Volume 65, Issue 5, 2021

Journal of Scientific Research

of

The Banaras Hindu University

Secure Colour Image Encryption Based on Dynamic DNA Coding and Different Chaotic Maps

Subhajit Das*[1], Manas Kumar Sanyal[2], and Joyjit Mandal[3]

*[1]University of Kalyani, Department of Business Administration, Kalyani, India, subhajit.batom@gmail.com
[2]University of Kalyani, Department of Business Administration, Kalyani, India, manas_sanyal@rediffmail.com
[3]Central University of Rajasthan, Department of Computer Science, Ajmer, India, joyjitmandal1@gmail.com

Abstract: **In recent years several chaos-based encryptions have been developed due to its extraordinary property, but its debris is an inexorable discrepancy for developing efficiency and security. In this paper, a new colour image encryption and decryption scheme with different dimensional chaos functions has been used. One-dimensional logistic map, two-dimensional Sine-Henon alteration map, and three-dimensional Lorenz chaotic systems have been applied in different stages of the encryption model. Moreover, to protect from different types of attacks, dynamic DNA sequences with its reversible operations have been applied. Different experimental outcomes exhibit the effectiveness and efficiency of the proposed method. It is also proved that the proposed method can combat statistical attack, differential attack and exhaustive attack.**

Index Terms: **DNA operation, dynamic DNA sequence, image encryption, Lorenz chaotic system, SHA 256, Sine-Henon alteration**

I. Introduction

This In the age of globalization, fast and secure communication brings a revolutionary change in human society. There are so many free applications in the market through which people can easily communicate with each other. Nowadays people are very much interested in multimedia communication services i.e. picture, voice, video rather than text message communication. As a result, confidentiality and security are a great issue for this type of communication. The digital image is an extensive information repository of communication. So preserving this information from unauthorized access during transmission is very much necessary. Traditional block ciphers such as Triple –DES, AES, and IDEA are not convenient for image cryptology. This is because the security of these algorithms is mainly concentrated on high computational cost whereas images are characterized by huge data capacity and high correlation between their neighbour pixels. Finding an efficient, effective, and secure image encryption algorithm has become a universal concern for researchers. Researchers applied different types of mathematical and statistical tools like the elliptic curve [Laiphrakpam Dolendro Singh (2015) et al.], fractional wavelet transform [Linfei Chen (2005) et al.], reversible cellular automata [Jun Jin (2012) et al.], image filtering [Xinsheng Li (2019) et al.], and pixel adaptive diffusion to overcome the challenge. Among them, a chaos-based image cryptosystem contributes an optimal establishment between security and efficiency. The quality of the image encryption algorithm is very enriched by dynamic properties of a chaotic system. Chaos-based image encryption algorithm performed in two stages: one is pixel position changing and the other is pixel value changing. In pixel position changing, the arrangement of pixels is changed and a new scrambled image is created. But the pixel position changing stage leads to the histogram of the image is the same as the original image. As a result, evolution of security is not accurately managed. On the other hand, in the pixel value changing method values are changed by using chaotic sequence and provide higher security but in terms of encryption effect this method is not good enough [Qiang Zhang (2012) et al.]. Most of the low dimensional chaos-based encryption model is confined by the computer word length which causes deterioration in the chaotic dynamics [Y. H. Zhang (2015) et al.]. There is no apprehension about that single chaotic map-based image encryption technique cannot support the surveillance of the encrypted image [Ying Niu (2017) et al.].

To overcome the drawback of single dimensional chaotic map

* Subhajit Das

in encryption Hua et al [Zhongyun Hua (2015) et al.] introduced a new two-dimensional sine logistic modulation map (2D-SLMM). They proved this map has larger chaotic range, many parameters, and good enough chaotic property. Authors [Hayder Natiq (2018) et al.] applied another two-dimensional chaotic map that is Sine-Henon alteration map in image encryption. Sine-Henon 2D alteration map is developed from Henon and Sine maps. Using dynamical analysis and simple entropy algorithm authors proved that 2D SHAM is overall hyperchaotic with high complexity. Moreover, Niu et al proposed a new three-dimensional Lornez chaotic system [Ying Niu (2017) et al.] with the DNA sequence. They described that Lorenz's chaotic system generates a more complex system structure that can develop a combination of univariate or multivariate chaotic sequences. Besides the hyperchaotic system, DNA coding system materialize an insurgent change in image cryptology. DNA coding system import some exceptional features such as huge storage, massive parallelism and ultra-power consumption. Moreover, DNA coding based logical operation is truly reversible in nature that is very crucial for image cryptology [QiangZhang (2010) et al.][R. Guesmi (2016) et al.][Changjiang Zhu (2020) et al.][Xiuli Chai (2019) et al.]. But our main focus is on the colour image encryption technique. The structure of colour image is different from the greyscale image because the colour image consists of three different channels namely Red, Green, and Blue. Two logistic maps and DNA sequence operation-based image encryption was proposed by Zhang et al but their proposed method has failed to get the desired encryption quality due to the low randomness of the applied logistic maps. In ref [L. Li (2011) et al.] authors applied Arnold map before DNA coding but their applied key value was independent of the plain image. So, this method cannot resist against different text attacks. Wang et al [Wang (2018) et al.] proposed a Lorenz system based colour image encryption where DNA permutation and logical operations can break the bit planes of the input image completely.

Analysing these characteristics, we propose an exclusive colour image encryption based on different chaotic maps and dynamic DNA sequences. The specialty of our proposed system is that it uses an extremely high order key value using SHA 256 that depends on the plain image. Moreover, three different channels of the colour image are related thoroughly throughout the encryption process. The proposed method is a combination of bit-level shuffling and pixel shuffling and the encryption process is based on dynamic DNA coding and reversible DNA sequence operations. The paper demonstrates as section 2 describes basic tools applied in our method, sec 3 demonstrate the encryption process including key generation, bit shuffling and pixel shuffling. In section 4 decryption processed is discussed. The experimental outcomes are reported in section 5 and lastly paper is closed with a conclusion.

II. Basic Theory

A. One Dimensional Logistic Map

In our proposed method one dimensional logistic map has been used to generate two random sequence numbers. These two random sequences are used to select a particular DNA coding rule and a particular DNA operation type. Both operations are used for encryption stage. The one-dimensional logistic map has been defined by

$$x_{n+1} = \alpha x_n(1 - x_n) \qquad (1)$$

Where $x_n \in (0,1), \alpha \in (0,4)$. In this equation value of α and value of x will be the input. It already proved that the system is in chaotic state when $3.99 \le \mu \le 4$.

B. Two Dimensional Logistic Map (2D Sine-Henon alteration map)

In our proposed algorithm 2D Sine Henon alteration map has been used to generate two extremely different random alterations. This type of 2D map is derived from Henon and Sine map. First Henon map is modulated and result is used to enhance the non-linearity and randomness of sine map. The new 2D SHAM is defined by

$$x_1(n+1) = \left(\frac{1}{nb}\right) sin(1 + a x_1(n)^2 - \pi^2 x_2(n)) \qquad (2)$$

$$x_2(n+1) = \left(\frac{2}{nb}\right) sin(\pi b x_1(n)) \qquad (3)$$

Here the value of a and b are known as controlled parameters. Where $0 \le a \le 5$ and $0.45 \le b \le 2$.Natiq et al(2018)showed the basic dynamic properties, Jacobian eigenvalues, trajectory, Bifurcation diagram, LE and sensitivity dependence test. Authors proved that 2D-SHAM is overall hyper chaotic and high sensitive to its beginning value and control parameter.

C. Lornez Chaotic Systems

In 1963, Edward Lorenz, with the help of Ellen Fetter, invented a very easy simplified mathematical l model for atmospheric convection. It is a system that consists of three ordinary differential equations. These equations are known as Lorenz equations [Xinsheng et al(2019)]. From a technical standpoint, the Lorenz system is nonlinear, non-periodic, three-dimensional and deterministic. These three dimensions are used to generate three different matrices. These three matrices are used as a different keyword for three different channels of original image. It is very much essential to disperse the system by the fourth order Runge-Kutta method for very sensible random number generation. 3D chaotic system is defined by

$$x' = a(y - x) \qquad (4)$$

$$y' = cx - y - xz \qquad (5)$$

$$z' = xy - bz \qquad (6)$$

Here a, b, c are system parameters. Initial values of x, y, z will be computed or taken as a key word. The Lorenz Chaotic system in chaotic state when a=10, b=8/3 and c=28.

D. DNA Sequence Rule

A DNA sequence has four different types of nucleotides they are Adenine(A), Thymine(T), Guanine(G) and Cytosine(C). Here ‘A’ can pair with ‘T’ and ‘G’ can pair with ‘C’. In other words, it can be said A, T and G, C are in complementary relation. Four DNA nucleotides are represented by two bits binary sequences. They are 00,01,10,11. As per the binary complementary rule, complement of 0 is 1 and vice versa. So, following this rule, 00 and 11 are a complement to each other. Similarly, 01 and 10 are also complementary to each other. Out of four sequences i.e. 00,01,10,11 anyone can choose any sequence to serve a nucleotide keeping DNA complementary rule in mind. Following this way there possibly 4! i.e. 24 types of combination for DNA coding. Scrutinizing the complementary concern [Chai XL et al(2019)] there are eight kind of valid rules that are given in table 1. In our proposed method pixel values are changed to a DNA sequence using a specified rule no. For example, if the value is 225, its equivalent binary sequence is ‘11100001’, which can be coded as ‘TGAC’ according to rule no 1 and coded as ‘GTCA’ according to rule no 3.

Table I. DNA coding rules

1	2	3	4	5	6	7	8
00-A	00-A	00-C	00-C	00-G	00-G	00-T	00-T
01-C	01-G	01-A	01-T	01-A	01-T	01-C	01-G
10-G	10-C	10-T	10-A	10-T	10-A	10-G	10-C
11-T	11-T	11-G	11-G	11-C	11-C	11-A	11-A

E. DNA Operations

By using DNA sequence, it is possible to perform some algebraic operations [101,102,103,104]. They are most common logical operation-addition, subtraction, XOR and XNOR. The influences of these DNA operations are that they are truly reversible in nature. Addition and subtraction are reversable each other, XOR and XNOR are themselves reversable in nature. This is the most important useful property in image encryption. Table [2-4] serve the result of each DNA operations considering that nucleotides are coded according to rule no 7 in Table I.

Table II. XOR operation

XOR	A	C	T	G
A	A	C	T	G
T	T	G	A	C
C	C	A	G	T
G	G	T	C	A

Table III. XNOR operation

XNOR	A	C	T	G
A	C	A	G	T
T	T	G	C	A
C	A	C	T	G
G	T	G	A	C

Table IV. ADDITION operation

+		C	T	G
A	C	A	G	T
T	G	T	C	A
C	A	C	T	G
G	T	G	A	C

Table V. SUBSTRACTION operation

+		C	T	G
A	C	A	G	T
T	G	T	C	A
C	A	C	T	G
G	T	G	A	C

III. PROPOSED ALGORITHM

Fig 1 represents the total encryption process of our proposed algorithm. Our encryption process made up with four sub steps - key generation, Partition of image, bit shifting, pixel shuffling, construction of corelating matrix, encryption and decryption.

A. Key Generation Algorithm

To produce a unique secret key SHA-256 has been used in our proposed algorithm. SHA -256 is used by many cryptographic algorithms because slight change in input value produces completely different output value. First of all we have produced a hex value using **KeyGen()** function. In this function a simple calculation has been performed using the values of Red, Green, Blue channel of colour image and an arbitrary number. The outcome of KeyGen() has been applied to SHA-256 to produce unique 256 bit hash value. This hash value has been used to initialize different input parameters for encrypting the colour image. As the key value totally depends on input image, so our algorithm can resist against known plain text, chosen cipher text and chosen plain text attacks.

KeyGen()

Input: Input Image and four-bit decimal random number.
Output: a 256-bit long key value

1. Devide the colour image consists of m rows and n columns into Red Channel(R), Green Channel(G) and Blue channel(B). Now we have three different matrices (R, G, B) of size m by n.
2. $R_{1=}\ celing\left(\frac{\sum_{i=1}^{m}\sum_{j=1}^{n} R_{i,j}}{m\times n}\right)$, $G_{1=}\ celing\left(\frac{\sum_{i=1}^{m}\sum_{j=1}^{n} G_{i,j}}{m\times n}\right)$, $B_1 = celing\left(\frac{\sum_{i=1}^{m}\sum_{j=1}^{n} B_{i,j}}{m\times n}\right)$
3. $key_{val} = ((((\left((R_1 \times 10^3) + G_1\right) \times 10^3) + B_1) \times 10^3) + randbetween(1 - 1000)$
4. $key = SHA256(key_{val}) = \{k_1, k_2, k_3, \dots \dots . k_{64}\}$ Each K contain 4 hexadecimal bit.
5. $M = rem(hex\_decimal(k_1),8)$.
6. $N = rem(hex\_decimal(k_2 k_3), 99) + 1$
7. $X_0 = (hex\_decimal(k_4 k_5 k_6 k_7 k_8 k_9 k_{10} k_{11}) \times 10^{-9})$
8. $Y_0 = (hex\_decimal(k_{12} k_{13} k_{14} k_{15} k_{16} k_{17} k_{18} k_{19}) \times 10^{-9})$
9. $a = rem(hex\_decimal(k_{20} k_{21} k_{22} k_{23}), 5)$
10. $b = 0.45 + rem(hex\_decimal(k_{24} k_{25} k_{26} k_{27}), 2$
11. $X_1 = (hex_{decimal}(k_{28} k_{29} k_{30} k_{31} k_{32} k_{33} k_{34} k_{35}) \times 10^{-9})$
12. $Y_1 = (\ hex_{decimal}(k_{36} k_{37} k_{38} k_{39} k_{40} k_{41} k_{42} k_{43}) \times 10^{-9})$
13. $Z_1 = (hex\_decimal(k_{44} k_{45} k_{46} k_{47} k_{48} k_{49} k_{51}) \times 10^{-9})$
14. $X_2 = (hex_{decimal}(k_{52} k_{53} k_{54} k_{55} k_{56} k_{57} k_{58} k_{59}) \times 10^{-9})$
15. $\propto = 3.99 + (hex\_decimal(k_{60} k_{61} k_{62} k_{63} k_{64}) \times 10^{-5})$

Here $celing(n)$ function gives the nearest highest integer value of n . $randbetween(range)$ function generates a random number within the specified range . $rem(a, n)$ generates remainder part by dividing a by n. $hex\_decimal(n)$ converts hexadecimal number n to its equivalent decimal number. $SHA256(a)$ produces 256 bit long hash value on input value a.

B. Partition of Image

we describe two functions add() and division() that are most useful for our encryption.

i) ***add*** () that performs concatenation of matrices of same order side by side in column direction. It converts m×n×3 matrix into m×3n

ii)***division*** () that breaks a matrix into three equal matrices in column direction i.e it converts m×3n matrix into three matrix of m×n.

Let the original colour image IM of size m rows and n columns.

$$IM = |IM|_{m\times n\times 3}$$

Three different channels of input colour image (red channel, green channel and blue channel) are separated and stored one by one in column direction.

$$IM_{m\times n\times 3} = (IM^R_{m\times n}, IM^G_{m\times n}, IM^B_{m\times n})$$

$$IM1_{m\times 3n} = add(IM^R_{m\times n}, IM^G_{m\times n}, IM^B_{m\times n}) \quad (10)$$

C. Bit Shifting

To make our proposed algorithm dependent upon plain image a circular shift operation ShiftCircu() is introduced. This function first circularly shift M number of bits of pixel resides in the upper left corner of the plain image. Then depending upon its new value, the other neighbour pixel values are updated. The value of M is constant provided by key value. ReShiftCircu() function is reverse of ShiftCircu() function.

Input: - IM1 and M

Output- A m×3n matrix IM2.

ShiftCircu()

1. *value=M;*
2. *for i=1 to m*
3. *for j=1 to n*
4. *new_image(i,j)=circularshift(image(i,j),value)*
5. *value=rem(new_image(i,j),7) +1*
6. *end of inner for in step 2*
7. *end of outter for in step 1*
8. *end*

Here circularshift (a,n) shifted n number of bits circularly on a and rem(a,n) operation generates the remainder part if a is divided by n.

$$IM2 = ShiftCircu(IM1, M)$$

ReShiftCircu()

1. *val=0;*
2. *for i=1 to m*
3. *for j=1 to n*
4. *new_image(i,j)=circularshift(image(i,j),value)*
5. *value=8-(mod(new_image(i,j),7) +1)*
6. *end of inner for in step 2*
7. *end of outter for in step 1*
8. *new_image(1,1)=circularshift(image(i,j),(8-M))*
9. *end*

D. Pixel Shuffling

In our proposed algorithm 2D Sine Henon Alteration Map is used to generate two extremely random numbers that used for pixel shuffling. Using equation 1 and 2 random sequences are generated. These sequences are used to change the locations of each pixel's row wise and column wise. Pixel shuffling using two random sequences (***Shuff***()) is described below. We introduce another function ***Re_Shuff()*** that arranges the pixels into its original position .This function is used during decryption process**.**

Shuff()

1. To avoid harmful effect of transactional procedure we iterate 2D SHAM equations N0 times. Here N0 is a fixed number.
2. Generate two sequences (*Ic* and *Ir*) each consist of 3m*n numbers with initial conditions (x_0, y_0, a, b)
3. I_c divided into $3n$ equal parts where each part contains m elements and Ir devided into m equal parts where each part contains $3n$ elements.
4. Every part from Ic are shorted into ascending order and every parts of Ir are sorted into descending order.

$$I_c = \{C_i\}: \ 1 \le i \le 3n;\ C_i = aesc(x_1, x_2 \ldots . x_m) \quad (11)$$

$$I_r = \{R_j\}: 1 \le j \le m; \quad R_j = desc(x_1, x_2, \ldots \ldots ., x_{3m})\}: \quad (12)$$

5. After sorting we keep locations of replacement of each element and change the pixel position accordingly. For shuffling each column location change of each C_i and shuffling each row location change of each R_j is considered. Process of location changing of pixels is described below with an example.

Example:

let consider a vector of (v) of eight elements $v = \{102,202,56,78,87,97,100,187\}$ a random sequence be $r = \{58.2,100.5,23.4,4.3,89.6,35.4,23.6,17.2\}$.

$r1 = aesc(r) = \{4.3,17.2,23.4,23.6,35.4,58.2,89.6,100.5\}$

Hence the location tracker defined as $LC = \{4,8,3,7,6,1,5,2\}$

According to LC, vector V is assembled as $v' = \{97,187,56,102,100,87,78,202\}$

After sorting r it is observed that 4th element moves in first position, 8th element moves into 2nd position and so on. To assemble any vector using this location tracker we moves first element to forth location. Second element to 8th location,3rd element to 3rd location,4th element 7th location and so.

Re_shuff()

To get back original v to perform Re_Shuff() where v' and LC taken as input. In this method forth element of V' moves in first position,8th element moves onto second position ,3rd element moves in 3rd position and so on.

Shuff() method is used during encryption process and Re_shuff() method is used in decryption process.

after sorting it is observed that in vector 'r' element 58.2 of fist position is shifted into 6th position and element in 2nd position (100.5) shifted into 8th position. Considering this way the location tracker(LC) defined as $LC = \{4,8,3,7,6,1,5,2\}$. Following the location tracker the final output of shuff() on vector v is

$v = \{78,187,56,100,97,102,87,202\}$

After shuffling matrix IM3 is obtained

$$IM3 = shuff(IM2, I_c, I_r)$$

E. Construction of Correlating Matrix

Lorenz chaotic system is applied here for generating three different correlating matrices. These correlating matrices are generated by solving equations by RK method (order 4). Like other chaotic equations these equations are also preliterate system N_0 times for avoiding the harmful effects. Forth order RK method solution is given by

$$x_{n+1} = x_n + \frac{h}{6}(K_1 + 2K_2 + 2K_3 + K_4) \quad (13)$$

$$y_{n+1} = y_n + \frac{h}{6}(L_1 + 2L_2 + 2L_3 + L_4) \quad (14)$$

$$Z_{n+1} = Z_n + \frac{h}{6}(M_1 + 2M_2 + 2M_3 + M_4) \quad (15)$$

Where

$K_j = a(y_n - x_n)$

$L_j = cx_n - y_n - x_n z_n$

$M_j = x_n z_n - bz_n$

From equation (13), (14) and (15) we generate m*n numbers from each equation. With initial values (x_1, y_1, z_1) From these sequences three m by n matrix is constructed $(cor^x), (cor^y), (cor^z)$

$$Co\_mat = add(cor^x_{m\times n}, cor^y_{m\times n}, cor^z_{m\times n}) \quad (16)$$

F. Encryption

Input: IM3, Co_mat, x_2, α

Output: Encrypted image (EI)

At this point we apply divide division function on IM3 that breaks the matrix into three equal parts. From one-dimension logistic map described in equation (1) with initial value (x_2, α),two sequences $P\ and\ Q$ are computed.

$$P = \{p_1, p_2, p_3, \dots\dots\dots.., p_{m\times n\times 3}\} \quad (17)$$

$$Q = \{q_1, q_2, q_3, \dots\dots\dots.., q_{m\times n\times 3}\} \quad (18)$$

$P' = \{mod((p_i \times 10^4), 7) + 1\}$:i=1,2,... $m \times n \times 3$ (19)

$Q' = \{mod((q_i \times 10^4), 3) + 1\}$: i= 1,2,… $m \times n \times 3$ (20)

Each number taken from P' represents the rule no of DNA encoding operation which are present in Table no 1. Numbers from Q' represents DNA operational code. In our method code 1 indicates for addition, code 2 indicates for subtraction, code 3 indicates XOR and code 4 indicates XNOR. Encryption method is described below.

Encry()

Input: p', q', Co_mat,*IM3*

Output: $Encrypted_{imge}$

1.*set count=0;*

2.for i=1 to m

2.for j=1 to 3n

3.c=to_DNA(Co_mat(i,j),p'(count));

4.d=to_DNA(IM3(i,j),p'(count));

5.EI(i,j)=from_DNA(DNA_op(c,d,q'(count)),p'(count));

6.End if j

7.End of i

8.count=count+1;

9.end

Here to_DNA(a,n) converts the decimal value into DNA sequence according to rule no n. from_DNA(a,n) converts DNA sequence a into ints equvalent decimal number following rule no n.DNA_op(c,d,n) performs one of DNA algebraic operation specified by n between c and d. At this point EI is encrypted image. Apply division to EI to get three equivalent matrix and using this matrix a three-dimensional image is constructed.

$$EI^1, EI^2, EI^3 = division(EI)$$

$$Encrypted_{image} = m \times n \times 3$$

where m and n are horizontal and vertical magnitude of image.

G. Decryption

Our proposed method is symmetric key encryption means same key is used for encryption as well as decryption. At the receiver end from the key value P', Q' is generated from one dimension logistic map, $(cor^x), (cor^y), (cor^z)$ is generated from three dimension Lorenz chaotic sequence and I_c,I_r generated from 2D SHAM chaotic map.

Step 1: apply ***division*** to encrypted image for getting three different two dimensional matrix.

$$\{DI^1, DI^2, DI^3\} = division(EI)$$

Step 2: apply ***add()*** to EI .

$$DI1 = add(DI^1, DI^2, DI^3)$$

Step 3: Before apply ***Encry()*** a little change have been made in sequence Q' .As addition and subtraction operation of DNA coding are reversable each other so in sequence Q' value 1 is converted to 2 , 2 is converted to1 and value 3 and 4 are remain unchanged. At this point a new sequence Q'' is obtained.

$$DI2 = Encry(DI1, Co_{mat}, p', Q'')$$

Step 4: apply ***Re_shuff()***

$$DI3 = Re\_shuff(DI2, I_c, I_r)$$

Step 5. Apply ***ReShiftCircu() .***

input -DI3 and M

output- Decrypted Image(DI)

1. *val=0;*
2. *for i=1 to m*
3. *for j=1 to n*
4. *new_image(i,j)=circularshift(image(i,j),value)*
5. *value=8-(mod(new_image(i,j),7) +1)*
6. *end of inner for in step 2*
7. *end of outter for in step 1*
8. *new_image(1,1)=circularshift(image(i,j),(8-M))*
9. *end*

$$DI = ReShiftCircu(DI3, M)$$

step 6. apply ***division ()*** to *DI*

$$\{DI_1, DI_2, DI_3\} = division(DI)$$

Constructing these three matrix final Decrypted image is obtained.

$$Decrypted_{image} = m \times n \times 3$$

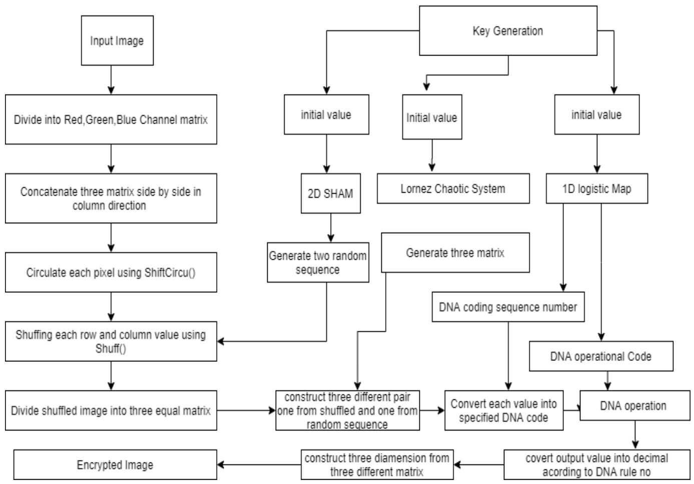


Fig. 1. Block diagram of proposed image encryption approach

IV. Performance Analysis

Efficiency of our proposed algorithm is tested by using colour benchmark images Babun, Lena, Papers, Flower of size 256×256. As the keyword of our method depends upon input image so to encrypt these images, we applied appropriate keyword for each image. Visual Analysis of described method demonstrate in Fig 2. Test case images are shown in Fig 2(a), their corresponding encrypted image are shown in 2(b) and in Fig 2(c) images after decryption are shown. It has been shown that images of 2(a) and 2(c) similar.

Fig. 2. a) input image, b)encrypted image, c)decrypted image

A. Key Sensitivity

To analyse the key sensitivity of our proposed algorithm we change a single bit of the key value and applied in Lena imge. Fig 3a and Fig 3b show two encrypted images with a single bit change in their key value. The differences between the two encrypted images are shown in Fig 3c. It has been observed that we have obtained a completely different cipher image. Both analyses and simulations demonstrate that the proposed algorithm is key sensitive and a slight change in the key value will cause a momentous variation on the output.

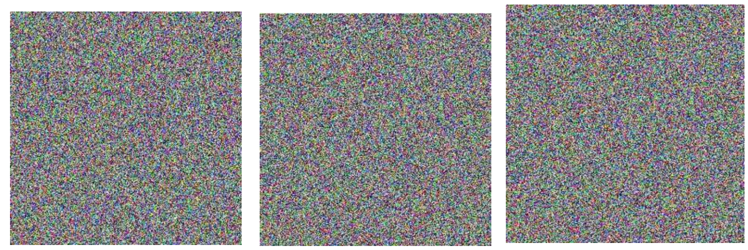
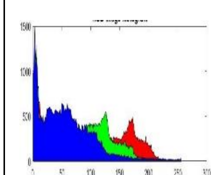
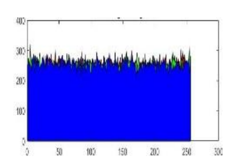
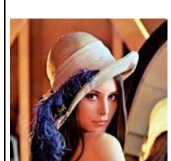
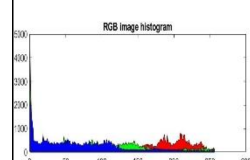
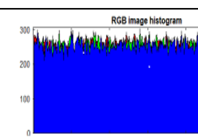
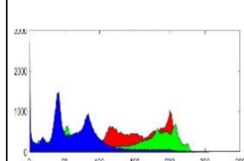
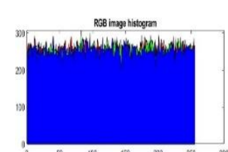


Fig. 3.a) Encrypted Lena, b) Encrypted Lena with single bit change, c) Difference a and c

B. Histogram Analysis

An image encryption algorithm is said to be perfect if it produces a constant distribution of pixels for encrypted images. Fig 4a, 4b,4c,4d show the histograms of four different cipher images. From these figures, we conclude that our model produces constant distributed histograms for different encrypted images and it is almost impractical for an adversary to extract any kind of important information from the histogram of cipher image.

Image	**Histogram of Original Image**	**Histogram of encrypted Image**
Babun 		
Lena 		
Pappers 		

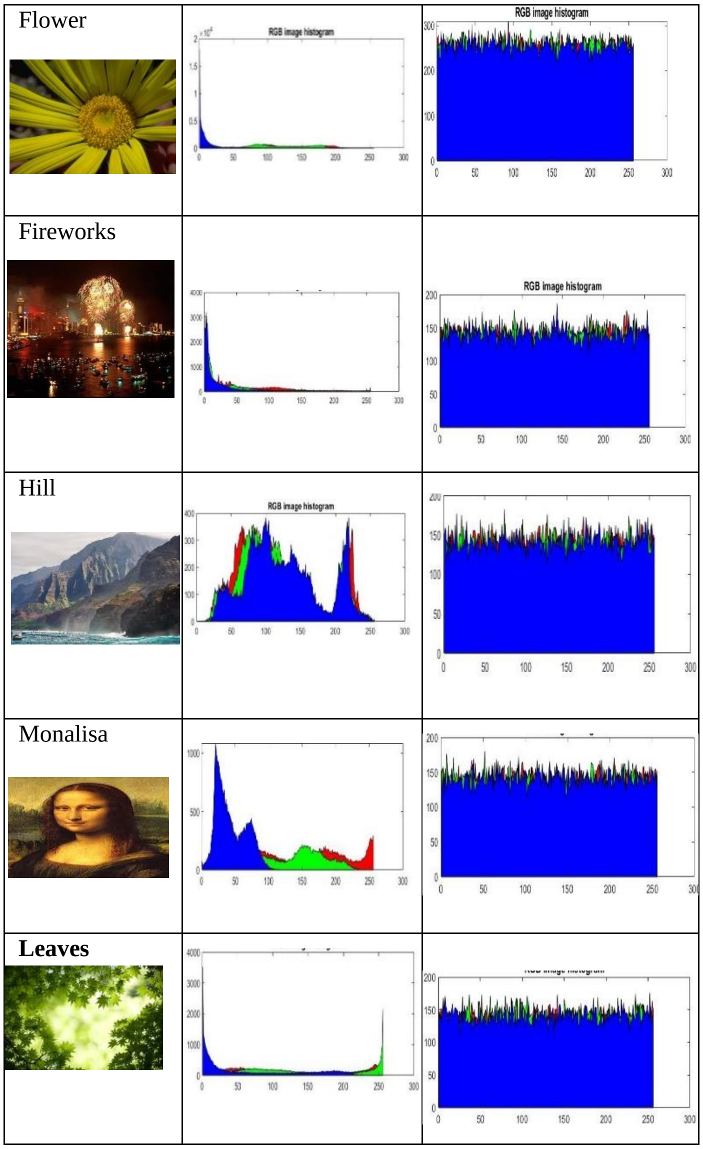


Fig. 4. Different histogram of original and encrypted image

C. Different Attack

UACI (Unified Average Changing Intensity) and NPCR (Number of Pixel Change Rate) are widely used to check the resistance against different attack of proposed encryption algorithm. UACI and NPCR can be defined as

$$UACI = \frac{1}{X \times Y}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right] \times 100\% \qquad (21)$$

$$D_{(i,j)} = \begin{cases} 1, & C_p(i,j) \neq C_e(i,j) \\ 0 & otherwise \end{cases}$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{X \times Y} \times 100\% \qquad (22)$$

Where C1 and C2 are two different encrypted images in which their input images have randomly selected only one pixel difference from each other. X and *Y* are the height and width of input image. Table VI demonstrate the computed UACI and NPCR values of our proposed algorithm. Considering two random images, the maximum expected value of UACI is 33.5% and maximum expected value of NPCR is 99.63% [Kwok et al(2017)]. Analysing the values of table 1 it concluded that values are close to the ideal one.

Table VI. NPCR and UACI values of different color image

images	UACI	NPCR
Babun	33.4878	99.6345
Lena	33.4716	99.6132
Pappers	33.4538	99.5906
Flower	33.5019	99.5816
Fireworks	33.5871	99.5785
Hill	33.4787	99.5547
Monalisa	33.5146	99.6015
leaves	33.5648	99.5974

D. Correlation Analysis

An encryption algorithm is said to be good if it significantly reduces the correlation between adjacent pixels of the ciphered images. To calculate the correlation of plain text image and cipher text image we first select randomly 2500 pairs of two adjacent pixels from an image. Then the correlation coefficients of adjacent pixels in horizontal, vertical and diagonal directions are computed using equation 23,24,25,26.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\,\sqrt{D(y)}} \qquad (23)$$

$$E(x) = \frac{1}{S}\sum_{i=1}^{S} x_i \qquad (24)$$

$$D(x) = \frac{1}{S-1}\sum_{i=1}^{S}(x_i - E(x))^2 \qquad (25)$$

$$cov(x,y) = \frac{1}{S}\sum_{i=1}^{S}(x_i - E(x))\,(y_i - E(y)) \qquad (26)$$

x and y are two adjacent pixels in the image. S represents total number of duplets(x,y) obtained from the image. Table VII demonstrate the correlation coefficient of test images.

Table VII. Correlation coefficient of different colour image

images	Component	Original Image			Encrypted Image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	Channel1	0.98174	0.96246	0.94170	0.00184	0.0055	0.0036
	Channel2	0.97474	0.9500	0.92841	0.00343	0.00568	0.00596
	Channel3	0.95989	0.93338	0.90722	0.00280	0.00113	0.00010
Bab	Channel1	0.98840	0.98914	0.98288	0.003468	0.00419	0.00168

	Channel2	0.98304	0.98400	0.97472	0.001865	-0.00787	0.00324
	Channel3	0.97787	0.97927	0.96712	0.00637	0.01361	0.00401
Pappers	Channel1	0.96796	0.96457	0.93694	0.00588	0.00429	0.00007
	Channel2	0.975	0.96983	0.94657	-0.00134	0.00153	0.00122
	Channel3	0.96361	0.95700	0.92629	0.00189	0.00351	0.00203
Flower	Channel1	0.97446	0.97013	0.95323	0.00848	0.00153	0.00290
	Channel2	0.97306	0.96857	0.95049	0.00021	0.00076	0.00428
	Channel3	0.88255	0.87617	0.81305	0.00132	0.00203	0.00286
Fire works	Channel1	0.95043	0.92132	0.86447	0.00213	0.00422	0.00385
	Channel2	0.94263	0.91000	0.84588	0.00228	0.00517	0.00185
	Channel3	0.91478	0.86569	0.77281	0.00051	0.00214	0.00179
Hill	Channel1	0.95356	0.96604	0.92926	0.00655	0.00014	0.00225
	Channel2	0.95461	0.96721	0.93216	0.00248	0.00143	0.00309
	Channel3	0.95249	0.96787	0.93166	0.00237	0.00149	0.00565
Monalisa	Channel1	0.98470	0.98825	0.97576	0.00341	0.00258	0.00518
	Channel2	0.97971	0.98466	0.96868	0.00470	0.00057	0.00498
	Channel3	0.89758	0.91406	0.84290	0.00310	0.00869	0.00379
Leaves	Channel1	0.96154	0.944137	0.92164	0.00123	0.00249	-0.00220
	Channel2	0.95856	0.93998	0.91600	0.00781	0.01082	0.00189
	Channel3	0.95902	0.93845	0.91412	0.00488	0.00197	0.00122

E. Information Entropy Analysis

An arbitrary distribution of media file is measured using information entropy. Information entropy is calculated using the formula described below[12].

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) log_2 \frac{1}{p(m_i)} \qquad (27)$$

The entropy value for an encrypted image should be as high as possible, and for ideal situation it is very closer to 8[Ying et al (2017)]. The result of computed entropy value of our proposed algorithm have been furnished in table 8. Entropy values of encrypted image demonstrate that our proposed techniques are quite secure in the face of entropy attacks. Presented in Table VIII

Table VIII. Information Entropy of different images

Image	Channel 1	Channel 2	Channel3
Lena	7.99789	7.99827	7.99880
Babun	7.99726	7.99667	7.99720
Pappers	7.99749	7.99734	7.99745
Flower	7.99762	7.99703	7.99757
Fireworks	7.99798	7.99819	7.99787
Hill	7.99816	7.99750	7.99788
Monalisa	7.99716	7.99756	7.99790
Leaves	7.99761	7.99751	7.99814

F. Resistance To Known And Chosen Plaintext attacks

In proposed method key robustly relies on input image and hash value. Different key values would be created for encrypting different images. It is not possible for an attacker to leak any type of information with a key that was used for other image. So, our method can resist both known plain text and chosen plain text attacks.

G. Comparisons

A comparison has been made of our proposed method to other algorithms. In terms of some important parameters in table IX. All the comparison has been made by taking Lena image as input. By observing these values, it is said that our proposed method is effective and efficient in many respects.

Table IX. Comparison of result

Encryption method	UACI	NPCR	Entropy		
			Channel 1	Channel 2	Channel 3
Proposed method	33.47	99.61	7.9978	7.9986	7.9988
Ref [25]	33.47	99.57	7.9927	7.9924	7.9936
Ref [26]	33.46	99.6	7.9975	7.9980	7.9975
Ref [27]	33.43	99.54	7.9982	7.9897	7.9885
Ref [28]	33.46	99.58	7.9967	7.981	7.9971

CONCLUSION

We describe an exclusive colour image encryption with different chaotic functions and dynamic DNA sequences. Different chaotic functions in different stages of our proposed algorithm are applied because chaotic function can generate sensible random sequences which are very effective for image encryption. Traditional cryptographic hash function SHA 256 is used for unique key word generation that make our algorithm resist against different plain text and cipher text attacks. Different important tests have been performed to prove the efficiency of our algorithm. Outcome of these tests proves that the proposed scheme has superior security and high efficacy in image encryption algorithm.

References

Z.Hua ,Y,Zhou,C.-M Pun,and C.L.P. Chen(2015), 2D Sine Logistic modulation map for image encryption, *Information Sciences*, Vol 297,pp 80-94,2015

Hayder Natiq,N.M.G. Al-Saidi,M.R.M Said and Adem Kilicman, (2018),A new hyperchaotic map and its application for image encryption", *The European Physical Journal Plus* pp-1-14

Ying Niu, Xuncai Zhang, and Feng Han (2017), Image Encryption Algorithm Based on Hyperchaotic Maps and Nucleotide Sequences Database,*Computational Intelligence and Neuroscience* Volume 2017, Article ID 4079793, 9 pages

Laiphrakpam, Dolendro Singh ,Khumanthem ,Manglem Singh (2015),Image Encryption using Elliptic Curve Cryptography", *Procedia Computer Science*, Volume 54,Pages 472-481

LinfeiChen,DaomuZhao,(2005)"Optical image encryption based on fractional wavelet transform",*Optics Communications* Volume 254, Issues 4–6, Pages 361-367

JunJin(2012), An image encryption based on elementary cellular automata, Optics and Lasers in Engineering Volume 50, Issue 12, Pages 1836-1843

Xinsheng Li, Zhilong Xie, Jiang Wu, Taiyong Li(2019), Image Encryption Based on Dynamic Filtering and Bit Cuboid Operations, *Hindawi Complexity Volume 2019*, Article ID 7485621, 16 pages

Qiang Zhang, Xianglian Xue, Xiaopeng Wei (2012), "A Novel Image Encryption Algorithm Based on DNA Subsequence Operation", *The Scientific World Journal / 2012* , Article ID 286741

Y. H. Zhang and B. Zhang (2015), Algorithm of image encrypting based on Logistic chaotic system, *Application Research of Computers*, vol. 32, no. 6, pp. 1770–1773.

Mohamed MA, Samarah AS, Fath Allah MI. Optical Encryption Techniques: AnOverview. Int J Comput Sci Issues (IJCSI) 2014;11(2):125–9

Akhavan A, Samsudin A, Akhshani A (2017) Cryptanalysis of an image encryption algorithm based on DNA encoding. *Opt Laser Technol* 95:94–99

Amani H, Yaghoobi M (2019) A new approach in adaptive encryption algorithm for color images based on DNA sequence operation and hyper-chaotic system. *Multimed Tools Appl* 78:21537–21556

Belazi A, Abd AA, El-Latif SB (2016),A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Procss* 128:155–170

Kwok H S and Tang W K S(2007),A fast image encryption system based on chaotic maps with finite precision representation Chaos Soliton. Fract. **32** 1518-29

QiangZhang,LingGuo,XiaopengWei(2010),Image encryption using DNA addition combining with chaotic maps *Mathematical and computer modelling*, Volume 52, Issues 11–12, Pages 2028-2035

R. Guesmi, M. A. B. Farah,A. Kachouri M. Samet , A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2,*Nonlinear Dynamics* volume 83, pages1123–1136(2016)

Changjiang Zhu,Zhihua Gan,Yang Lu & Xiuli Chai(2020) , An image encryption algorithm based on 3-D DNA level permutation and substitution scheme, *Multimedia Tools and Applications* volume 79, pages7227–7258

Chai XL, Gan ZH, Yuan K, Chen YR, Liu XX (2019) ,A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural Computer Appl* 31:219–237

Chai XL, Fu XL, Gan ZH, Lu Y, Chen YR (2019),A color image cryptosystem based on dynamic DNA encryption and chaos, *Signal Process* 155:44–62

Z. Qiang, L. Guo, and X. Wei (2010), Image encryption using DNA addition combining with chaotic maps, *Mathematical & Computer Modelling*, vol. 52, no. 11-12, pp. 2028–2035

Y. Zhou, L. Bao, and C. L. P. Chen (2014), "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, no. 7, pp. 172–182.

L. Li, Z. Qiang, X. Wei, and C. Zhou, Image encryption algorithm based on chaotic modulation of Arnold dual scrambling and DNA computing, *Advanced Science Letters*, vol. 4, no. 11, pp. 3537–3542, 2011.

Wang X, Li P, Qian Y, Liu L, Zhang H, Wang X (2018), A novel color image encryption scheme using DNA permutation based on the Lorenz system, *Multimed Tools Appl* 77:6243–6265

Z. Yong(2014), Cryptanalysis of an image encryption algorithm based on chaotic modulation of Arnold dual scrambling and DNA computing, *Advanced Science Focus*, vol. 2, no. 1, pp. 67–82, 2014

Ying-Qian Zhang,Yi He,Pi Li,Xing-Yuan Wang(2020), "A new color image encryption scheme based on 2DNLCML system and genetic operations, Optics and Lasers in Engineering 128(2020) Elsevier

Hongjun Liu, Fengtong Wen,Abdurahman Kadir(2019) ,Construction of a new 2D Chebyshev-Sine map and its application to color image encryption, *Multimedia Tools and Applications* 78:15997–16010

Nabil Ben Slimane1, Nahed Aouf,Kais Bouallegue1 ,Mohsen Machhout (2018),A novel chaotic image cryptosystem based on DNA sequence operations and single neuron model, Multimed Tools Appl volume 77, pages30993–31019,

Wu X , Kurths J , Kan H (2018), A robust and lossless dna encryption scheme for color images. *Multimedia Tools Appl*; 77:12349–76.

Liu L L, Zhang Q and Wei X (2012), A RGB image encryption algorithm based on DNA encoding and chaos map, *Computers. And Electrical. Engineering.* 38, 1240-1248

Chai X, Chen Y and Broyde L (2017), A novel chaos-based image encryption algorithm using DNA sequence operations *Opt. Laser. Eng.* 88 197-213

Liyan Liu, Yingqian Zhang and Hengzhi Zhang(2018), A color image encryption algorithm based on DNA computation and Chen system, IOP Conf. Series: Journal of Physics: Conf. Series 1074 (2018) 012096I

Akgul A,Pehlivan I(2016) A new three dimension chaotic system without equilibrium points ,its dynamic analysis and electronic circuit application. DOI:10.17559/TV-20141212125942

Zaidan AA, Zaidan BB, Alsalem MA, Albahri OS, Albahri AS, Qahtan MY (2020) ,Multi-agent learning neural network and Bayesian model for real-time IoT skin detectors : a new evaluation and benchmarking methodology. *Neural Comput & Application* 32(12):8315–8366

***