diffused image A by diffusing the values of R, G and B channels. $A(x,z) = \big(D(x,z) + A(x,z-1)\big) mod 256, z\epsilon\ [2, M \times N]$ (18) where $A(x,z-1)$ and $D(x,z)$ are the previous and current values of the channels, respectively. Step 6: Perform the Fast Fourier Transform to obtain the final encrypted image.

C. Decryption

Decryption algorithm, inverse of proposed encryption, is also performed in various steps, starting from bottom to the step first. Firstly, perform the inverse Fast Fourier Transform followed by the reverse diffusion phase. After jth iteration, the output to recovers the plain image. By following this procedure, the rows and columns of the original matrix are obtained and at last the original plaintext image with the size of ($M \times N$) is recovered.

4. Simulation Setup and Security Analysis

The proposed work has been carried out using simulator MATLAB version 8.1 (R2013a) on i-3 processor based system. The security analysis of multidimensional function with alternate logistic map and Fast Fourier Transform is done by using the parametric values as v = 3.99, v_1 =3.39, v_2= 3.4489, L_1= 0.21, L_2= 0.15, x_0= 0.345, y_0= 0.365, z_0= 0.537. The original input image is shown in Figure 3(i) of size 512 × 512. Figures 3(ii) and Figure 3(iii) show the corresponding encrypted and decrypted color images, respectively. Similarly, Figure 3(iv), Figure 3(vii) and Figure 3(x) show the channel wise input images. Corresponding to red channel input image shown in Figure 3(iv), Figure 3(v) gives the encrypted image and Figure 3(vi) gives the decrypted image. Corresponding to green channel input image shown in Figure 3(vii), Figure 3(viii) gives the encrypted image and Figure 3(ix) gives the decrypted image. Corresponding to blue channel input image shown in Figure 3(x), Figure 3(xi) gives the encrypted image and Figure 3(xii) gives the decrypted image.



3(i) Original color image	3(ii) Encrypted color image	3(iii) Decrypted color image
3(iv) Red_channel	3(v) Encrypted Red_channel	3(vi) Decrypted Red_channel
3(vii) Green_channel	3(viii) Encrypted Green_channel	3(ix) Decrypted Green_channel
3(x) Blue_channel	3(xi) Encrypted Blue_channel	3(xii) Decrypted Blue_channel

Figure 3. Encryption & Decryption Process for Given Input Image

A. Generation of Cryptosystem Key Evaluation

The key size of the implemented cryptosystem increases exponentially. It also depends on the seed values of the system [34-35]. The proposed cryptosystem uses multi-dimensional

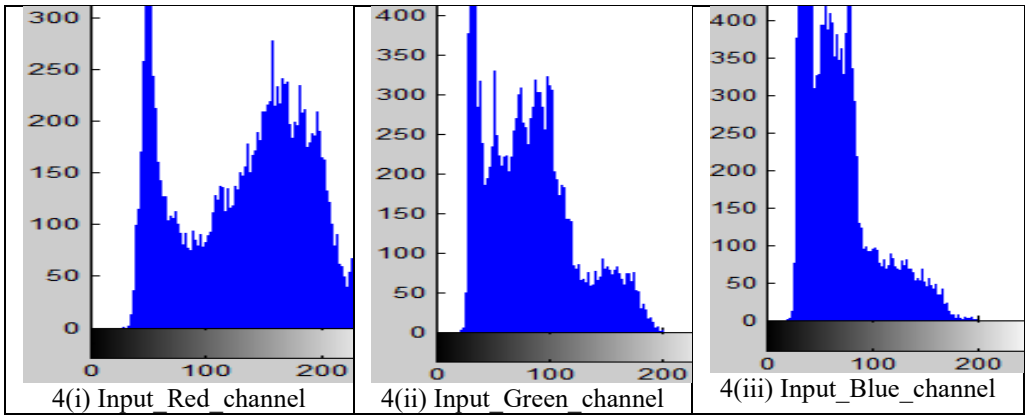
chaotic system with alternate one dimensional and two dimensional which has eight initial values v, v_1 v_2, L_1, L_2, x_0, y_0, z_0, therefore the key size of the system is $10^{14\times3}$, which is higher than 2^{186}. The precision for this is10^{-15}. The proposed system has the key space size is approximately 10^{164}, which is capable enough to avoid the brute force attack.

B. Statistical Evaluation

Statistical evaluation describes the closeness between the original and encrypted image. The encrypted output should be totally different from the original input. The two tests that are used for statistical evaluations are, histogram and correlation distribution [36].

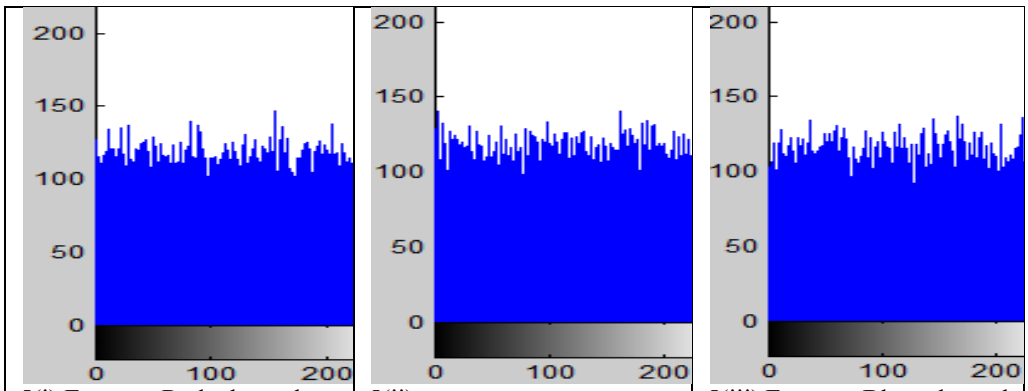
B.1. Histogram Evaluation

The histogram evaluation describes the pixel distribution of the image and is represented by plotting graph [37]. Normally, for the original plaintext images, the plotted graph is precarious while for the encrypted images graph is uniform. Hence, it is difficult to identify the intensity level at different part of the images for an encrypted image [36-37]. Figures 4(i) to 4(iii) describe the channel wise (i.e. red, green and blue channels) histograms of the original input image, and Figures 5(i) to 5(iii) show the corresponding channel wise histograms for red, green and blue channels of the encrypted image. The uniform histogram distribution of encrypted images reveal that the proposed method is capable of resisting attacks.



4(i) Input_Red_channel 4(ii) Input_Green_channel 4(iii) Input_Blue_channel

Figure 4. Input Image Histograms

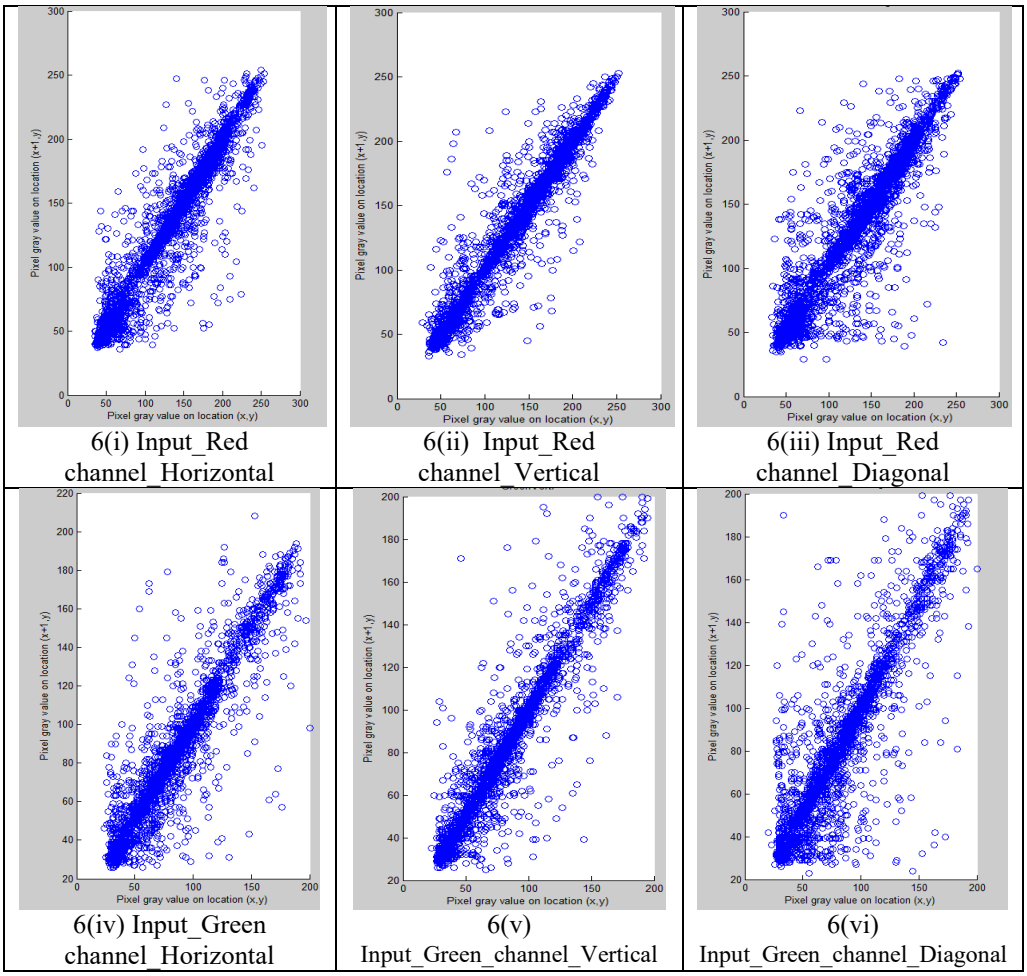


5(i) Encrypt_Red_channel 5(ii) Encrypt_Green_channel 5(iii) Encrypt_Blue_channel

Figure 5. Encrypted Image Histograms

B.2. Correlation Distribution Evaluation

The correlation evaluation between the neighboring pixels of the original image is higher, whereas the correlation between the encrypted image pixels is low in comparison to original plaintext image pixels [38]. Correlation is evaluated between two vertically, horizontally and diagonally placed neighbor pixels. Figure 6 shows the channel (i.e. red, green and blue) and dimension (i.e. horizontal, vertical and diagonal) wise correlation distribution of the input image. Figure 7 shows of the corresponding red, blue and green channel wise correlation distribution, and horizontal, vertical and diagonal dimension wise correlation distribution of the encrypted image. It can be observed from the shown distribution that it becomes hard to predict relationship among the pixels in each dimension after encryption is performed using the proposed approach.



6(i) Input_Red channel_Horizontal

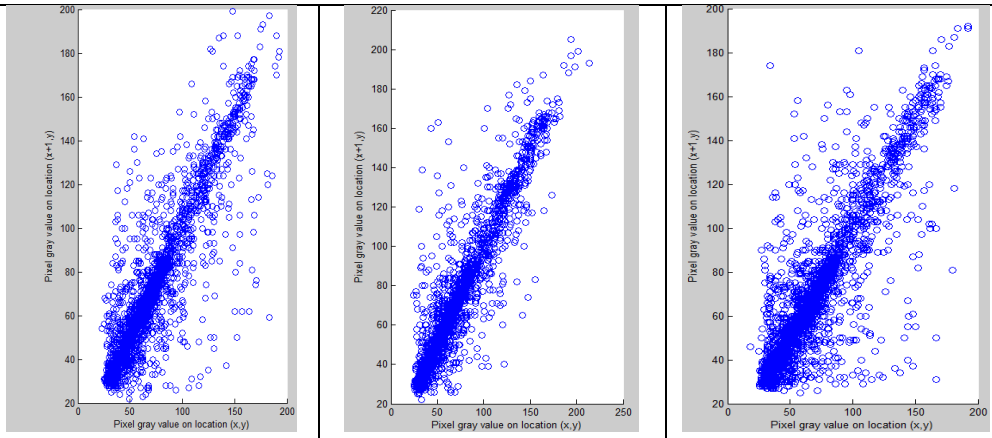
6(ii) Input_Red channel_Vertical

6(iii) Input_Red channel_Diagonal

6(iv) Input_Green channel_Horizontal

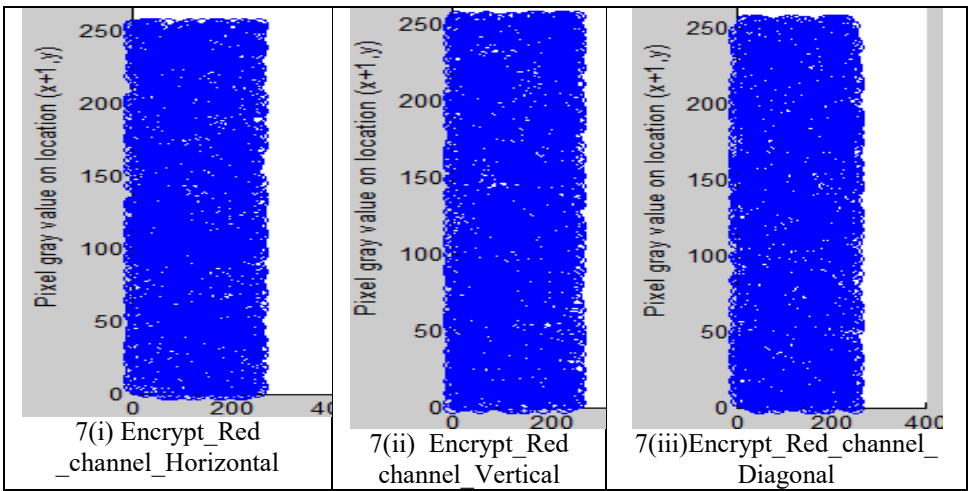
6(v) Input_Green_channel_Vertical

6(vi) Input_Green_channel_Diagonal



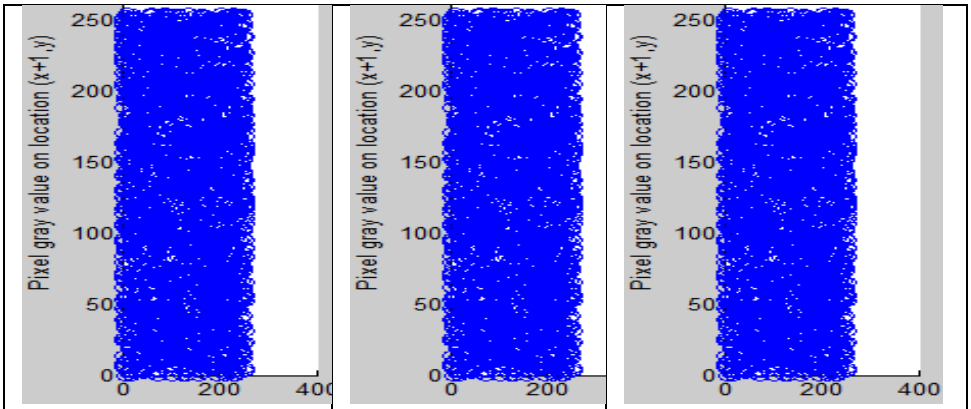
6(vii) Input_Blue_channel_Horizontal | 6(viii) Input_Blue_channel_Vertical | 6(ix) Input_Blue_channel_Diagonal

Figure 6. Channel and Dimension Wise Correlation distribution of Original Color Image



7(i) Encrypt_Red _channel_Horizontal | 7(ii) Encrypt_Red channel_Vertical | 7(iii)Encrypt_Red_channel_ Diagonal

7(iv) Encrypt_Green_channel_ Horizontal | 7(v) Encrypt_Green_ channel_Vertical | 7(vi) Encrypted Green_channel_diagonal



7(vii) Encrypt_Blue_channel_ Horizontal | 7(viii) Encrypt_Blue_channel _Vertical | 7(ix) Encrypt_Blue_channel_ Diagonal

Figure 7. Channel and Dimension Wise Correlation distribution of Encrypted Color Image

C. Correlation Coefficient Evaluation

Encrypted images should eliminate the drawback of the high correlation between pixels. Correlation is analyzed between two adjacent pixels in three dimensions i.e. horizontally, vertically and diagonally adjacent pixels [39]. The correlation coefficient of the encrypted image should be minimum such that the proposed algorithm should be highly efficient and has capability to resist the attack [40]. It is mathematically expressed using equations (19) to (21). Table 1 gives the correlation coefficient for the cipher image in all diagonal, vertical and horizontal directions for each channel i.e. red, green and blue channel. It can be observed from the obtained results that all values are approaching the value zero, which indicates a good encryption efficiency of the proposed approach.

$$A_{c,d} = \frac{cov(c,d)}{\sqrt{D(c)}\sqrt{D(d)}} \tag{19}$$

where,

$$E(c) = \frac{1}{N}\sum_{i=1}^{k}(c_i) \tag{20}$$

$$D(d) = \frac{1}{N}\sum_{i=1}^{k}(c_i - E(c))^2 \tag{21}$$

Table 1. Channel wise Correlation Coefficient

Channels	Correlation Coefficient (CC)		
	Diagonal	Vertical	Horizontal
Red_channel	0.0126	-0.0125	0.0040
Green_channel	0.0118	-0.0061	0.0044
Blue_channel	0.0223	0.0022	-0.0013

D. Entropy Evaluation

Entropy evaluation describes the security strength of an encryption algorithm. A good encryption algorithm has a higher entropy value. The minimum entropy value is zero and maximum entropy value is 8 [41]. The entropy is calculated by using the following expression [29-30].

$$H(r) = -\sum_{i=1}^{2^N-1} R(p_j)\, log_2\, R(p_j) \tag{22}$$

Here, $R(p_j)$ denotes the probability. Table 2 gives the channel wise entropy values of the input and corresponding encrypted image for all three red, blue and green channels. Also, the average value has also been evaluated. It can be seen that the entropy value of the cipher image

for each channel, and average entropy value is very close to eight, which makes it difficult for the intruder to retrieve the information from the encrypted image.

Table 2. Channel wise Entropy

Image	Entropy	
	Original Image	Cipher or Encrypted Image
Red_channel	5.2541	7.9936
Green_channel	6.0786	7.9938
Blue_channel	6.4223	7.9929
Average	5.9183	7.9937

E. Differential Evaluation

The differential evaluation, attackers normally do a little change in the original image while this little change would a major change in the encrypted image. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are the two perceptible measures used to probe the performance an encryption algorithm against the differential attacks [41-42]. These are mathematically expressed as:

$$NPCR = \frac{\sum_{i,j} x(i,j)}{y \times z} \quad (23)$$

where $x(i,j)$ is a two-dimensional array.

$$UACI = \frac{1}{y \times z}\left[\sum_{i,j} \frac{|x_1(i,j) - x_1(i,j)|}{255}\right] \times 100\% \quad (24)$$

where, y and z are the width and height of the image. x_1 and x_2 are the encrypted images before and after one pixel of the color plain image is changed. Table 3 gives the NPCR and UACI values of the encrypted image for all three red, green and blue image components. The obtained value clearly indicate that the proposed approach has the ability to resist differential attacks.

Table 3. NPCR and UACI

Channel	NPCR	UACI
Red_channel	99.6540	30.0956
Green_channel	99.5433	30.8273
Blue_channel	99.5986	32.4349

F. PSNR and MSE

Peak signal to noise ratio (PSNR) and Mean Square Error (MSE) are the two measures applied to analyze encryption and decryption effectiveness. MSE criteria measures the error between the input image and encrypted image [43]. These are evaluated by computing the following equations.

Table 4. PSNR and MSE

Channel	PSNR		MSE	
	Encrypted Image	Decrypted Image	Encrypted Image	Decrypted Image
Red_channel	9.1554	39.2612	7.2063+03	8.6752
Green_channel	9.2332	39.9876	7.6544+03	8.7265
Blue_channel	9.2583	36.4683	8.8381+03	9.1978

$$\text{Peak signal to noise ratio (PSNR)} = 20 \times \log_{10}\left(\frac{I_{max}}{\sqrt{MSE}}\right). \quad (25)$$

$$MSE = \frac{1}{N}\sum_{i=1}^{n}(h'_i - h_i) \quad (26)$$

Here h' is the original input image and h is the encrypted output image. Table 4 represents the PSNR and MSE values of the red, green and blue component in encryption. It can be observed from the obtained results that the proposed approach has a good decryption efficiency.

G. Encryption Speed Evaluation

Time evaluation is an important parameter in the image cryptosystem [44-45]. The implemented work also analyses the speed of the proposed image encryption algorithm on a personal computer (PC) with a CPU 2.10 GHz, 2 GB Memory (RAM) and the operating system is Microsoft Windows 7 ultimate using MATLAB version 8.1 (R2013a). Table 5 represents the encryption and key generation time taken by the all three components of the image.

Table 5. Key Generation & Encryption time

Channel	Key Generation Time (seconds)	Encryption Time (seconds)
Red channel	15.9535	52.2585
Green channel	15.9533	52.2128
Blue channel	15.6781	52,4667
Total time	16.1949	52.3126

H. Comparative Analysis

This section describes the comparatively analysis of the proposed scheme with the some of the existing encryption strategies. Table 6 shows the comparison by taking various security parameters such as the NPCR, UACI, CCH, CCV, CCD, Entropy, MSE, and PSNR into consideration. It can be observed from the given analysis that the proposed image cryptosystem is more secure, efficient and robust in handling various types of attacks.

Table 6. Comparative Analysis of the Proposed Approach with Existing Methods

Work	Color	NPCR	UACI	Correlation Coefficient			Entropy	MSE	PSNR	MSE	PSNR
				CCH	CCV	CCD		Encrypted Image		Decrypted Image	
Wang et al. [25]	R	99.63	33.43	0.0018	0.0016	0.0005	7.9926	-	-	-	-
	G	99.59	33.39	0.0004	0.0021	-0.0007	7.9934	-	-	-	-
	B	99.67	33.51	0.0029	0.0011	0.0037	7.9923	-	-	-	-
Suri et al. [47]	RGB	99.62	31.97	0.0148	0.0092	-0.0124	7.9968	-	-	-	-
Suri et. al. [48]	RGB	99.707	30.57	-	-	-	7.8091	-	-	-	-
Kumar et al. [46]	R	99.6212	33.4539	1.72e-4	6.08e-5	1.02e-5	7.9912	1.0519e+04	7.9109	-	-
	G	99.6380	33.4275	7.67e-6	2.38e-4	1.62e-4	7.9914	9.1034e+03	8.5388	-	-
	B	99.5930	33.4399	7.29e-5	1.21e-4	2.31e-4	7.9915	7.1417e+03	8.5928	-	-
Zhu et al. [49]	RGB	99.608	33.29	-0.0081	0.0035	-0.0368	7.9026	-	-	-	-
Zeng et al. [50]	RGB	99.635	33.56	0.0053	-0.0089	0.0126	7.9987	-	-	-	-
Proposed Scheme	R	99.6540	30.6956	0.0126	-0.0125	0.0040	7.9936	7.2063+03	9.1554	8.6752	39.2612
	G	99.5433	30.8273	0.0118	-0.0061	0.0044	7.9938	7.6544+03	9.2332	8.7265	39.9876
	B	99.5986	32.4349	0.0223	0.0022	-0.0013	7.9937	8.8381+03	9.2583	9.1978	36.4683

5. Conclusion

This paper discussed implementation of color image encryption scheme that uses alternate one and two-dimensional chaotic Logistic map (LM), four-dimensional differential equations based Lorenz System (LS) and Fast Fourier Transform (FFT). The proposed approach divides the color image into red, green and blue channel, and generates the security key using four-dimensional differential equations with LS in its first stage. It encrypts the original color image using Logistic one dimensional and two dimensional chaotic functions alternatively, and Fast Fourier Transform. The proposed method has been evaluated using various standard parameters. It can be observed from the obtained results that the proposed image encryption scheme is secure and has the ability to resist different types of attack. The work can be further extended by replacing the Logistic map, that has been applied alternatively in the proposed scheme, with more powerful chaos functions.

6. References

[1]. Priya R Sankpal, P. A. Vijaya (2014). Image Encryption Using Chaotic Maps: A Survey. *Fifth International Conference on Signals and Image Processing. IEEE.*

[2]. John Justin, M., & Manimurugan, S. (2012). A survey on various encryption techniques. *International Journal of Soft Computing and Engineering (IJSCE)* ISSN, 2231, 2307.

[3]. Jung, K., Kim, K. I., & Jain, A. K. (2004). Text information extraction in images and video: a survey. Pattern recognition, 37(5), 977-997.

[4]. Soleymani, A., Ali, Z. M., & Nordin, M. J. (2012, June). A survey on principal aspects of secure image transmission. *In Proceedings of World Academy of Science, Engineering and Technology (No. 66). World Academy of Science, Engineering and Technology*.

[5]. Subramanyan, B., Chhabria, V. M., & Babu, T. S. (2011, February). Image encryption based on AES key expansion. In Emerging Applications of Information Technology (EAIT), 2011 *Second International Conference on (pp. 217-220). IEEE.*

[6]. Kamali, S. H., Shakerian, R., Hedayati, M., & Rahmani, M. (2010, August). A new modified version of advanced encryption standard based algorithm for image encryption. *In Electronics and Information Engineering (ICEIE), 2010 International Conference* On (Vol. 1, pp. V1-141). IEEE.

[7]. Zeghid, M., Machhout, M., Khriji, L., Baganne, A., & Tourki, R. (2007). A modified AES based algorithm for image encryption. *International Journal of Computer Science and Engineering*, 1(1), 70-75.

[8]. Hoang, T. (2012, February). An efficient FPGA implementation of the Advanced Encryption Standard algorithm. In Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), 2012 IEEE RIVF *International Conference on* (pp. 1-4). IEEE.

[9]. Han, Z., Feng, W. X., Hui, L. Z., Da Hai, L., & Chou, L. Y. (2003, October). A new image encryption algorithm based on chaos system. In Robotics, intelligent systems and signal processing, 2003. *Proceedings. 2003 IEEE international conference on (Vol. 2, pp. 778-782). IEEE.*

[10]. Lorenz, E. N. (1995). The essence of chaos. University of Washington Press.

[11]. Qi, G., Chen, G., Du, S., Chen, Z., & Yuan, Z. (2005). Analysis of a new chaotic system. Physica A: Statistical Mechanics and its Applications, 352(2), 295-308.

[12]. Sankpal, P. R., & Vijaya, P. A. (2014, January). Image encryption using chaotic maps: a survey. *In Signal and Image Processing (ICSIP), 2014 Fifth International Conference on (pp. 102-107). IEEE*

[13]. Ahmad, M., & Alam, M. S. (2009). A new algorithm of encryption and decryption of images using chaotic mapping. *International Journal on computer science and engineering, 2(1), 46-50.*

[14]. Mazloom, S., & Eftekhari-Moghadam, A. M. (2009). Color image encryption based on coupled nonlinear chaotic map. Chaos, Solitons & Fractals, 42(3), 1745-1754.

[15]. Enayatifar, R., Abdullah, A. H., & Isnin, I. F. (2014). Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Optics and Lasers in Engineering, 56, 83-93.

[16]. Pak, C., & Huang, L. (2017). A new color image encryption using combination of the 1D chaotic map. Signal Processing, 138, 129-137

[17]. Han, Z., Feng, W. X., Hui, L. Z., Da Hai, L., & Chou, L. Y. (2003, October). A new image encryption algorithm based on chaos system. In Robotics, intelligent systems and signal processing, 2003. Proceedings. *2003 IEEE international conference on (Vol. 2, pp. 778-782). IEEE.*

[18]. (18)Yang, Y. G., Tian, J., Lei, H., Zhou, Y. H., & Shi, W. M. (2016). Novel quantum image encryption using one-dimensional quantum cellular automata. Information Sciences, 345, 257-270.

[19]. Yu, F., Gao, L., Gu, K., Yin, B., Wan, Q., & Zhou, Z. (2017). A fully qualified four-wing four-dimensional autonomous chaotic system and its synchronization. *Optik-International Journal for Light and Electron Optics, 131, 79-88.*

[20]. Tong, X. J., Zhang, M., Wang, Z., Liu, Y., Xu, H., & Ma, J. (2015). A fast encryption algorithm of color image based on four-dimensional chaotic system. *Journal of Visual Communication and Image Representation, 33, 219-234.*

[21]. Yuan, W., Yang, X., Guo, W., & Hu, W. (2017, July). A double-domain image encryption using hyper chaos. *In 2017 19th International Conference on Transparent Optical Networks (ICTON) (pp. 1-4). IEEE.*

[22]. Liu, L., Hao, S., Lin, J., Wang, Z., Hu, X., & Miao, S. (2017). Image block encryption algorithm based on chaotic maps. IET Signal Processing, 12(1), 22-30.

[23]. Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R. M., & Del Campo, O. A. (2015). A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Processing, 109, 119-131.

[24]. H.Y. Jia, Z.Q. Chen, Z.Z. Yuan, Generation and circuit implementation of a large range hyper-chaotic system, Acta Phys. Sin. 58 (7) (2009) 4469–4476.

[25]. Wang, X., Zhao, Y., Zhang, H., & Guo, K. (2016). A novel color image encryption scheme using alternate chaotic mapping structure. Optics and Lasers in Engineering, 82, 79-86.

[26]. Zhang, X., Zhu, G., & Ma, S. (2012). Remote-sensing image encryption in hybrid domains. Optics Communications, 285(7), 1736-1743.

[27]. Ahmad, M., & Alam, M. S. (2009). A new algorithm of encryption and decryption of images using chaotic mapping. *International Journal on computer science and engineering, 2(1), 46-50.*

[28]. Zhang, Y. Q., & Wang, X. Y. (2015). A new image encryption algorithm based on non-adjacent coupled map lattices. Applied Soft Computing, 26, 10-20.

[29]. Wang, X., & Wang, M. (2008). A hyperchaos generated from Lorenz system. Physica A: Statistical Mechanics and its Applications, 387(14), 3751-3758.

[30]. Liu, H., & Wang, X. (2011). Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Optics Communications, 284(16), 3895-3903.

[31]. Enayatifar, R., Abdullah, A. H., Isnin, I. F., Altameem, A., & Lee, M. (2017). Image encryption using a synchronous permutation-diffusion technique. Optics and Lasers in Engineering, 90, 146-154.

[32]. Weisstein, E. W. (2015). Fast fourier transform.

[33]. Cheung, C. K., Keough, G. E., Gross, R. H., & Landraitis, C. (2005). Getting started with Mathematica. J. Wiley.

[34]. Zhang, T. T., Yan, S. J., Gu, C. Y., Ren, R., & Liao, K. X. (2018, April). Research on Image Encryption Based on DNA Sequence and Chaos Theory. In Journal of Physics: Conference Series (Vol. 1004, No. 1, p. 012023). IOP Publishing.

[35]. Bisht, A., Dua, M., & Dua, S. (2019). A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random transform. *Journal of Ambient Intelligence and Humanized Computing*, *10*(9), 3519-3531.

[36]. Dua, M., Wesanekar, A., Gupta, V., Bhola, M., & Dua, S. (2020). Differential evolution optimization of intertwining logistic map-DNA based image encryption technique. *Journal of Ambient Intelligence and Humanized Computing*, *11*(9), 3771-3786.

[37]. Bisht, A., Dua, M., Dua, S., & Jaroli, P. (2020). A color image encryption technique based on bit-level permutation and alternate logistic maps. *Journal of Intelligent Systems*, *29*(1), 1246-1260.

[38]. Dua, M., Suthar, A., Garg, A., & Garg, V. (2021). An ILM-cosine transform-based improved approach to image encryption. *Complex & Intelligent Systems*, *7*(1), 327-343.

[39]. Kumar, A., & Dua, M. (2021). Novel pseudo random key & cosine transformed chaotic maps based satellite image encryption. *Multimedia Tools and Applications*, 1-21.

[40]. Niyat, A. Y., Moattar, M. H., & Torshiz, M. N. (2017). Color image encryption based on hybrid hyper-chaotic system and cellular automata. Optics and Lasers in Engineering, 90, 225-237.
[41]. Bisht, A., Dua, M., & Dua, S. (2019). A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random transform. *Journal of Ambient Intelligence and Humanized Computing*, *10*(9), 3519-3531.
[42]. Pankaj, S., & Dua, M. (2021). A novel ToCC map and two-level scrambling-based medical image encryption technique. Network Modeling Analysis in Health Informatics and Bioinformatics, 10(1), 1-19.
[43]. Dua, M., Dua, S., Jaroli, P., & Bisht, A. (2021). An Improved Approach for Multiple Image Encryption Using Alternate Multidimensional Chaos and Lorenz Attractor. In Handbook of Research on Machine Learning Techniques for Pattern Recognition and Information Security (pp. 139-156). IGI Global.
[44]. Kar, M., Mandal, M. K., & Nandi, D. (2017, November). RGB image encryption using hyper chaotic system. In 2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN) (pp. 354-359). IEEE.
[45]. Suneja, K., Dua, S., & Dua, M. (2019, March). A review of chaos based image encryption. *In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 693-698). IEEE.*
[46]. Kumar, M., Sathish, G., Alphonse, M., & Lahcen, R. A. M. (2019). A new RGB image encryption using generalized heat equation associated with generalized Vigen è $\grave {e} $ re-type table over symmetric group. Multimedia Tools and Applications, 78(19), 28025-28061.
[47]. Suri, S., & Vijay, R. (2019). A synchronous intertwining logistic map-DNA approach for color image encryption. *Journal of Ambient Intelligence and Humanized Computing*, *10*(6), 2277-2290.
[48]. Suri, S., & Vijay, R. (2019). A bi-objective genetic algorithm optimization of chaos-DNA based hybrid approach. *Journal of Intelligent Systems*, *28*(2), 333-346.
[49]. Zhu, H., Dai, L., Liu, Y., & Wu, L. (2021). A three-dimensional bit-level image encryption algorithm with Rubik's cube method. *Mathematics and Computers in Simulation*, *185*, 754-770.
[50]. Zeng, J., & Wang, C. (2021). A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata. Security and Communication Networks, 2021.

Mohit Dua* (Corresponding Author) received Ph.D in the area of Automatic Speech Recognition from National Institute of Technology, Kurukshetra, India in 2018. He is presently working as Assistant Professor in Department of Computer Engineering at NIT Kurukshetra, India. He has more than 17 years of Teaching and Research experience. He is a member of Institute of Electrical and Electronics Engineers (IEEE), and life member of Computer Society of India (CSI) and Indian Society for Technical Education (ISTE). His research interests include Speech processing, Chaos based Cryptography, Information Security, Theory of Formal languages, Statistical modelling and Natural Language Processing. He has published approximately 60 research papers including abroad paper presentations including USA, Canada, Australia, Singapore, Mauritius and Dubai.

Shelza Dua received her Ph.D in the area of Image Encryption from Banasthali Vidyapith, Rajasthan, India in 2019. She is presently working as Assistant Professor in Department of Electronics and Communication Engineering at NIT Kurukshetra, India. She has more than 15 years of Teaching and Research experience. She is a life member of Institution of Engineers (India) [IEI]. Her research interests include Speech processing, Chaos based Cryptography, and Information Security. She has published approximately 20 research papers in various reputed international conferences and journals.

Priyanka Jaroli completed her M.Tech Computer Science and Engineering from Banasthali Vidyapith, Rajasthan, India in 2018. She is pursing PhD in the area of Machine Learning from Banasthali Vidyapith, Rajasthan, India. She is presently working as an Assistant Professor in the Department of Computer science & Engineering at JECRC University, India. Her research interests include Image processing, Image encryption, Machine learning and Deep learning.