Multimedia Tools and Applications (2019) 78:11675–11700
https://doi.org/10.1007/s11042-018-6711-0

# RADIANT - hybrid multilayered chaotic image encryption system for color images

N. Sasikaladevi[1] · K. Geetha[1] · K. Sriharshini[1] · M. Durga Aruna[1]

Received: 14 November 2017 / Revised: 1 August 2018 / Accepted: 19 September 2018 /
Published online: 2 October 2018

## Abstract

Rapid growth in the use of digitized images in commercial, business, government and medical use has led to the need for protecting the images against eavesdroppers and securely transmit them in the network. Images pertained to finance, medical and crime investigation fields are expected to be confidential because of its sensitivity. As reported in the literature most of encryption algorithms developed for gray images is only applied for color images. An exclusive system to exploit color spaces has been proposed that functions in a multilayered model. It is named as Hyb**R**id multil**A**yere**D** chaotic **I**m**A**ge e**N**cryp**T**ion (RADIANT) system to process sensitive color images especially applicable for medical and forensic domains. In the first layer, logistic mapping is done to perform chaotic masking, followed by DNA encoding in the second layer. This layer objective is to increase confusion diffusion level by substitution permutation. In the third layer, ECC over GF(p) that focus on spatial domain is adopted for encryption as it has been identified as a prominent encryption technique being popular for its mathematical strength. The proposed RADIANT system is hybrid in nature as it operates on both symmetric and asymmetric cryptosystem combination. Experimental results obtained by testing with bench mark images ascertain an ideal measure for MSE, PSNR that makes it more suitable for signal processing activities involving sensitive color images.

**Keywords** Elliptic curve cryptography · DNA encoding · Encryption · Decryption · Logistic map

## 1 Introduction

Expeditious growth of Internet increased the demand of protecting the data transmitted across the network. One way of protecting the data is by applying the cryptography mechanisms. It is used to secure the data in storage and data in transit. It ensures confidentiality and integrity of the data. As it is based on one way trap door function, only the authorized user can recover the

✉ N. Sasikaladevi
sasikalade@gmail.com

[1] Department of CSE/SoC, SASTRA University, Thanjavur, India

data and it prevents the modification by the intruders. Internet is used to exchange the data in different format such as text, image, audio etc. One of the predominant types of representation is image. In medical field, the medical images are transmitted over network for analysis and diagnosis. Patient can get the medical consultation from the medical expert across the world by sending medical reports in the form of images. In this case, preserving the privacy of the medical images is mandatory [45]. There is a demand to ensure the confidentiality for these medical records without altering the images. In the crime investigation, there is a need to transmit the images over the network in the secured manner. Ensuring the confidentiality is needed for the government domain also. In specific, it is needed in deference related issues. Hence, there is a need to protect the images.

There are two different ways to encrypt the images such as spatial domain and transform domain. Image encryption can further be classified as lossy encryption and lossless encryption. In lossy encryption methods, were the image details are somewhat distorted, the resulting decrypted image is different from the original image. Due to the characteristics of human perception, and depending on the application, a decrypted image with little distortion is usually acceptable.

## 1.1 Motivation

Since lossless encryption methods are more applicable in applications that insist distortion-free original image like in: medical images, aerospace images, satellite images, and in applications that involve huge classification. Lossy encryption is not suitable for medical images and crime record investigation [42]. Because even a microscopic change in the medical image may lead to wrong diagnosis which is undesirable. This requirement motivated us to put forward lossless encryption and decryption algorithms named as RADIANT. As compared to existing image encryption algorithms, RADIANT provides ideal MSE and PSNR. It shows that the decrypted image is exactly same as original image. Hence it is better suits for medial image encryption.

Images should be treated in the different manner and not like text data. Hence, modern symmetric crypto systems like DES (Data Encryption Standard), AES (Advanced Encryption Standards), IDES (International Data Encryption Standards) and asymmetric crypto system like RSA (Rivest Shamir Adleman) are not suitable for image encryption. The proposed RADIANT system is based on elliptic curve. By using elliptic curve, we can achieve the security level of RSA with minimal key length. Elliptic curve with 160 bit key size provides the security of RSA with 4096 bit key size. As it has minimal key length, the complexity of elliptic curve is less than RSA. Elliptic curve will further resist the side channel attack and timing attack. Research on elliptic curve based image encryption is less, because of the complexity of selecting the suitable elliptic curve for image encryption over finite field. In the proposed RADIANT system, the best suitable curve is used for encryption. The elliptic curve prime field is chosen by using Complex Multiplication (CM) method. It is proved in the result that the selected curve suits well for the image encryption.

Confidentiality requirement is very high for the images from the domain such as medical, defense and crime investigation. In this paper, multi layered encryption algorithm is proposed to provide high degree of confidentiality. Elliptic curve is used in one layer. In order to provide higher level of security, DNA scrambling is used to provide confusion and diffusion. DNA based permutation and substitution are performed in the image to scramble the pixel value. In this RADIANT system, individual color components are scrambled to provide high level of security. In the recent years, many chaotic image encryptions are proposed to ensure better security as compared to non-chaotic image encryption. Hence the proposed RADIANT system also contemplates on chaotic masking.

## 2 Related work

Image encryption algorithms are proposed by various researchers. Liansheng, et al. [40] proposed a chaotic encryption based on logistic map and Fractional Fourier Transform (FFT) for gray scale images. Plain image is first scrambled using two level logistic maps and then encrypted by FFT. Bhatnagar et al. [3] proposed multiple encryptions based on Discrete Factional Wavelet Transform (FrWT) for grayscale images. Image encryption based on scrambling and FFT is proposed in [23]. Image is randomly shifted by using Jigsaw Transform and then again scrambled by using Arnold Transform (ART). Zhang et al. [47] proposed Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. Discrete version of Chirikov standard map is used to scramble the pixels. Misra et al. [30] propose Security of color image data designed by public-key cryptosystem associated with 2D-DWT. Lima et al. [22] proposed image encryption based on FFT over finite fields for gray scale images. Symmetrical image encryption based on DWT is proposed in [29]. These image encryption algorithms are based on transform domain and it is lossy in nature. Hence, theses algorithms are not suitable for the domain in which recovered image need to be lossless. And, all theses algorithms are designed for gray scale images.

Jun Lang [20] proposed chaotic image encryption based on color blend and chaotic permutation. Red, Green and Blue color spaces are randomly mixed and then rotated with random angle matrix. Multi stage image encryption is proposed in [15] based on discrete affine cipher and Discrete Wavelet Transform (DWT). Zhang et al. [46] proposed RGB color image encryption based on Lorenz chaotic system and DNA computing. Liu et al. [28] proposed color image encryption based on DNA encoding and chaotic map. Wang et al. [43] proposed color image encryption based on column scrambling. Liu et al. [24] proposed color image encryption based on one-time keys and robust chaotic maps. Color image encryption using spatial bit-level permutation and high-dimension chaotic system is proposed in [25**].** Kumar et al. [16, 18] proposed RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography and RGB image encryption using diffusion process associated with chaotic map. Chaotic based image encryptions are proposed in [4, 5, 35–37]. Murillo et al. [32] proposed RGB image encryption algorithm based on total plain image characteristics and chaos. All these are color image encryption algorithms. Still, there is a need for multi level encryption algorithm to provide higher level of security.

Elliptic curve Elgamal image encryption for gray scale images is proposed in [21, 41, 44]. Chaotic Image encryption based on cyclic elliptic curve is proposed in [7]. Key stream with the size of 256 bit is created and mixed with key sequences from the cyclic elliptic curve points. Dolendro et al. [39] proposed image encryption using elliptic curve cryptography. Shukla et al. [38] proposed image encryption based on elliptic curve cryptography. Multi level color image encryption without loss is needed for privacy preserving medical images [27]. Light weight cryptography is demand for medical application [1, 2, 31]. The hardware realization of elliptic curve is analyzed in [9–12, 14] In this paper, multi layer color image encryption is proposed by exploiting the DNA computing for pixel scrambling Elliptic curve security. RADIANT system is proposed to provide high level of security for medical images and forensic images.

# 3 Preliminaries

## 3.1 Elliptic curve cryptography

Elliptic Curve Cryptography (ECC) is an asymmetric crypto system. It yields the equal level of security presented by RSA but with lesser key size. Hence it reduces the processing overhead. Elliptic curve is based on the Weierstrass equation of the form (1)

$$y^2 + axy + by = x^3 + cx^2 + dx + e \tag{1}$$

Where, a,b,c,d and e are real numbers and x and y take n values in the real numbers. Simplified form of the Eq. (1) is

$$y^2 = x^3 + ax + b(2) \tag{2}$$

(2) is the equation with the degree 3 where a and b are coefficients and x and y are variables. Elliptic curve over finite fields classified as either prime curve or binary curve. The prime curve is based on GF(p), the coefficients values lies in the set {0 to p-1} and depicted as $E_p$(a,b). The binary curve is based on GF($p^m$), the coefficients of the equation take values in GF($p^m$) and it is depicted as $E_p{}^m$(a,b) [9–11].

### 3.1.1 Arithmetic operations on ep(a,b)

$P + 0 = P$ where $P$, $Q \epsilon E_p(a, b)$.
If $P = (x_p, y_p)$ then $-P = (x_p, -y_p)$
If $P = (x_p, y_p)$ and $Q = (x_Q, y_Q)$ with $P \neq -Q$ then $R = P + Q = (x_R, y_R)$ is based on the formula given below,

$$x_R = \left(\lambda^2 - xp - xq\right) modp$$
$$y_R = (\lambda(xp - xR) - yp) modp$$

Where

$$\lambda = \begin{cases} \dfrac{y_Q - y_p}{x_q - x_p} modp, ifP \neq Q \\ \dfrac{3x^2 p + a}{2yp} modp, ifP = Q \end{cases}$$

Elliptic curve process involves a Generator G and an elliptic curve $E_p$(a,b). B picks a private key d and estimates the public key by $P_A$ = d* G. B sends the pair (G, $P_A$) to A. A picks the data $P_m$ and choose the session key r. Then he encrypts the $P_m$ based on (3)

$$C1 = r{*}G, C2 = P_m + rP_A \tag{3}$$

The cipher pair (C1, C2) sent across the channel. B decrypts the data based on (4)

$$P_m = C2 - d{*}C1 \tag{4}$$

A transmits the encrypted data over the channel and B successfully decrypts the data without revealing their own secrets.

### 3.2 DNA computing

DNA computing is a form of computing which uses DNA, biochemistry and molecular biology, instead of the traditional silicon-based computer technologies. DNA computing, or more generally, bimolecular computing, is a fast developing interdisciplinary area. With the rapid development of DNA computing, the researchers presented many biological operations and algebra operations based on DNA sequence [6, 33]. A new method of computing using DNA plasmids is introduced in [14]. DNA computing is used in the security domain [8, 13, 34, 48] for enforcing confidentiality, integrity and authentication. DNA sequencing is based on four basic nucleic acids namely, Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). Adenine and Thymine; Cytosine and Guanine are complements of each other

Single-strand DNA sequence is composed by four bases, they are A, C, G and T, where A and T are complement to each other, so are C and G. In the modern theory of electronic computer, all information is expressed by binary system. But in DNA coding theory, information is represented by DNA sequences. So we use binary numbers to express the four bases in DNA sequence and two bits binary number to represent a base. In the theory of binary system, 0 and 1 are complementary, so we can obtain that 00 and 11, 01 and 10 are also complementary. We can use 00, 01, 10 and 11 to express four bases and the number of coding combination kinds is 4! = 24. Due to the complementary relation between DNA bases, there are only eight kinds of coding combinations that satisfy the principle of complementary base pairing in 24 kinds of coding combinations. Table 1 lists eight encoding rules:

xExample: The binary pixel value of an image is [0 0 1 1 1 0 1 0], so the corresponding DNA sequence is [A T G G] according to the first encoding rule, similarly according to the seventh decoding rule, the decoding sequence is [1 1 0 0 1 0 1 0]. In the proposed algorithm, we put the eight encoding and decoding rules mapped to the eight sub-region of (0,1), and using the seed generated by random number to choose different rules. In the proposed RADIANT system rule 1 is used for DNA encoding. The 32 bit pixel values of the image is divided into 4 components such as a, r, b and g. Each of these components is the 8 bit binary data. It is further divided into four 2-bit DNA sequence.

### 3.3 The addition and subtraction operation of DNA sequence

Since the development of DNA computing, researchers have proposed algebraic operation of DNA sequence to replace the traditional computer algebraic operation. Based on this, we use DNA addition operation to realize DNA sequence matrix computing for R, G, B components. The algorithm of this paper finds out DNA addition and subtraction rules by using mod 2 operations of binary figure when 01 – A, 10 – T, 00 – C, 11 – G, as mentioned in Table 2.

**Table 1** DNA mapping rule

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

**Table 2** DNA addition and DNA subtraction

| + | A | T | C | G | – | A | T | C | G |
|---|---|---|---|---|---|---|---|---|---|
| G | C | A | G | G | G | C | A | G | G |
| C | A | T | C | T | C | A | T | C | T |
| T | G | C | T | A | T | G | C | T | A |
| A | T | G | A | C | A | T | G | A | C |

## 4 Proposed RADIANT framework

The proposed image encryption scheme is having three phases. In the first phase, image is masked by logistic map. In the second phase, the resultant image is encrypted using

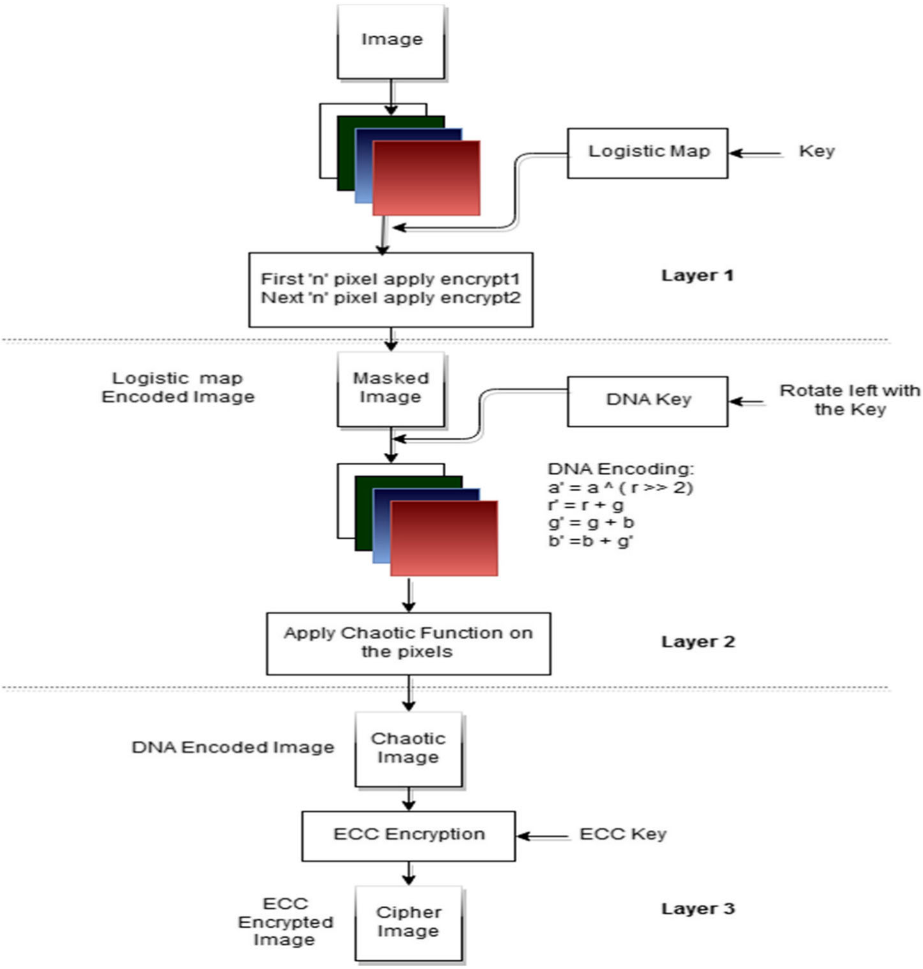


**Fig. 1** RADIANT Forward process

DNA encoding. In the third phase, the image is encrypted by ECC. The proposed framework is implemented in three phases to achieve high confidentiality as compared to Elliptic curve based encryption scheme. It is used to provide better secrecy for medical images. Elliptic curve with prime field $E_{2147483647}(0, 390064447)$ is used in this model. This curve is designed by using prime number. Bit size of this prime number is 32 bits. Only Quantum computers can break this curve, because brute force crypt analysis requires $2^{32}$ trials. One possible solution is increasing the curve size. Increased curve size will result in increased complexity of point addition and doubling operations. Hence, DNA based cryptography has been identified and implemented in the second phase as depicted in Fig. 1. The forward process of the proposed RADIANT algorithm starts with logistic mapping to mask the image. Then it is encoded with the DNA key and then chaotic function is applied. This phase is then followed by ECC encryption to generate the cipher image

In this paper keyed logistic map is proposed. The color components (Red, Green and Blue) are first extracted. Two chaotic sequences are generated for each color plane. Random seed is calculated based on Eq. (5) and it is based on given key. Logistic map is created based on the equation.

$$X_0 = [( K_{7-0} \oplus K_{24-32}) \oplus ( K_{15-8} \& K_{23-16})]\%255 \tag{5}$$

where, k is the key.

$$X_{n+1} = r^* X_n \,(1-X_n) \tag{6}$$

where, r is 3.999. (6) as mentioned in Fig. 2.

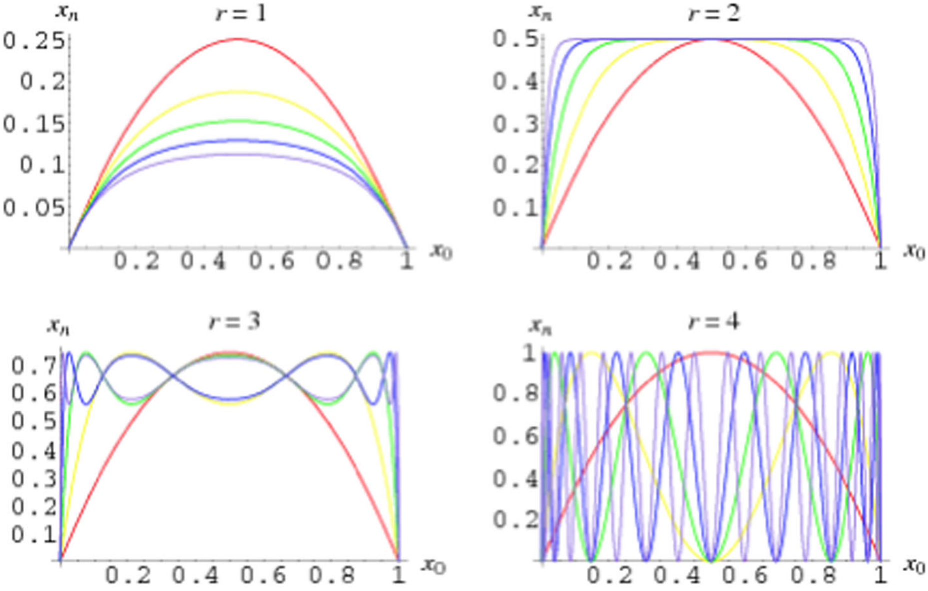


**Fig. 2** Performance of Control parameter ‘r’

Logistic map based pixel masking is performed based on the given formulas.

Encoding 1:

Case 1:

$$\left.\begin{aligned} A_i &= A_i \\ R_i &= R_i + 256 - A_i \\ G_i &= G_i + 256 - R_i \\ B_i &= B_i + 256 - G_i \end{aligned}\right\} \begin{array}{c} \text{where,} \\ 0 \geq X_i > 0.125 \\ 0.375 \geq X_i > 0.5 \end{array}$$

Case 2:

$$\left.\begin{aligned} A_i &= A_i \\ R_i &= R_i + 256 - (\, K_{7-0} + \, K_{15-8}) \\ G_i &= G_i + 256 - R_i \\ B_i &= B_i + 256 - G_i \end{aligned}\right\} \begin{array}{c} \text{where,} \\ 0.25 \geq X_i > 0.375 \\ 0.75 \geq X_i \\ > 0.8755 \end{array}$$

Case 3:

$$\left.\begin{aligned} A_i &= A_i \\ R_i &= R_i + 256 - 255 \\ G_i &= G_i + 256 - A_i \\ B_i &= B_i + 256 - \, K_{15-8} \end{aligned}\right\} \begin{array}{c} \text{where,} \\ 0.125 \geq X_i \\ > 0.275 \\ 0.625 \geq X_i > 0.75 \end{array}$$

Case 4:

$$\left.\begin{aligned} A_i &= A_i \\ R_i &= R_i + 256 - \, K_{15-8} \\ G_i &= G_i + 256 - \, K_{7-0} \\ B_i &= B_i + 256 - \, K_{15-8} \end{aligned}\right\} \begin{array}{c} \text{where,} \\ 0.5 \geq X_i > 0.625 \\ 0.875 \geq X_i > 1 \end{array}$$

Encoding 2:

Case 1:

$$\left.\begin{aligned} A_i &= A_i \\ R_i &= (R_i + A_i) \,\%\, 256 \\ G_i &= (G_i + R_i\,) \,\%\, 256 \\ B_i &= (B_i + G_i) \,\%\, 256 \end{aligned}\right\} \begin{array}{c} \text{where,} \\ 0 \geq X_i > 0.125 \\ 0.375 \geq X_i > 0.5 \end{array}$$

Case 2:

$$\left.\begin{aligned} A_i &= A_i \\ R_i &= (R_i + \, K_{7-0} + \, K_{15-8}) \,\%\, 256 \\ G_i &= (G_i + R_i\,) \,\%\, 256 \\ B_i &= (B_i + G_i) \,\%\, 256 \end{aligned}\right\} \begin{array}{c} \text{where,} \\ 0.25 \geq X_i > 0.375 \\ 0.75 \geq X_i \\ > 0.8755 \end{array}$$

Case 3:

$$\left.\begin{aligned} A_i &= A_i \\ R_i &= (R_i + 255) \,\%\, 256 \end{aligned}\right\} \text{where,}$$

$$\begin{aligned} G_i &= (G_i + A_i\,) \,\%\, 256 \\ B_i &= (B_i + A_i) \,\%\, 256 \end{aligned} \qquad \begin{array}{c} 0.125 \geq X_i \\ > 0.275 \\ 0.625 \geq X_i > 0.75 \end{array}$$

Case 4:

$$\left.\begin{aligned} A_i &= A_i \\ R_i &= (R_i + \, K_{15-8}) \,\%\, 256 \\ G_i &= (G_i + A_i\,) \,\%\, 256 \\ B_i &= (B_i + A_i) \,\%\, 256 \end{aligned}\right\} \begin{array}{c} \text{where,} \\ 0.5 \geq X_i > 0.625 \\ 0.875 \geq X_i > 1 \end{array}$$

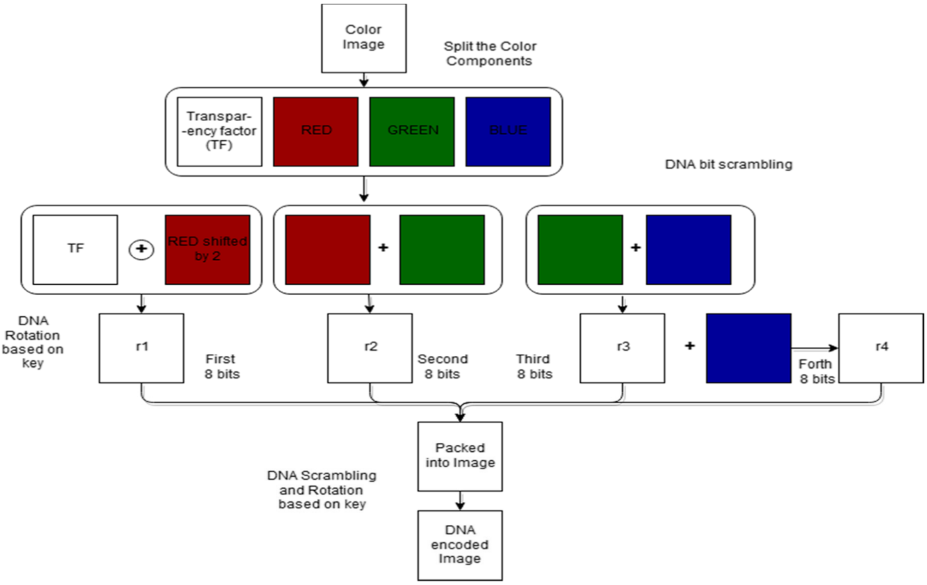
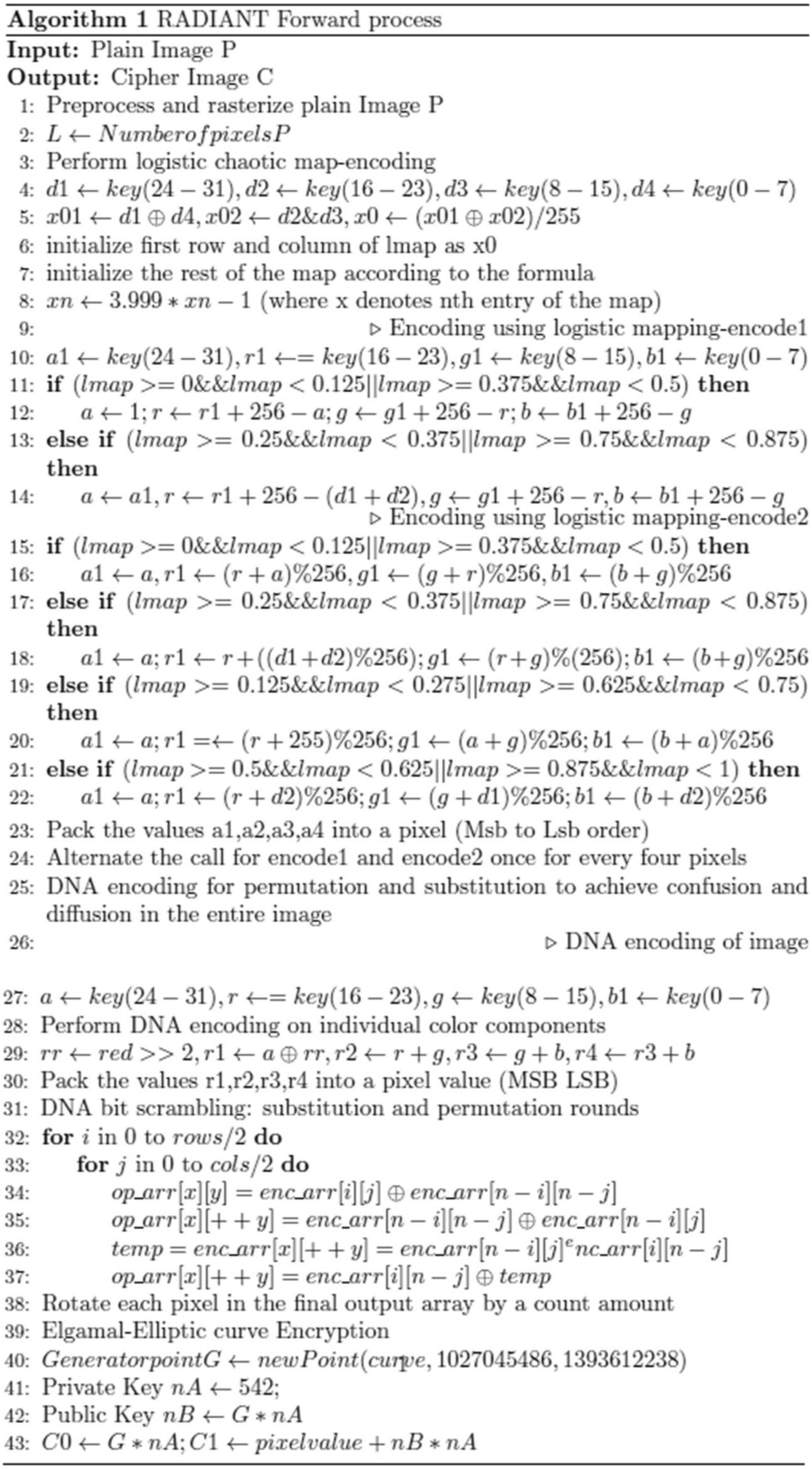


**Fig. 3** DNA Encoding Process

Encoding 1 and Encoding 2 are alternated once for every four pixels.

Figure 3 explains the flow of DNA encoding process that reserves 8 bit for transparency factor and 8 bits for each of the RED,GREE, BLUE color component and hence a total 32 bit representation. DNA scrambling and rotations are made to obtain DNA encoded image. In the third phase of the forward process, Elgamal elliptic curve based encryption performed on every pair of pixels. Elliptic curve is chosen to improve the security strength of the forward process.

Algorithm1 named as Radiant Forward process illustrates the various steps carried out in the forward process. The input plain image P is processed to get the required encrypted cipher image C. As mentioned in the algorithm the plain image is preprocessed and rasterized. Logistic chaotic map encoding is performed followed by DNA encoding to achieve confusion and diffusion in the entire image. The complexity of this forward process algorithm is in the order of O(n2) which falls under the quadratic time complexity.



```
Algorithm 1 RADIANT Forward process
Input: Plain Image P
Output: Cipher Image C
Preprocess and rasterize plain Image P
$L \leftarrow NumberofpixelsP$
Perform logistic chaotic map-encoding
$d1 \leftarrow key(24-31), d2 \leftarrow key(16-23), d3 \leftarrow key(8-15), d4 \leftarrow key(0-7)$
$x01 \leftarrow d1 \oplus d4, x02 \leftarrow d2\&d3, x0 \leftarrow (x01 \oplus x02)/255$
initialize first row and column of lmap as x0
initialize the rest of the map according to the formula
$xn \leftarrow 3.999 * xn - 1$ (where x denotes nth entry of the map)
                                        ▷ Encoding using logistic mapping-encode1
$a1 \leftarrow key(24-31), r1 \leftarrow= key(16-23), g1 \leftarrow key(8-15), b1 \leftarrow key(0-7)$
if $(lmap >= 0\&\&lmap < 0.125||lmap >= 0.375\&\&lmap < 0.5)$ then
    $a \leftarrow 1; r \leftarrow r1 + 256 - a; g \leftarrow g1 + 256 - r; b \leftarrow b1 + 256 - g$
else if $(lmap >= 0.25\&\&lmap < 0.375||lmap >= 0.75\&\&lmap < 0.875)$ then
    $a \leftarrow a1, r \leftarrow r1 + 256 - (d1 + d2), g \leftarrow g1 + 256 - r, b \leftarrow b1 + 256 - g$
                                        ▷ Encoding using logistic mapping-encode2
if $(lmap >= 0\&\&lmap < 0.125||lmap >= 0.375\&\&lmap < 0.5)$ then
    $a1 \leftarrow a, r1 \leftarrow (r + a)\%256, g1 \leftarrow (g + r)\%256, b1 \leftarrow (b + g)\%256$
else if $(lmap >= 0.25\&\&lmap < 0.375||lmap >= 0.75\&\&lmap < 0.875)$ then
    $a1 \leftarrow a; r1 \leftarrow r + ((d1 + d2)\%256); g1 \leftarrow (r + g)\%(256); b1 \leftarrow (b + g)\%256$
else if $(lmap >= 0.125\&\&lmap < 0.275||lmap >= 0.625\&\&lmap < 0.75)$ then
    $a1 \leftarrow a; r1 =\leftarrow (r + 255)\%256; g1 \leftarrow (a + g)\%256; b1 \leftarrow (b + a)\%256$
else if $(lmap >= 0.5\&\&lmap < 0.625||lmap >= 0.875\&\&lmap < 1)$ then
    $a1 \leftarrow a; r1 \leftarrow (r + d2)\%256; g1 \leftarrow (g + d1)\%256; b1 \leftarrow (b + d2)\%256$
Pack the values a1,a2,a3,a4 into a pixel (Msb to Lsb order)
Alternate the call for encode1 and encode2 once for every four pixels
DNA encoding for permutation and substitution to achieve confusion and diffusion in the entire image
                                        ▷ DNA encoding of image

$a \leftarrow key(24-31), r \leftarrow= key(16-23), g \leftarrow key(8-15), b1 \leftarrow key(0-7)$
Perform DNA encoding on individual color components
$rr \leftarrow red >> 2, r1 \leftarrow a \oplus rr, r2 \leftarrow r + g, r3 \leftarrow g + b, r4 \leftarrow r3 + b$
Pack the values r1,r2,r3,r4 into a pixel value (MSB LSB)
DNA bit scrambling: substitution and permutation rounds
for $i$ in 0 to $rows/2$ do
    for $j$ in 0 to $cols/2$ do
        $op\_arr[x][y] = enc\_arr[i][j] \oplus enc\_arr[n-i][n-j]$
        $op\_arr[x][++y] = enc\_arr[n-i][n-j] \oplus enc\_arr[n-i][j]$
        $temp = enc\_arr[x][++y] = enc\_arr[n-i][j]^{e}nc\_arr[i][n-j]$
        $op\_arr[x][++y] = enc\_arr[i][n-j] \oplus temp$
Rotate each pixel in the final output array by a count amount
Elgamal-Elliptic curve Encryption
$GeneratorpointG \leftarrow newPoint(curve, 1027045486, 1393612238)$
Private Key $nA \leftarrow 542$;
Public Key $nB \leftarrow G * nA$
$C0 \leftarrow G * nA; C1 \leftarrow pixelvalue + nB * nA$
```

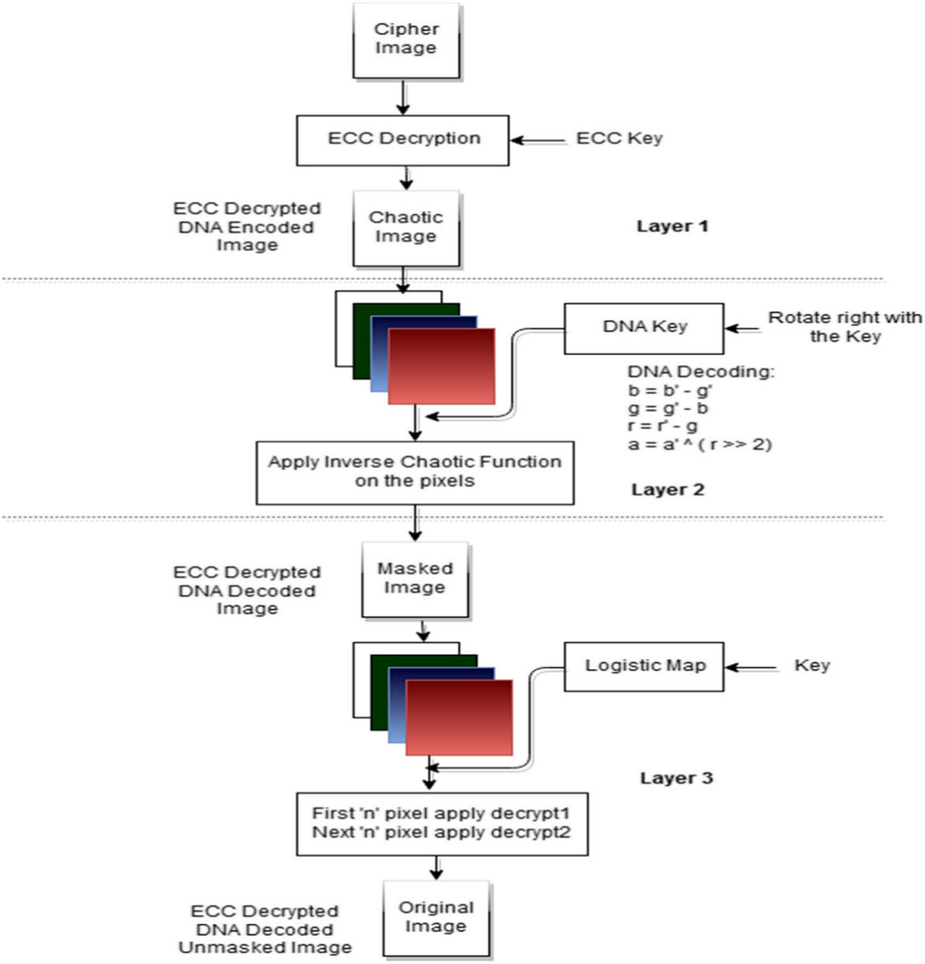

Cipher Image
ECC Decryption
ECC Key
ECC Decrypted DNA Encoded Image
Chaotic Image
Layer 1
DNA Key
Rotate right with the Key
DNA Decoding:
b = b' - g'
g = g' - b
r = r' - g
a = a' ^ ( r >> 2)
Apply Inverse Chaotic Function on the pixels
Layer 2
ECC Decrypted DNA Decoded Image
Masked Image
Logistic Map
Key
Layer 3
First 'n' pixel apply decrypt1
Next 'n' pixel apply decrypt2
ECC Decrypted DNA Decoded Unmasked Image
Original Image

**Fig. 4** RADIANT Reverse Process

Figure 4 outlines the RADIANT reverse process that is initiated with a decryption process of the cipher image and then DNA encoded. Inverse chaotic function is then applied before the application of logistic map to get the decrypted version.

Logistic map based pixel unmasking is performed based on the given formulas.

Encoding 1: Case 1:

$$\left.\begin{array}{c} A_i = A_i \\ R_i = R_i + 256 - A_i \\ G_i = G_i + 256 - R_i \\ B_i = B_i + 256 - G_i \end{array}\right\} \begin{array}{c} \text{where,} \\ 0 \geq X_i > 0.125 \\ 0.375 \geq X_i > 0.5 \end{array}$$

Case 2:

$$\left.\begin{array}{c} A_i = A_i \\ R_i = R_i + 256 - (\,K_{7-0} + \,K_{15-8}) \\ G_i = G_i + 256 - R_i \\ B_i = B_i + 256 - G_i \end{array}\right\} \begin{array}{c} \text{where,} \\ 0.25 \geq X_i > 0.375 \\ 0.75 \geq X_i \\ > 0.8755 \end{array}$$

Case 3:

$$\left.\begin{array}{c} A_i = A_i \\ R_i = R_i + 256 - 255 \\ G_i = G_i + 256 - A_i \\ B_i = B_i + 256 - \,K_{15-8} \end{array}\right\} \begin{array}{c} \text{where,} \\ 0.125 \geq X_i \\ > 0.275 \\ 0.625 \geq X_i > 0.75 \end{array}$$

Case 4:

$$\left.\begin{array}{c} A_i = A_i \\ R_i = R_i + 256 - \,K_{15-8} \\ G_i = G_i + 256 - \,K_{7-0} \\ B_i = B_i + 256 - \,K_{15-8} \end{array}\right\} \begin{array}{c} \text{where,} \\ 0.5 \geq X_i > 0.625 \\ 0.875 \geq X_i > 1 \end{array}$$

Encoding 2: Case 1:

$$\left.\begin{array}{c} A_i = A_i \\ R_i = (R_i + A_i)\ \%\ 256 \\ G_i = (G_i + R_i\,)\ \%\ 256 \\ B_i = (B_i + G_i)\ \%\ 256 \end{array}\right\} \begin{array}{c} \text{where,} \\ 0 \geq X_i > 0.125 \\ 0.375 \geq X_i > 0.5 \end{array}$$

Case 2:

$$\left.\begin{array}{c} A_i = A_i \\ R_i = (R_i + \,K_{7-0} + \,K_{15-8})\ \%\ 256 \\ G_i = (G_i + R_i\,)\ \%\ 256 \\ B_i = (B_i + G_i)\ \%\ 256 \end{array}\right\} \begin{array}{c} \text{where,} \\ 0.25 \geq X_i > 0.375 \\ 0.75 \geq X_i \\ > 0.8755 \end{array}$$

Case 3:

$$\left.\begin{array}{c} A_i = A_i \\ R_i = (R_i + 255)\ \%\ 256 \end{array}\right\} \begin{array}{c} \text{where,} \end{array}$$

$$\begin{array}{c} G_i = (G_i + A_i\,)\ \%\ 256 \\ B_i = (B_i + A_i)\ \%\ 256 \end{array} \qquad \begin{array}{c} 0.125 \geq X_i \\ > 0.275 \\ 0.625 \geq X_i > 0.75 \end{array}$$

Case 4:

$$\left.\begin{array}{c} A_i = A_i \\ R_i = (R_i + \,K_{15-8})\ \%\ 256 \\ G_i = (G_i + A_i\,)\ \%\ 256 \\ B_i = (B_i + A_i)\ \%\ 256 \end{array}\right\} \begin{array}{c} \text{where,} \\ 0.5 \geq X_i > 0.625 \\ 0.875 \geq X_i > 1 \end{array}$$

Decoding 1 and Decoding 2 are alternated once for every four pixels. Figure 5 illustrates the DNA decoding process that performs the subtraction and Ex-OR operations.

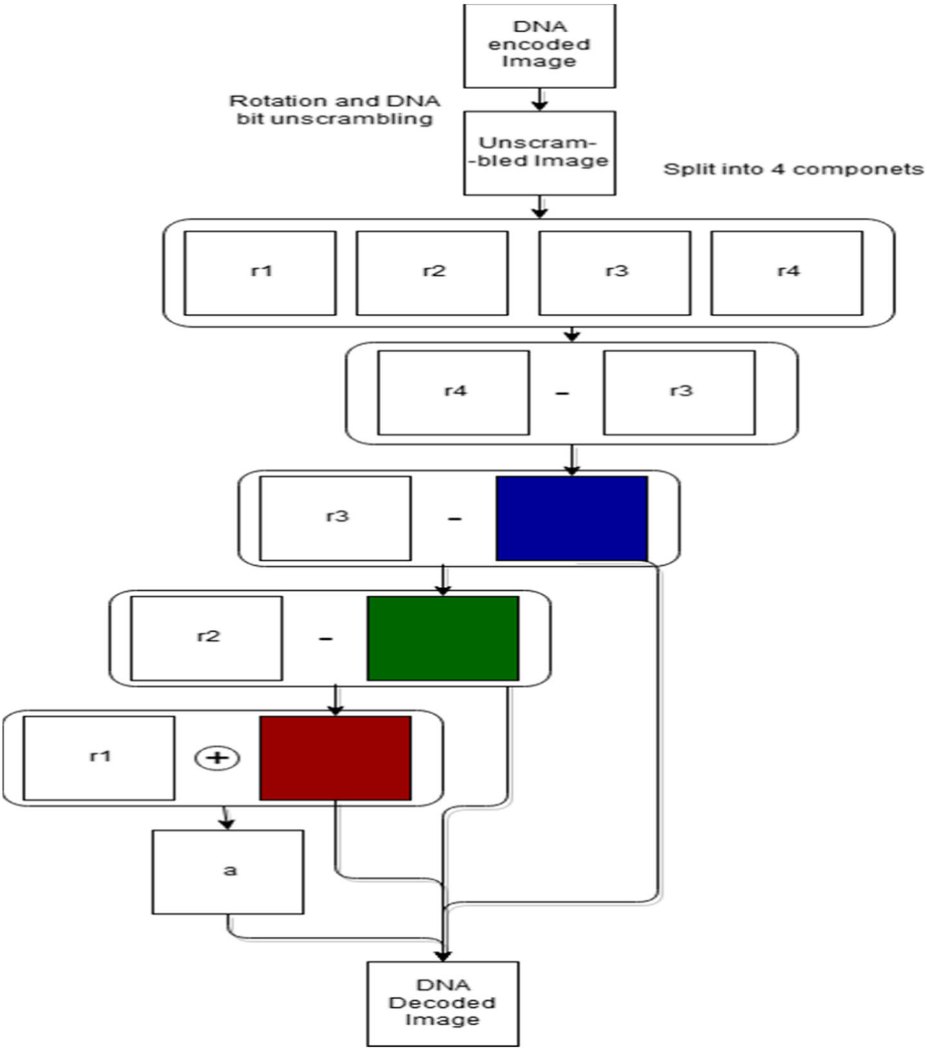
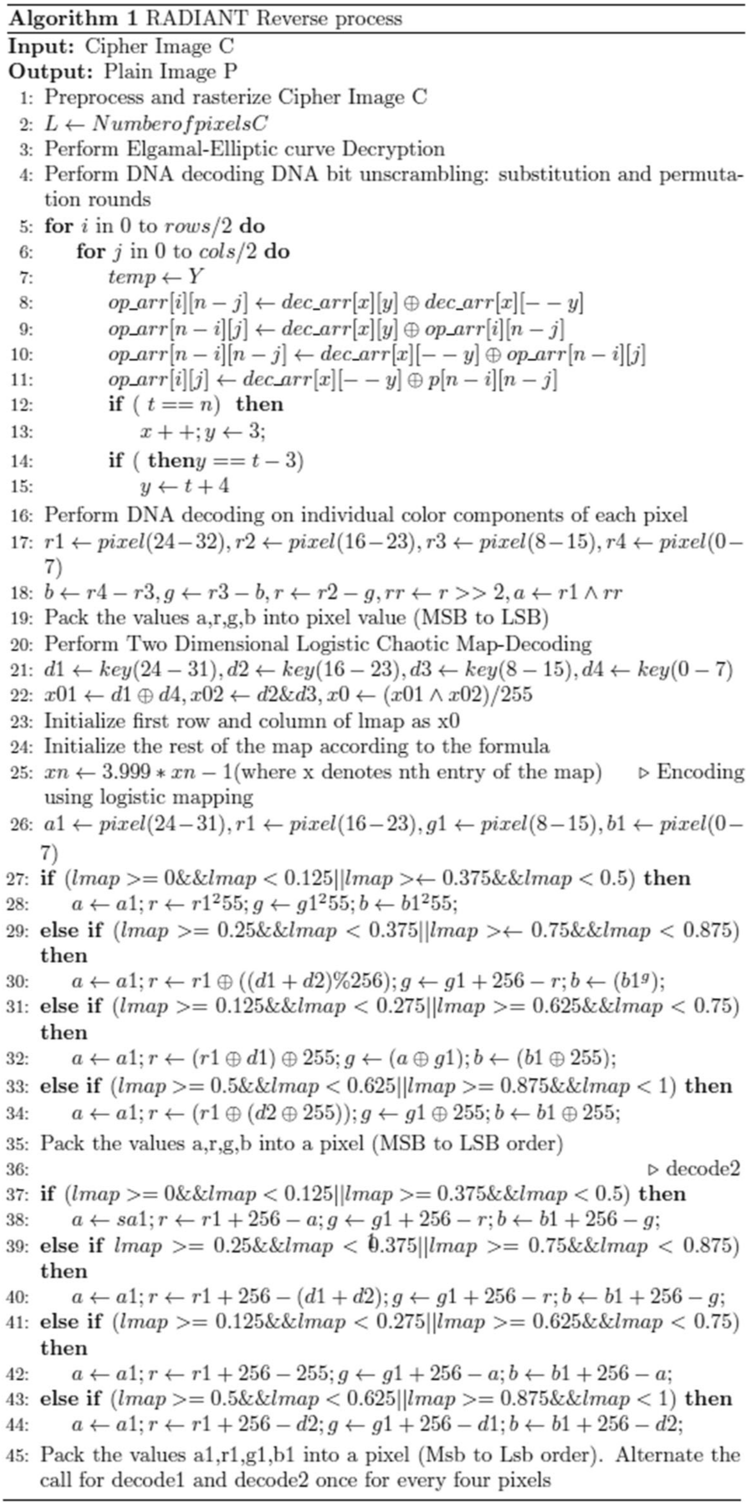


**Fig. 5** DNA Decoding Process

Algorithm 2 Radian Reverse process explains the phases involved in the reverse process. It accepts the Cipher image C as input and derives Plain image P as output. The image is preprocessed and Elgamal elliptic decryption is done by DNA decoding and then unscrambled. Logistic chaotic map decoding is performed at the end before decryption. The complexity of this reverse process algorithm is in the order of O(n$^2$) which falls under the quadratic time complexity.



**Algorithm 1** RADIANT Reverse process

**Input:** Cipher Image C

**Output:** Plain Image P

```
Preprocess and rasterize Cipher Image C
$L \leftarrow NumberofpixelsC$
Perform Elgamal-Elliptic curve Decryption
Perform DNA decoding DNA bit unscrambling: substitution and permutation rounds
for $i$ in 0 to $rows/2$ do
    for $j$ in 0 to $cols/2$ do
        $temp \leftarrow Y$
        $op\_arr[i][n-j] \leftarrow dec\_arr[x][y] \oplus dec\_arr[x][--y]$
        $op\_arr[n-i][j] \leftarrow dec\_arr[x][y] \oplus op\_arr[i][n-j]$
        $op\_arr[n-i][n-j] \leftarrow dec\_arr[x][--y] \oplus op\_arr[n-i][j]$
        $op\_arr[i][j] \leftarrow dec\_arr[x][--y] \oplus p[n-i][n-j]$
        if ( $t == n$ ) then
            $x++; y \leftarrow 3;$
        if ( then$y == t-3$)
            $y \leftarrow t+4$
Perform DNA decoding on individual color components of each pixel
$r1 \leftarrow pixel(24-32), r2 \leftarrow pixel(16-23), r3 \leftarrow pixel(8-15), r4 \leftarrow pixel(0-7)$
$b \leftarrow r4-r3, g \leftarrow r3-b, r \leftarrow r2-g, rr \leftarrow r >> 2, a \leftarrow r1 \wedge rr$
Pack the values a,r,g,b into pixel value (MSB to LSB)
Perform Two Dimensional Logistic Chaotic Map-Decoding
$d1 \leftarrow key(24-31), d2 \leftarrow key(16-23), d3 \leftarrow key(8-15), d4 \leftarrow key(0-7)$
$x01 \leftarrow d1 \oplus d4, x02 \leftarrow d2\&d3, x0 \leftarrow (x01 \wedge x02)/255$
Initialize first row and column of lmap as x0
Initialize the rest of the map according to the formula
$xn \leftarrow 3.999 * xn - 1$(where x denotes nth entry of the map)    ▷ Encoding using logistic mapping
$a1 \leftarrow pixel(24-31), r1 \leftarrow pixel(16-23), g1 \leftarrow pixel(8-15), b1 \leftarrow pixel(0-7)$
if ($lmap >= 0\&\&lmap < 0.125||lmap > \leftarrow 0.375\&\&lmap < 0.5$) then
    $a \leftarrow a1; r \leftarrow r1^255; g \leftarrow g1^255; b \leftarrow b1^255;$
else if ($lmap >= 0.25\&\&lmap < 0.375||lmap > \leftarrow 0.75\&\&lmap < 0.875$) then
    $a \leftarrow a1; r \leftarrow r1 \oplus ((d1+d2)\%256); g \leftarrow g1+256-r; b \leftarrow (b1^g);$
else if ($lmap >= 0.125\&\&lmap < 0.275||lmap >= 0.625\&\&lmap < 0.75$) then
    $a \leftarrow a1; r \leftarrow (r1 \oplus d1) \oplus 255; g \leftarrow (a \oplus g1); b \leftarrow (b1 \oplus 255);$
else if ($lmap >= 0.5\&\&lmap < 0.625||lmap >= 0.875\&\&lmap < 1$) then
    $a \leftarrow a1; r \leftarrow (r1 \oplus (d2 \oplus 255)); g \leftarrow g1 \oplus 255; b \leftarrow b1 \oplus 255;$
Pack the values a,r,g,b into a pixel (MSB to LSB order)
                                                                 ▷ decode2
if ($lmap >= 0\&\&lmap < 0.125||lmap >= 0.375\&\&lmap < 0.5$) then
    $a \leftarrow sa1; r \leftarrow r1+256-a; g \leftarrow g1+256-r; b \leftarrow b1+256-g;$
else if $lmap >= 0.25\&\&lmap < 0.375||lmap >= 0.75\&\&lmap < 0.875$) then
    $a \leftarrow a1; r \leftarrow r1+256-(d1+d2); g \leftarrow g1+256-r; b \leftarrow b1+256-g;$
else if ($lmap >= 0.125\&\&lmap < 0.275||lmap >= 0.625\&\&lmap < 0.75$) then
    $a \leftarrow a1; r \leftarrow r1+256-255; g \leftarrow g1+256-a; b \leftarrow b1+256-a;$
else if ($lmap >= 0.5\&\&lmap < 0.625||lmap >= 0.875\&\&lmap < 1$) then
    $a \leftarrow a1; r \leftarrow r1+256-d2; g \leftarrow g1+256-d1; b \leftarrow b1+256-d2;$
Pack the values a1,r1,g1,b1 into a pixel (Msb to Lsb order). Alternate the call for decode1 and decode2 once for every four pixels
```

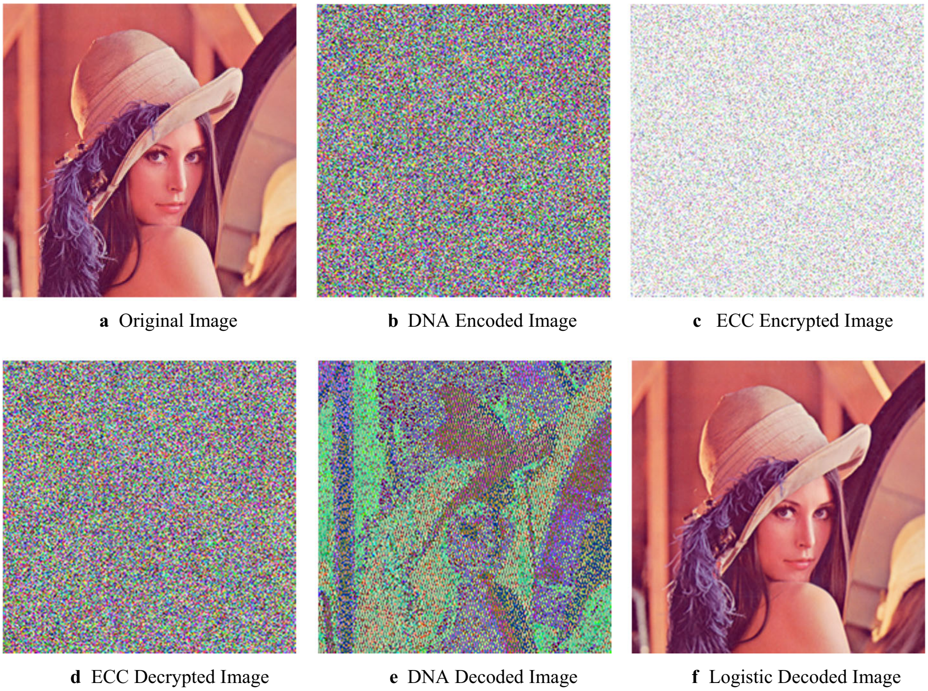


**Fig. 6** **a** Original Image **b** DNA Encoded Image **c** ECC Encrypted Image **d** ECC Decrypted Image **e** DNA Decoded Image **f** Logistic Decoded Image

## 5 Simulation and analysis

Bench mark color images are taken with the resolution of 512 * 512. The following Elliptic curve has been chosen for the image encryption, where p is 214783647, which is a 32 bit prime number.

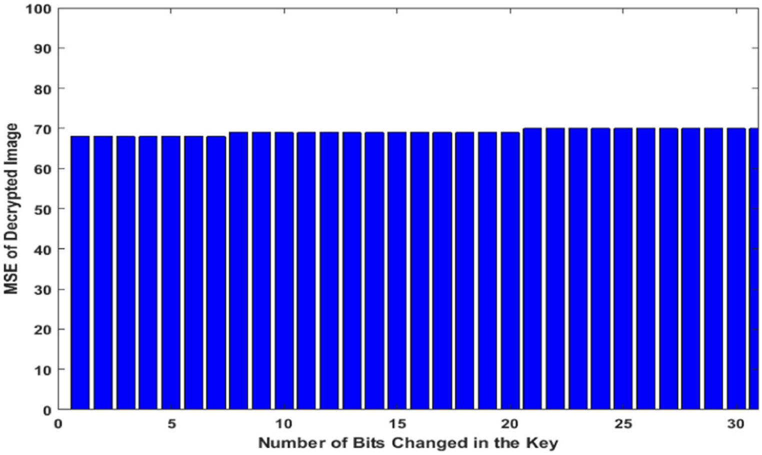


**Fig. 7** Key Sensitivity of Lena Image

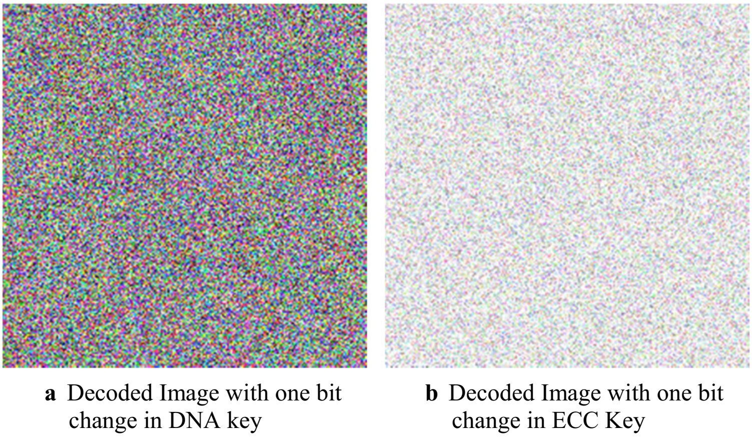

a Decoded Image with one bit change in DNA key
b Decoded Image with one bit change in ECC Key

**Fig. 8** **a** Decoded Image with one bit change in DNA key. **b** Decoded Image with one bit change in ECC Key

$$E_{2147483647}(0, 390064447) \tag{7}$$

Each pixel intensity of the image is converted into curve co-ordinate value. Since, the proposed model is designed for color image with 32 bit pixel, the curve is selected over 32 bit prime number. Elliptic curve is selected based on complex multiplication method. Figure 6 depicts the RADIANT forward process and the RADIANT reverse process of Lena image. The proposed RADIANT system yields better results on true color images of any size. The proposed RADIANT system is hybrid in nature. Asymmetric crypt-system is applied by using ECC. Further the security is increased by symmetric crypto-system by using DNA encoding. Logistic mapping is designed for chaotic images which improves the degree of confidentiality. In elliptic curve encryption layer, entire image is transformed into binary, pixel intensity and then the values are paired to form the point chosen curve.

## 5.1 Key space analysis

The security of the algorithm is based on the key space. Larger the key space more the effort on crypt analysis. The key space of the RADIANT is high and hence less vulnerable to different attacks.

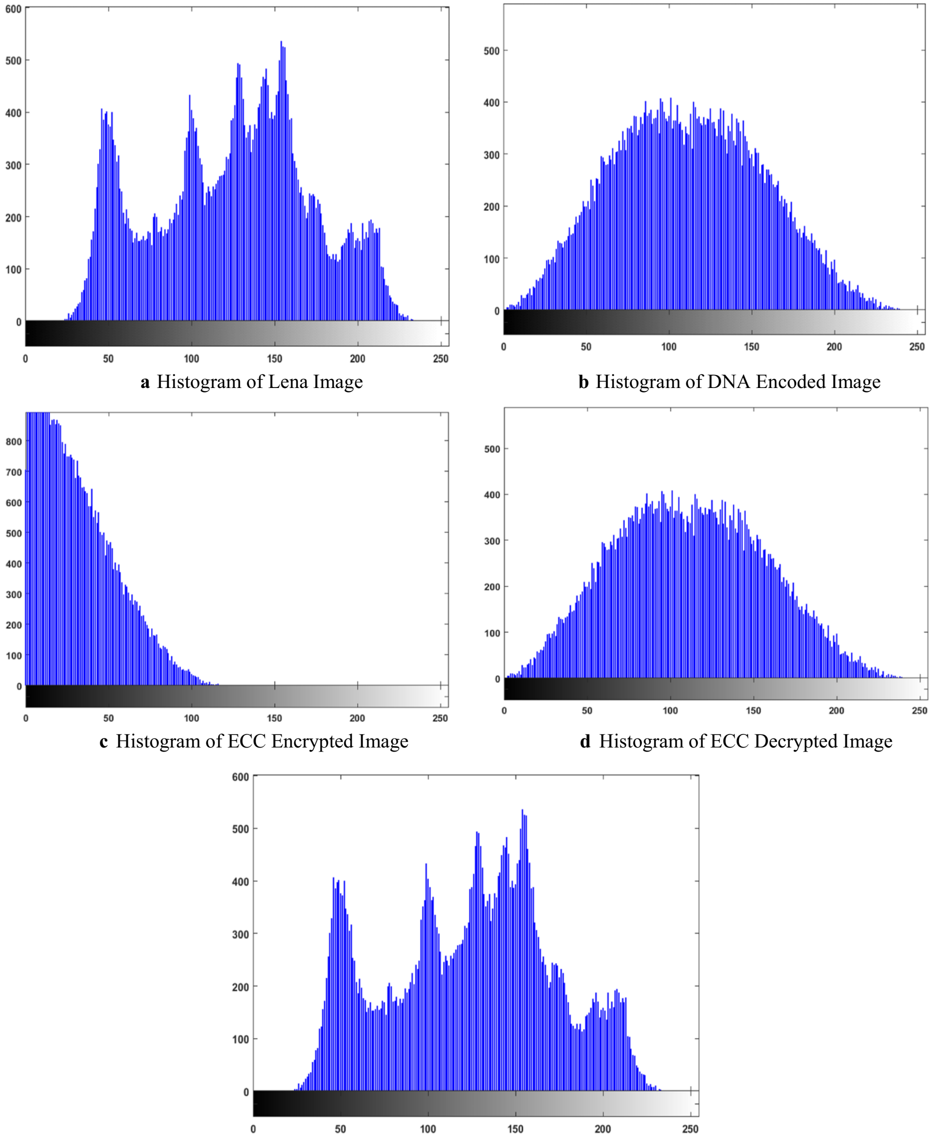
Key space = Seed of Logistic Map * Number of DNA complement rule * DNA computing Key * ECC private key * ECC ephemeral key

Key space = $2^{32} * 8 * 2^{32} * 2^{32} * 2^{32} = 8 * 2^{128}$

The key space of the proposed work is eight times higher than the key space of AES ($2^{128}$). This is achieved without any extra overhead and also with less computational complexity as that of AES. The proposed algorithm uses the large elliptic curve. Number of points in the curve is also high enough to resist the attacks.

## 5.2 Key sensitivity analysis

The proposed algorithm uses three keys such as the logistic seed, DNA shifting value and ECC private key. All the three keys are needed to perform the encryption perfectly. Decryption should not be allowed with minar change in any of these three keys.



**a** Histogram of Lena Image

**b** Histogram of DNA Encoded Image

**c** Histogram of ECC Encrypted Image

**d** Histogram of ECC Decrypted Image

**e** Histogram of Logistic Decoded Image

**Fig. 9** **a** Histogram of Lena Image **b** Histogram of DNA Encoded Image **c** Histogram of ECC Encrypted Image **d** Histogram of ECC Decrypted Image

Figure depicts the performance of key sensitivity analysis. Figure 7 shows the result of bit change in the key of logistic mapping.

Figure 8a shows the result of one bit change in the Logistic seed. All the tests are applied on the bench mark color image Lenna. An increased level of security is guaranteed, as it will be impossible to decrypt without knowing the DNA key and logistic key, even if ECCs public and private keys are known. The keys for DNA and logistic mapping decryption should be exactly

**Table 3** Corelation coefficient of Images

| | | Original | Encrypted | Decrypted |
|---|---|---|---|---|
| Lena | Red | 0.9806 | −0.0283 | 0.9810 |
| | Blue | 0.9986 | 0.0303 | 0.9375 |
| | Green | 0.9327 | −7.0241e-04 | 0.9283 |
| Baboon | Red | 0.9203 | −0.0202 | 0.9280 |
| | Blue | 0.8583 | −0.0189 | 0.8723 |
| | Green | 0.9709 | −0.0108 | 0.9090 |
| Peppers | Red | 0.9919 | 0.0121 | 0.9916 |
| | Blue | 0.9926 | 0.0016 | 0.9941 |
| | Green | 0.9740 | −0.0305 | 0.9690 |
| Airplane | Red | 0.8806 | −0.0045 | 0.8912 |
| | Blue | 0.8986 | 4.81414e-04 | 0.8753 |
| | Green | 0.8327 | 0.0022 | 0.8293 |
| Sailboat | Red | 0.9321 | 0.0011 | 0.9532 |
| | Blue | 0.9345 | 6.98552e-04 | 0.9723 |
| | Green | 0.9567 | 0.0022 | 0.9761 |
| Splash | Red | 0.9577 | −0.0036 | 0.974 |
| | Blue | 0.9436 | 6.1422e-04 | 0.954 |
| | Green | 0.9634 | 0.0012 | 0.965 |

the same to retrieve the original image. Both the keys are integers of length 32 bits. Hence, the probability of a successful attack is extremely low.

ECC encoded image portrayed in Fig. 8b as a nearly white-distribute image exhibits excellent de-correlation capability to realize good diffusion and confusion as mentioned in [19].

### 5.3 Histogram analysis

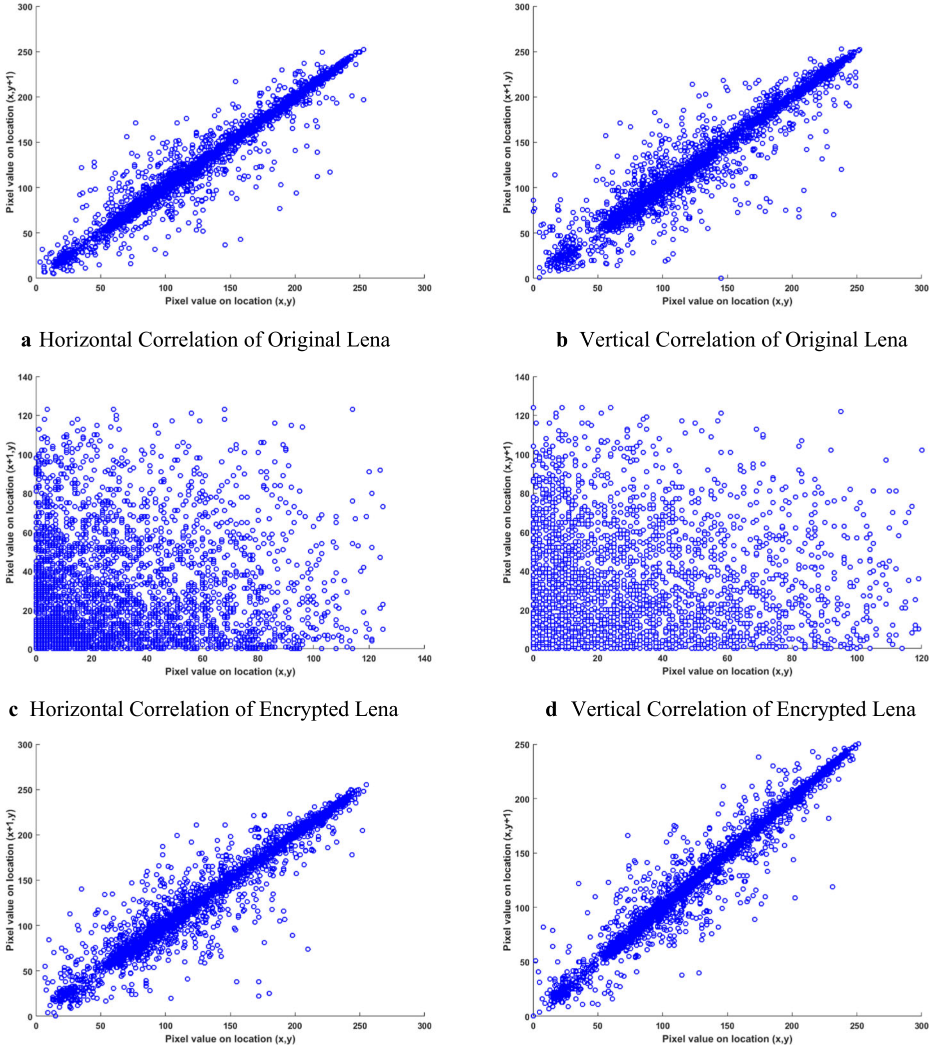
Histogram depicts the visible representation of pixel intensity. Figure 9 shows the histogram analysis Lena Image. The RADIANT system has been identified as a stochastic system as it involves Ephemeral key. Bit wise scrambling has been employed in DNA encoding phase which yields more noise as shown in Fig. 9b. Figure 9b represents Gaussian distribution which can be claimed as better representation for highly noisy image as mentioned in [19] rather than uniform distribution. The RADIANT system diffuses the statistics characteristics of the original image in the entire space. All the RADIANT encrypted bench mark images follow Gaussian distribution. This ensures the confusion property as defined by Shannon theory. This claim ascertains the difficulty of deriving the useful information from the cipher image for crypt analysis. In addition to these aspects, the pixels are further encoded by ECC encoding

**Table 4** MSE (decrypted and original)

| Image | Red | Green | Blue |
|---|---|---|---|
| Lena | 0 | 0 | 0 |
| Baboon | 0 | 0 | 0 |
| Peppers | 0 | 0 | 0 |
| Airplane | 0 | 0 | 0 |
| Sailboat | 0 | 0 | 0 |
| Splash | 0 | 0 | 0 |

**Table 5** MSE (encrypted and original)

| Image | Red | Green | Blue |
|---|---|---|---|
| Lena | 1.3095e + 04 | 6.3518e + 03 | 4.7909e + 03 |
| Baboon | 8.3163e + 03 | 6.8928e + 03 | 7.6403e + 03 |
| Peppers | 1.4145e + 04 | 8.3186e + 03 | 1.1557e + 04 |
| Airplane | 1.2240e + 04 | 1.2979e + 04 | 1.3497e + 04 |
| Sailboat | 6.7088e + 03 | 1.0229e + 04 | 9.6967e + 03 |
| Splash | 1.3652e + 04 | 7.7360e + 03 | 5.9198e + 03 |



**a** Horizontal Correlation of Original Lena

**b** Vertical Correlation of Original Lena

**c** Horizontal Correlation of Encrypted Lena

**d** Vertical Correlation of Encrypted Lena

**e** Horizontal Correlation of Decrypted Lena

**f** Vertical Correlation of Decrypted Lena

**Fig. 10** **a** Horizontal Correlation of Original Lena. **b** Vertical Correlation of Original Lena. **c** Horizontal Correlation of Encrypted Lena. **d** Vertical Correlation of Encrypted Lena. **e** Horizontal Correlation of Decrypted Lena. **f** Vertical Correlation of Decrypted Lena

**Table 6** PSNR (decrypted and original)

| Image | Red | Green | Blue |
|---|---|---|---|
| Lena | Inf | Inf | Inf |
| Baboon | Inf | Inf | Inf |
| Peppers | Inf | Inf | Inf |
| Airplane | Inf | Inf | Inf |
| Sailboat | Inf | Inf | Inf |
| Splash | Inf | Inf | Inf |

that augments the noise level, resulting in exponential distribution shown in Fig. 9c. This enhances the confusion and diffusion to the larger extent making the crypt analysis unrealistic.

### 5.4 Correlation analysis

Correlation analysis is applied by selecting random pixels in the images. Vertically neighboring pixels, horizontally neighboring pixels and diagonally neighboring pixels of scrambled image of Airplane, Sailboat and Splash image are considered for correlation analysis. Tables 3, 4 and 5 and Fig. 10 depicts the results. Correlation coefficient is calculated based on (8)

$$r_{xy} = \frac{Covariance(x, y)}{\sigma_x \sigma_y} \tag{8}$$

Table 3 shows the correlation coefficient of images in the proposed RADIANT system.

### 5.5 MSE and PSNR analysis

Mean Square Error (MSE) and Peak Signal to Noise Ratio is considered for the chosen bench mark images.

$$MSE = \frac{1}{N*M} \sum_{n=1}^{N} \sum_{m=1}^{M} \left[ \lfloor f(i,j) - f_0(i,j) \rfloor^2 \right] \tag{9}$$

Where, f and $f_0$ are the pixel intensity of decrypted and plain images. (i,j) is the coordinate of the pixels. (N*M) is the dimension of the image. Table 4 depicts the MSE of original with decrypted image. It depicts that the MSE of the decrypted image with respect to its original image is 0. Table 5 depicts the MSE of the plain image and encrypted image. It demonstrates that the MSE of the encrypted image with respect to its plain image is high. Logistic mapping,

**Table 7** PSNR(decrypted and original)

| Image | Red | Green | Blue |
|---|---|---|---|
| Lena | 6.9595 | 10.1018 | 11.3266 |
| Baboon | 8.9315 | 9.7468 | 9.2996 |
| Peppers | 6.6245 | 8.9302 | 7.5021 |
| Airplane | 8.3256 | 9.7865 | 10.5252 |
| Sailboat | 7.6575 | 8.9532 | 8.9645 |
| Splash | 8.7854 | 9..9541 | 9.5041 |

**Table 8** Entropy values for the individual color components

| Image | Red Original | Red Encrypted | Green Original | Green Encrypted | Blue Original | Blue Encrypted |
|---|---|---|---|---|---|---|
| Lena | 7.4562 | 7.8763 | 7.7874 | 7.7880 | 7.7891 | 7.6880 |
| Baboon | 7.2343 | 7.9466 | 7.7895 | 6.7871 | 7.6871 | 7.6871 |
| Peppers | 7.9874 | 6.9874 | 7.7880 | 6.7880 | 7.7880 | 7.7880 |
| Airplane | 6.7178 | 7.7882 | 6.7990 | 7.7880 | 6.2138 | 7.7889 |
| Sailboat | 7.3322 | 7.7874 | 7.6364 | 7.7871 | 7.3378 | 7.7866 |
| Splash | 7.1453 | 7.7895 | 7.0036 | 7.7884 | 7.7884 | 7.7856 |

DNA encoding are applied to scramble the image without any loss in the original. The proposed RADIANT system is based on ECC in the final layer. ECC is chosen to yield high level of security with less computing complexity. In the decryption phase, image is recovered without any loss. Hence, it provides an ideal measure of zero for MSE between original and decrypted image.

PSNR is the ratio of the mean square difference two images to the maximum mean square differences that exist between two images. Larger the value of PSNR leads to greater the quality of the image. In the proposed RADIANT system, the PSNR between the original and decrypted is infinity. The algorithm is designed for highly sensitive color image. There is a need to recover the image as it is without any loss. Lossless image recovery is proved by the PSNR values (Tables 6 and 7).

$$PSNR = 20{*}log\frac{255^2}{\sqrt{MSE}}$$

PSNR value is calculated for the decrypted images with respect to its original images. It is infinite. PSNR value is calculated for red, blue and green component separately for lena image, baboon image and pepper image.

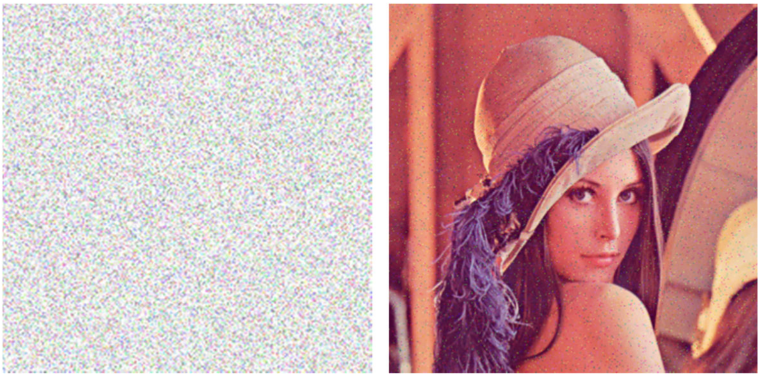
## 5.6 Entropy analysis

Entropy analysis is performed on the images to measure the unpredictability of content. Entropy is the desirable property of the images to verify randomness and it is used to measure the uncertainty of the system. Equation 4 describes the entropy.

$$H(m) = \frac{1}{N}\sum_{i=0}^{2^n-1} p(m_i)log_2\frac{1}{p(m_i)} \tag{10}$$

**Table 9** NPCR and UACI

| Image | NPCR % | UACI % |
|---|---|---|
| Lena | 99.13 | 34.51 |
| Baboon | 99.01 | 33.34 |
| Peppers | 99.76 | 33.62 |
| Airplane | 99.85 | 33.30 |
| Sailboat | 99.60 | 33.50 |
| Splash | 99.61 | 33.53 |



**a** Encrypted Image of Lena **b** Decrypted Noisy Image

**Fig. 11** **a** Encrypted Image of Lena. **b** Decrypted Noisy Image

Where, p(mi) describes the probability of symbol m. Entropy is calculated for each color components separately. Each color component is the 8 bits values ranges from 0 to 255. Ideal entropy value is 8 bit for each color component. Calculated entropy values are listed in the Table 8. All the values are closer to ideal measure.

### 5.7 Sensitivity analysis

Number of pixels change rate (NPCR) and unified average changing intensity (UACI) are performed on the images listed in the Table 9. In each of the bench mark images referred as P1, one of the pixel has been selected at random and modified to get P2. All the images from the set P1 and P2 are encrypted by RADIANT Forward process to get the Cipher images T1 and T2 respectively. In the third phase of the RADIANT Forward process namely ECC Encoding is designed with an Ephemeral Key which is highly significant, as it makes the entire system as stochastic.

The proposed RADIANT system is guaranteed to provide different cipher images for the same pair of plain image and a key at different instances.

$$D(i,j) = \begin{cases} 0, & T_1(i,j) = T_2(i,j) \\ 1, & T_1(i,j) \neq T_2(i,j) \end{cases} \tag{11}$$

$$NPCR = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)}{W*H} *100\% \tag{12}$$

**Table 10** Comparison of MSE of decrypted lena image with proposed algorithm and other authors [17, 30]

| | Proposed Algorithm | Kumar et al. [17] | Mishra et al. [30] |
|---|---|---|---|
| Red | 0 | 1.281 | $8.3014 * 10^{-26}$ |
| Green | 0 | .9456 | $1.0696 * 10^{-25}$ |
| Blue | 0 | 1.2331 | $3.1629 * 10^{-25}$ |

**Table 11** Comparison of PSNR of decrypted lena with proposed algorithm and other authors [17, 30]

| | Proposed Algorithm | Kumar et al. [1] | Mishra et al. [46] |
|---|---|---|---|
| Red | Inf | 47 | 298 |
| Green | Inf | 48 | 297 |
| Blue | Inf | 47 | 303 |

$$UACI = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} T_1(i,j)-T_2(i,j)}{255\ W*H}*100\% \tag{13}$$

where W and H represent the width and the height of the image, respectively. T1 and T2 represent two cipher images. The proposed encryption method has the ability to resist differential attack. In Table 9. It is observed that all NPCR are higher than 95% as well as near to the ideal value 99.61%, most of UACI are near to the ideal value 33.46%.

The strength of the differential attack can be ascertained by means of NPCR and UACI metrics. It is evident from the above results that the non-deterministic nature of the RADIANT system influenced by the inclusion of the Ephemeral key has substantiated higher values. This could be interpreted as the well-accepted measure for validating the resistance of differential attack.

### 5.8 Noise analysis

The proposed algorithm is robust against the transmission noise. This analysis is performed on lena image by applying salt and pepper noise. Figure 11 shows the noise analysis on lena image. The original image is revocable by using the proposed decryption algorithm.

### 5.9 Resistance to known-plaintext

The known-plaintext attack is an attack model for cryptanalysis where the attacker has access to both the plaintext, and its encrypted version. These can be used to reveal further secret information such as secret keys. In the proposed model, image is encrypted based on ECC and Ephemeral key. Ephemeral key is the one time key. It is not possible to derive the key based on the relationship between plain image and cipher image.

**Table 12** Comparison of correlation of encrypted lena image with proposed algorithm and other authors [16, 18, 30, 32, 35, 43]

| | Proposed Algorithm | Mishra et al. [30] | Wang et al. [43] | M. Kumar et al. [18] | Kumar et al. [16] | Zhang et al. [35] | Murillo et al. [32] |
|---|---|---|---|---|---|---|---|
| Red | −.0283 | .0219 | −.010899 | .003535 | .0181 | −.0065 | .0135 |
| Green | .0303 | −.0046 | −.01811 | −0.009706 | −.0067 | .009 | −.0835 |
| Blue | −.00070241 | −.0211 | −.006104 | .018571 | .0154 | −.0008 | −.0170 |

## 6 Comparison with exisitng work

The proposed hybrid multilayered image encryption and decryption algorithm is evaluated with the related work. Table 10 depicts the performance of the proposed RADIANT system with the author's work in [17, 30]. It shows that MSE of decrypted image with respect to the original image is zero. It performs lossless efficient encryption on images.

Table 11 depicts the performance of the proposed RADIANT system with the author's work in [17, 30] based on PSNR. It shows that PSNR of decrypted image with respect to the original image is infinity. It shows that the RADIANT system provides better performance as compared to others.

RADIANT performs the forward process and reverse process based of keyed logistic map and DNA encoding where as [26, 33] performs only grayscale image encryption based on chaotic map and DNA encoding respectively. Table 12 depicts the performance of RADIANT with the authors work in 7, 14, 17, 18, 20 and 24 based on correlation of encrypted image. It depicts that proposed RADIANT is more robust as compared to others work.

## 7 Conclusion

In this work a hybrid multilayered image encryption and decryption algorithm based on ECC and DNA encoding is proposed. Elliptic curve has been selected in such a way that it should be very large so that the proposed algorithm will resist attacks. In the first layer, the image is masked by using logistic map. In the second layer, image is scrambled by applying DNA scrambling. DNA encoding rule is identified cautiously to yield better confidentiality. In the third layer, image is encrypted using elliptic curve cryptography. The proposed RADIANT algorithm provides three level of confidentiality by means of masking, DNA scrambling and ECC encryption. It is evident that RADIANT can claim high level of robustness by obtaining promising results from Key space, Key sensitivity and entropy analysis. The MSE and PSNR values obtained for benchmark color images substantiate the proposed work can be tailor made for high sensitive color image applications. Extensible statistical analysis are performed in the proposed model to prove that RADIANT system is loss-free and hence more expedient for processing medical images, aerospace images and satellite images.

**Acknowledgments** The part of this research work is supported by Department of Science and Technology (DST), Science and Engineering Board (SERB), Government of India under the ECR grant (ECR/2017/000679/ES)

## References

1. Alassaf N, Alkazemi B, and Gutub A (2003) Applicable light-weight cryptography to secure medical data in iot systems. *Arabia*
2. Al-Otaibi Nouf A., and Gutub A A (2014) Flexible stego-system for hiding text in images of personal computers based on user security priority. *Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014)*

3. Bhatnagar G, Jonathan Wu QM, Raman B (2013) Discrete fractional wavelet transform and its application to multiple encryption. Inf Sci 223:297–316
4. Chai X, Yang K, Gan Z (2017) A new chaos-based image encryption algorithm with dynamic key selection mechanisms. Multimedia Tools and Applications 76(7):9907–9927
5. Chen J et al (2018) Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. Signal Process 142:340–353
6. Clelland CT, Risca V, Bancroft C (1999) Hiding messages in DNA microdots. Nature 399(6736):533–534
7. El-Latif AAA, Niu X (2013) A hybrid chaotic system and cyclic elliptic curve for image encryption. AEU-International Journal of Electronics and Communications 67(2):136–143
8. Gehani A, LaBean T, Reif J (2003) DNA-based cryptography. Lect Notes Comput Sci 2950:167–188
9. Gutub A (2007) Efficient utilization of scalable multipliers in parallel to compute GF (p) elliptic curve cryptographic operations. Kuwait Journal of Science & Engineering (KJSE), December 2007 34(2):165–182
10. Gutub AA-A (2010) Preference of efficient architectures for GF (p) elliptic curve crypto operations using multiple parallel multipliers. International Journal of Security (IJS) 4(4):46
11. Gutub AA-A, El-Shafei A-RM, Aabed MA (2011) Implementation of a pipelined modular multiplier architecture for GF (p) elliptic curve cryptography computation. Kuwait J Sci Eng 38(2B):125–153
12. Gutub Adnan Abdul-Aziz, et al. (2013) Serial vs. parallel elliptic curve crypto processor designs. *IADIS International Conference: Applied Computing*
13. Halvorsen K, Wong WP (2012) Binary DNA nanostructures for data encryption. PLoS One 7(9):e44212
14. Head T et al (2000) Computing with DNA by operating on plasmids. Biosystems 57(2):87–93
15. Kumar M, Mishra DC, Sharma RK (2014) A first approach on an RGB image encryption. Opt Lasers Eng 52:27–34
16. Kumar M, Powduri P, Reddy A (2015) An RGB image encryption using diffusion process associated with chaotic map. Journal of Information Security and Applications 21:20–30
17. Kumar M, Powduri P, Reddy A (2015) An diffusion process associated with chaotic map. Journal of Information Security and Applications 21:20–30
18. Kumar M, Iqbal A, Kumar P (2016) A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. Signal Process 125:187–202
19. Lang J (2012) A no-key-exchange secure image sharing scheme based on Shamir's three-pass cryptography protocol and the multiple-parameter fractional Fourier transform. Opt Express 20(3):2386–2398
20. Lang J (2015) Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain. Opt Commun 338:181–192
21. Li L, Abd El-Latif AA, Niu X (2012) Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. Signal Process 92(4):1069–1078
22. Lima JB, Novaes LFG (2014) Image encryption based on the fractional Fourier transform over finite fields. Signal Process 94:521–530
23. Liu S, Sheridan JT (2013) Optical encryption by combining image scrambling techniques in fractional Fourier domains. Opt Commun 287:73–80
24. Liu H, Wang X (2010) Color image encryption based on one-time keys and robust chaotic maps. Computers & Mathematics with Applications 59(10):3320–3327
25. Liu H, Wang X (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 284(16):3895–3903
26. Liu H, Wang X (2012) Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 12(5):1457–1466
27. Liu Zeyu, and Xia T. (2017) Novel two dimensional fractional-order discrete chaotic map and its application to image encryption. *Applied Computing and Informatics*
28. Liu L, Zhang Q, Wei X (2012) A RGB image encryption algorithm based on DNA encoding and chaos map. Computers & Electrical Engineering 38(5):1240–1248
29. Luo Y, Minghui D, Liu J (2015) A symmetrical image encryption scheme in wavelet and time domain. Commun Nonlinear Sci Numer Simul 20(2):447–460
30. Mishra DC et al (2014) Security of color image data designed by public-key cryptosystem associated with 2D-DWT. Fractals 22(04):1450011
31. Mondal B, Mandal T (2017) A light weight secure image encryption scheme based on chaos & DNA computing. Journal of King Saud University-Computer and Information Sciences 29(4):499–504
32. Murillo-Escobar MA et al (2015) A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Process 109:119–131
33. Ning K 2009 A pseudo DNA cryptography method. *arXiv preprint arXiv:0903.2693*
34. Niu Y, Wang X (2011) An anonymous key agreement protocol based on chaotic maps. Commun Nonlinear Sci Numer Simul 16(4):1986–1992

35. Pan SM et al (2017) Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform. Multimedia Tools and Applications 76(2):2933–2295
36. Ponuma R, Amutha R (2017) Compressive sensing based image compression-encryption using novel 1D-chaotic map. Multimedia Tools and Applications:1–26
37. Radhika KR, and Nalini MK (2017) Biometric Image Encryption Using DNA Sequences and Chaotic Systems. *Recent Advances in Electronics and Communication Technology (ICRAECT), International Conference on*. IEEE
38. Shukla A (2015) Image encryption using elliptic curve cryptography. International Journal of Students' Research in Technology & Management 1(2):115–117
39. Singh LD, Singh KM (2015) Image encryption using elliptic curve cryptography. Procedia Computer Science 54:472–481
40. Sui L et al (2014) Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain. Opt Lasers Eng 62:139–152
41. Toughi S, Fathi MH, Sekhavat YA (2017) An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. Signal Process 141:217–227
42. Wang X-Y et al (2010) A chaotic image encryption algorithm based on perceptron model. Nonlinear Dynamics 62(3):615–621
43. Wang X, Lin T, Xue Q (2012) A novel colour image encryption algorithm based on chaos. Signal Process 92(4):1101–1108
44. Wu J, Liao X, Yang B (2017) Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. Signal Process 141:109–124
45. Zhang Y-Q, Wang X-Y (2014) A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf Sci 273:329–351
46. Zhang Q, Wei X (2013) RGB color image encryption method based on Lorenz chaotic system and DNA computation. IETE Tech Rev 30(5):404–409
47. Zhang Y, Xiao D (2013) Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. Opt Lasers Eng 51(4):472–480
48. Zheng X, Xu J, Li W (2009) Parallel DNA arithmetic operation based on n-moduli set. Appl Math Comput 212(1):177–184

**Dr. N. Sasikaladevi** completed doctoral degree in computer science. She authored a book titled “Programming in C#.NET” and “Object Oriented Programming using C#.NET”. She published more than 20 papers in the peer reviewed journals. She has contributed chapter in Springer series. She has completed a research project funded by DST. She received the Woman Scientist Award and Early Research Career Award from Department of Science and Technology, Government of India. She is presently working on cryptography, cloud computing and big data analytics.