IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 10, 2021, accepted March 31, 2021, date of publication April 9, 2021, date of current version June 1, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3072075*

# Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps

**PRIYANSI PARIDA[1], CHITTARANJAN PRADHAN[1], XIAO-ZHI GAO[2], DIPTENDU SINHA ROY[3], (Senior Member, IEEE), AND RABINDRA KUMAR BARIK[4], (Member, IEEE)**

[1]School of Computer Engineering, KIIT University, Bhubaneswar 751024, India
[2]School of Computing, University of Eastern Finland, 70211 Kuopio, Finland
[3]Department of Computer Science and Engineering, NIT Meghalaya, Shillong 793003, India
[4]School of Computer Applications, KIIT University, Bhubaneswar, Odisha 751024, India

Corresponding author: Priyansi Parida (priyansiparida@gmail.com)

**ABSTRACT** Many researchers have used the properties of the popular Elliptic Curve Cryptography(ECC) to devise a stronger and faster image encryption algorithm to assure the secrecy of images during online transmission. In this paper, a robust Elliptic curve based image encryption and authentication model for both grayscale and color images has been proposed. The model uses the secure Elliptic Curve Diffie-Hellman(ECDH) key exchange to compute a shared session key along with the improved ElGamal encoding scheme. 3D and 4D Arnold Cat maps are used to effectively scramble and transform the values of plain image pixels. A well-structured digital signature is used to verify the authenticity of the encrypted image prior to decryption. The model produces good-quality cipher images with an average entropy of 7.9993 for grayscale and 7.99925 for the individual components of color images. The model has high average NPCR of 99.6%, average UACI of 33.3% and low correlation for both grayscale and color images. The model has low computational costs with minimized point multiplication operations. The proposed model is robust with high resilience against statistical, differential, chosen-plaintext(CPA), known-plaintext(KPA) and occlusion attacks.

**INDEX TERMS** Arnold cat map, chaotic map, digital signature, elliptic curve cryptography, image encryption.

## I. INTRODUCTION

Extensive amount of data which consists of a variety of images is transmitted back and forth between users online everyday. Ensuring the availability of correct data to the intended receiver with guaranteed secrecy of data from other users in the network is a challenge. Many image encryption algorithms have been presented for fast and powerful real-time encryption of images. The encryption algorithms include both symmetric and asymmetric encryption algorithms. Symmetric encryption is fast with low computational complexity making it suitable for large data sets. The key distribution and management poses a huge overhead on the symmetric encryption models where each user has his own secret key which needs to be shared before communication. Asymmetric encryption eliminates this issue by using two different keys for encryption and decryption.

Elliptic Curve Cryptography(ECC) is a popular asymmetric encryption algorithm which provides higher level security with smaller key sizes with reduced resource consumption making it an ideal choice for resource-constraint devices. The unpredictability introduced by chaotic maps in encryption algorithms, in addition makes the model easy to implement, swift and strong against the attacker. Logistic map, Henon map, Baker's map, Arnold Cat map, Sine map and Lorenz system are some of the well-known chaotic systems used in encryption algorithms. Chaos based image encryption schemes show higher efficacy than the simple symmetric or asymmetric image encryption schemes without it. The encryption schemes that use a combination of chaotic maps

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed Farouk.

perform better than the ones employing single chaotic map. The use of higher dimensional chaotic maps is known to enhance the security and quality of encryption.

Chen *et al.* [1] proposed a symmetric image encryption algorithm with 3D cat map and logistic map for shuffling of image data with an added layer of confusion between plain-cipher image after every two rounds of shuffling. The encryption also uses Chen's chaotic system for key generation. Pareek *et al.* [2] used the outcome of two logistic maps to randomly opt for one of the eight modes designed to encrypt every pixel in the image. Liu and Wang [3] designed a one-time key stream cipher for color image encryption based on Piecewise Linear chaotic map(PWLCM) to compute the key stream for color image encryption. The generation of key stream depends on another sequence obtained from the Chebyshev map.

Liu *et al.* [4] devised an encryption algorithm with DNA encoding where the XOR and complement operation is carried out using the random sequences generated by the logistic map to encrypt individual components of the color image. However, Liu *et al.* [5] proved that the algorithm can be broken by the known-plaintext attack with only one known pair of plain-cipher images. Luo *et al.* [9] used two chaotic sequences generated by Tent map for the permutation and diffusion of pixels in grayscale images. The initial seed value of Tent map depends on the plain image. Singh and Singh [10] proposed an Elliptic curve(EC) block based image encryption scheme with digital signature for cipher image authentication. The scheme faces the cipher data expansion issue due to additional amount of pixels added during encryption. Singh and Singh [11] presented another refined Elliptic curve based algorithm which uses 2D Arnold Cat map for pixel shuffling and improved ElGamal encryption encoding techniques. The scheme eliminated the data expansion issue.

Xu *et al.* [12] designed a block based image encryption that uses a quantized chaos matrix obtained from the logistic map for creating X coordinate, Y coordinate and swapping control table to swap pixels together with dynamic indexes for diffusion. Saljoughi and Mirvaziri [22] designed an encryption model which uses 3D logistic maps and XOR operation for row-column pixel permutation. Broumandnia [24] presented a color image encryption that uses a 3D Modular Chaotic Map(3DMCM) for pixel shuffling with exclusive OR and circular shift operation for pixel substitution. Kumar and Girdhar [26] used the Lorenz-Rossler chaotic system for pixel diffusion and 2D logistic maps for confusion as well as DNA cryptography for encryption of pixels of color images.

The paper is organized as follows. Section II delves into the theoretical view of our model. In Section III, the proposed EC based image encryption algorithm and the digital signature is described in detail. In section IV, we review the experimental results acquired from the proposed model with the two scrambling methods. In Section V, we analyse the strength of the proposed model against various statistical and intruder attacks. In Section VI, we discuss the performance of the proposed model in comparison to the other schemes prevailing in the field of image encryption. In Section VII, the conclusions follow.

## II. PRELIMINARIES

### A. ELLIPTIC CURVE CRYPTOGRAPHY

The elliptic curve, $E$ in Fig.1 is a non-singular algebraic plane curve defined over a finite field $F_p$ that consists of a set of points satisfying the well known Weierstrass equation of form [27],

$$y^2 \, mod \, p = x^3 + ax + b \, mod \, p \tag{1}$$

where $x, y, a, b \in F_p$, and $4a^3 + 27b^2 \, mod \, p \neq 0$ with a point of infinity, $O$.

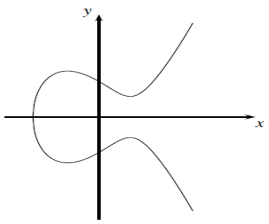


**FIGURE 1.** An Elliptic Curve E defined over a finite field $F_p$.

#### 1) GROUP OPERATIONS ON ELLIPTIC CURVE

We assume $P$ and $Q$ as two unique points on the elliptic curve $E$. The group operations on the curve $E$ are as follows.

- Point addition: The point addition of $P$ and $Q$ is given by

$$P + Q = T \tag{2}$$

  The line that joins the given points $P$ and $Q$ intersects the curve E at the point $(-T)$. The mirror image of the point $(-T)$ with respect to the abscissa is thus obtained to be $T$.
- Point subtraction: The point subtraction of $P$ and $Q$ is given by

$$P - Q = P + (-Q) \tag{3}$$

  where $Q = (x, y)$ then $(-Q) = (x, -y)$.
- Point doubling: The addition of the curve point $P$ to itself results in a point $S$ on the curve E. This is known as point doubling and is given by

$$P + P = 2P = S \tag{4}$$

  The tangent drawn at the point $P$ intersects the curve at $(-S)$. The mirror image of the point,$(-S)$ with respect to $x$-axis is the point $S$.
- Point multiplication: The point multiplication of the point $P$ with a scalar, $m$ is computed by performing $m$ repetitive point additions of $P$ with itself.

$$mP = P + P + P + \ldots + P \, (m \, times) \tag{5}$$

  where $m$ is a scalar, $m \in Z_p$.

#### 2) ELLIPTIC CURVE DIFFIE–HELLMAN (ECDH) KEY EXCHANGE

The ECDH key exchange is used for secure exchange of a shared session key between two users in a network. The key exchange is carried out as follows.

- User A generates its random secret key, $n_A$. A then computes the public key $P_A$ using his private key, $n_A$ and generator point, $G$ on the curve as,

$$P_A = n_A * G \tag{6}$$

  and sends it to user B.
- User B generates its random secret key, $n_B$. B then computes the public key $P_B$ using his private key, $n_B$ and generator point, $G$ on the curve as,

$$P_B = n_B * G \tag{7}$$

  and sends it to user A.
- Both the users A and B compute the shared ECDH key, $Z_{AB}$ as in (8) and (9).
  A computes $Z_{AB}$ as follows.

$$Z_{AB} = n_A * P_B = n_A * n_B * G \tag{8}$$

  B computes $Z_{AB}$ as follows.

$$Z_{AB} = n_B * P_A = n_B * n_A * G \tag{9}$$

### B. ARNOLD'S CAT MAP

Arnold's Cat map [28] is a popular discrete chaotic map that performs scrambling of image pixels by $P$ repetitive shear mapping on the input image to obtain the originally taken image again. The parameter $P$ is defined as the periodicity of the transformation map. The cat map is known for its remarkable mixing properties and high sensitivity to the initial state and control parameters of the map.

#### 1) 2D ARNOLD'S CAT MAP

The two-dimensional Arnold's cat map can be expressed as follows.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} mod\ N \tag{10}$$

where the positive integers, a and b are the control parameters and N is the dimensional value of a $N \times N$ image.

#### 2) EXTENSION TO HIGHER DIMENSIONS

The 2D Arnold's Cat map can be extended to higher dimensional mappings to perform more secure and efficient transforms. The three-dimensional Arnold's mapping is performed with the introduction of two new control parameters, c and d [1]. The general 3D extended form of existing 2D cat map is as follows.

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 1 & a & 0 \\ b & ab+1 & 0 \\ c & d & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} mod\ N \tag{11}$$

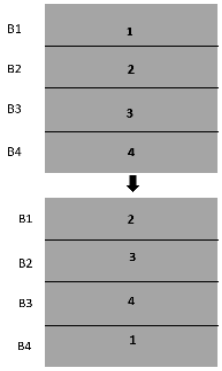


**FIGURE 2.** 4D Horizontal Block Reordering of Grayscale image.

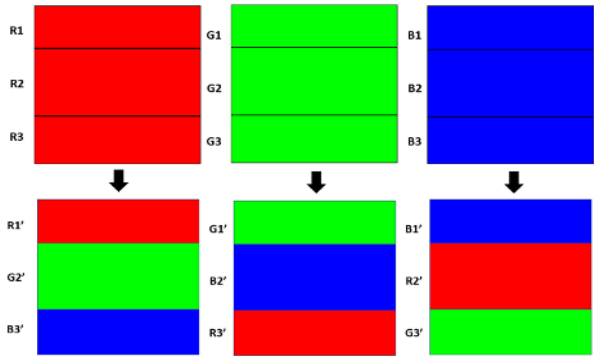


**FIGURE 3.** 4D Horizontal Block Reordering of a RGB image.

Liu *et al.* [29] modified the general form of 3D Arnold's map to carry out pixel position scrambling with subsequent value transform as given in (12).

$$\begin{cases} \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} mod\ N \\ p' = (cx + dy + p)\ mod\ M \end{cases} \tag{12}$$

where p and p' in equation (12) are the pixel values of the initial and remodeled images, and M is maximum pixel intensity. The values of pixel intensity in an image varies from 0 to 255. The modified 3D cat map can also be extended to 4D mapping by reordering the blocks of pixels between the image components. The block reordering can be carried out either vertically [31] or as horizontally [32]. Fig.2 and Fig.3 show the horizontal block reordering for a grayscale image and shuffling among the individual components of a color(RGB) image.

## III. PROPOSED MODEL

The proposed model is divided into three phases viz. ECDH Key Exchange, Encryption/Decryption, and Signing/Verification of encrypted data. The encryption is carried out on blocks of pixels instead of individual pixels to increase efficiency and speed of encryption. The model uses the improved ElGamal encryption encoding [11] for encryption of scrambled pixels. We assume A and B are two users in the network where Sender A wants to transmit data(i.e.images) to

Receiver B in a secure manner. The private and public key pair of Sender,A and Receiver,B are $(n_A, P_A)$ and $(n_B, P_B)$ respectively. A and B compute the ECDH session key, $Z_{AB}$ through their private-public key pairs using equations (8) and (9).

A digital image is characterised by a matrix of smaller image elements called pixels. The number of pixels that can be grouped together is limited by the size of the prime elliptic curve parameter(p). A 512-bit elliptic curve limits the maximum number of pixels in a group to 64.

The scrambling of pixels using Arnold's Cat map can be performed in two ways.

- **Scheme 1**: 3D Cat map transform
- **Scheme 2**: 4D Cat map transform

The proposed design of the image encryption model, as shown in the Fig. 4 and 5, is explained as follows.

### A. ENCRYPTION

1) Record the pixel intensities, dimensional size and channel information from the original image. Adjust the values of pixels by random subtraction or addition of 1 or 2 to each pixels.
2) Choose a random integer k between 2 to $(n-1)$, where n is the cyclic order of the 512-bit elliptic curve.
3) Scrambling of pixels can be carried out in following ways.
   - **Scheme 1: 3D Cat Map Scrambling**
     Shuffle the pixels for j rounds using modified 3D Cat map equation in (12) with control parameters a = 1 and b = 1.

     $$j = kG_x \ mod \ P \tag{13}$$

     where $kG_x$ = x-coordinate of kG and P is the period of the 3D Arnold scrambling for a given image of size N × N.
   - **Scheme 2: 4D Cat Map Scrambling**
     After shuffling the pixels for j rounds using 3D Cat map, perform horizontal block reordering of the scrambled image as described in Fig.2 and Fig.3.
4) Partition the scrambled image pixels into groups of 64 each. Convert each group into a single large integer value with 256 as base.
5) Pair up every successive two integer values to form the plain text input list,$P_M$. Compute cipher text list,$P_C$ as follows.

   $$P_C = P_M + (kG + Z_{AB}) \tag{14}$$

6) Convert cipher text list, $P_C$ to byte values with base 256. Ensure each list has 64 pixel values with required left zeroes padding.
7) Convert the cipher pixel values into the cipher image, $C$.

### B. SIGNING THE ENCRYPTED IMAGE

1) Compute the hash value $h_{xy}$ from $kG$ as follows.

   $$k_{xy} = kG_x \oplus kG_y \tag{15}$$

   $$h_{xy} = SHA_{256}(k_{xy}) \tag{16}$$

2) Perform hash of the encrypted image C as $h_C$ and concatenate $h_C$ with $h_{xy}$ to obtain the combined hash value $H$.

   $$h_C = SHA_{256}(C) \tag{17}$$
   $$H = (h_C \ || \ h_{xy}) \tag{18}$$

3) Compute the parameter, k' as follows.

   $$Z = Z_{AB_x} \oplus Z_{AB_y} \tag{19}$$
   $$k' = Z \oplus k \tag{20}$$

4) Calculate the signature $(R, U)$ as follows.

   $$R = SHA_{256}(H) \tag{21}$$
   $$U = ((k') - R) \ mod \ n \tag{22}$$

5) The encrypted image C is sent to the receiver along with digital signature,$(R, U)$.

### C. VERIFICATION OF ENCRYPTED IMAGE

1) Compute the value of $kG$ from $(R, U)$ and $Z_{AB}$.

   $$Z = Z_{AB_x} \oplus Z_{AB_y} \tag{23}$$
   $$k = ((R + U) \oplus Z) \tag{24}$$
   $$kG = (k * G) \tag{25}$$

2) Calculate the hash value $h_{xy}$ from $kG$.

   $$k_{xy} = kG.x \oplus kG.y \tag{26}$$
   $$h_{xy} = SHA_{256}(k_{xy}) \tag{27}$$

3) Perform hash of the encrypted image C as $h_C$. Combine $h_C$ with $h_{xy}$ to obtain the hash value $H$.

   $$h_C = SHA_{256}(C) \tag{28}$$
   $$H = (h_C \ || \ h_{xy}) \tag{29}$$

4) Calculate $R'$ from computed hash values. If R' is equal to R received digital signature $(R, U)$ from Sender A, then the signature is verified.

   $$R' = SHA_{256}(H) \tag{30}$$
   $$R' == R \tag{31}$$

### D. DECRYPTION

1) Record the pixel intensities, size and related information from the encrypted image,C.
2) Partition the encrypted image pixels into groups of 64 each. Convert each group into a single large integer value with 256 as base.
3) Pair up the integer values as cipher text list,$P_C$ process and compute plain text list, $P_M$ as follows.

   $$P_M = P_C - (kG + Z_{AB}) \tag{32}$$

4) Convert calculated plain text list, $P_M$ back to byte values with base as 256 and ensure each list has 64 values with necessary left zero padding.

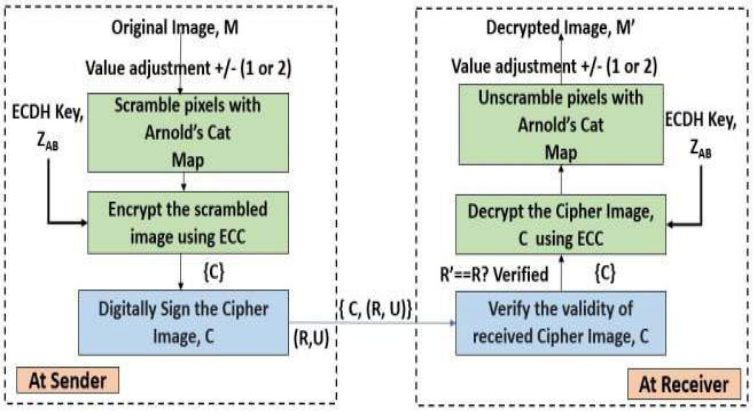


**FIGURE 4.** Overview of the Proposed Model.

5) Unscramble the scrambled pixels in two ways.
   - **Scheme 2:4D Cat map Unscrambling** Reorder the blocks of scrambled image back to generate the 3D scrambled image.
   - **Scheme 1:3D Cat map Unscrambling** Unscramble the scrambled pixel values for P-j rounds to obtain the value adjusted image.
6) Adjust the values of pixels back by random subtraction or addition of 1 or 2 to each pixel to attain the original image again.

## IV. EXPERIMENTAL RESULTS

The proposed model is implemented using Python 3.7 with Spyder 4.1.5 IDE on a HP laptop with system configuration as Intel(R) Core(TM) i5-8250U CPU@1.80GHz with 8GB RAM. The Elliptic curve used in the proposed algorithm is the secure 512-bit curve from ECC Brainpool [33]. The elliptic curve parameters used for implementation are depicted in Table 1.

**TABLE 1.** Elliptic curve parameters used in the implementation of proposed scheme.

| Parameter | Values |
|---|---|
| p | 8948962207650232551656602815159153422162609644098<br>3545113445971872000570104135524399179343041919569<br>4276544653038642734593796389430992392853607053460<br>7816947 |
| a | 6294860557973063227666421306476379324074715770 6<br>2274622713691044545030191428127609802799096840 79<br>8396269115185367856387783422183402743971823806 57<br>25844264138 |
| b | 3245789008328967059274849584342077916531909009 6<br>3750191832832366873617917658326349646352512848 82<br>8261155980077350697377179776481149883499523434 15<br>30862286627 |
| $G_x$ | 6792059140424575174435640431269195087843153390 1<br>0252188146802301273204748257985307754564744627 28<br>6679493637152241077453268658248461794601392887 42<br>96844351522 |
| $G_y$ | 6592244555240112873324748381429610341312712940 3<br>2626633132744506668701054541525646109770748328 86<br>5021699261309018504295771631830118015923478850 43<br>07628509330 |

## V. SECURITY ANALYSIS

Various security and statistical tests are carried out to explore the strength of the proposed algorithm with the two implementations of the algorithm using the explained scrambling methods, Scheme 1 and Scheme 2. The proposed model is tested on grayscale and color(RGB) images sourced from the SIPI Image Database [34]. The analyses carried out include histogram analysis, variance analysis, chi-square test, key space analysis, Shannon's entropy of cipher images, measuring resistance to differential attacks with NPCR(Number of Pixel Change Rate) and UACI(Unified Average Changed Intensity) parameters, similarity measurement (PSNR and SSIM), resistance to intruder attacks, correlation coefficient analysis and computation cost comparison.

### A. HISTOGRAM ANALYSIS

Histogram of an image plots the frequency of pixel intensities in the ordinate against the values of the pixel intensities in the abscissa. An effective encryption algorithm produces a cipher image with even distribution of frequencies across the histogram graph plot. Grayscale images taken in consideration are the Lena, Barbara, and Mandrill. RGB images taken as input images include Lena, House, and Mandrill. Fig. 6 and Fig.7 illustrate the plots for input plain grayscale and RGB images with their cipher images from Scheme 1 and 2 scrambling methods respectively. The cipher images show the uniform frequency distribution of pixels across the histograms indicating good quality of cipher images.

### B. HISTOGRAM VARIANCE ANALYSIS

Variance is a quantitative measure of resistance against statistical attacks by analysing the distribution of pixel frequencies in the histogram of a grayscale image. Variance of a histogram can be computed as follows.

$$VAR(Z) = \frac{1}{P^2} \sum_{i=1}^{P} \sum_{j=1}^{P} \frac{(p_i - p_j)^2}{2} \tag{33}$$

P is the grayscale pixel intensity value and the parameters, $p_i$ and $p_j$ are the number of pixels with intensity value $i$ and $j$.

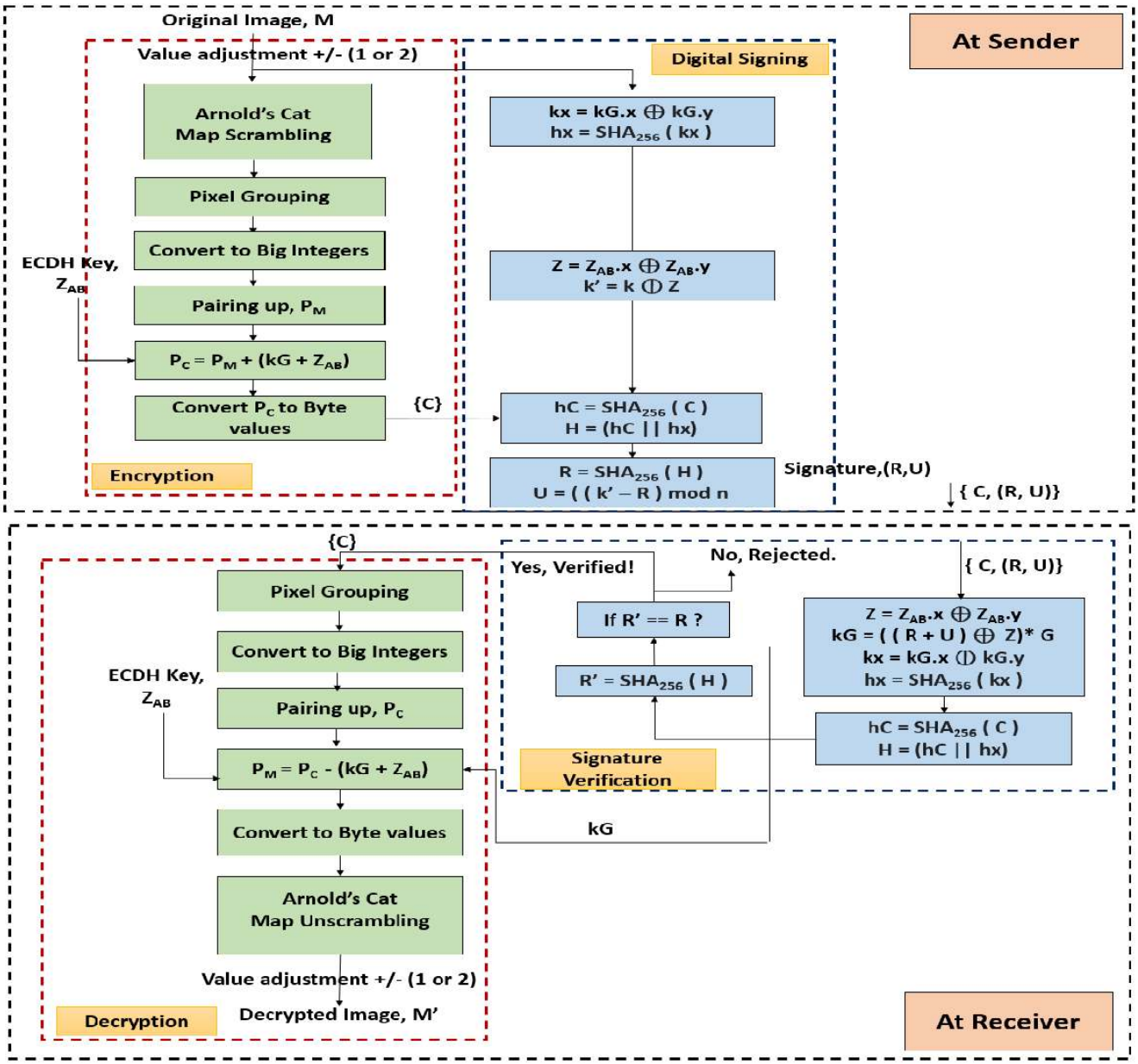


**FIGURE 5.** Proposed design model.

Lower is the computed variance, higher is the uniformity of pixel distribution of the histogram. From Table 2, we infer that the cipher images obtained from the proposed model have lower values of variance indicating high resistance to statistical attacks.

### C. CHI-SQUARE TEST ANALYSIS

Chi-square test measures the uniformity of pixel distribution in the histogram of grayscale images quantitatively. The Chi-square value can be evaluated as follows.

$$\chi^2_{test} = \sum_{i=0}^{255} \frac{(OF_i - EF_i)^2}{EF_i} \tag{34}$$

where the $OF_i$ and $EF_i$ are the observed and expected values of frequency of pixel intensity value $i$.$EF_i$ is

$$EF_i = \frac{M \times N}{I_{max}} \tag{35}$$

$I_{max}$ is the total number of pixel intensities for a grayscale image. Table 3 depicts the calculated values of Chi-square for cipher images obtained from the proposed model with significance level of 1% and 5% at 255 degrees of freedom. The ideal values of Chi-square at 1% and 5% significance level are $\chi^2_{255,0.01} = 310.457$ and $\chi^2_{255,0.05} = 293.2478$. Lower the value of Chi-square, higher is the uniformity of pixel distribution in the histogram. At 1% and 5%

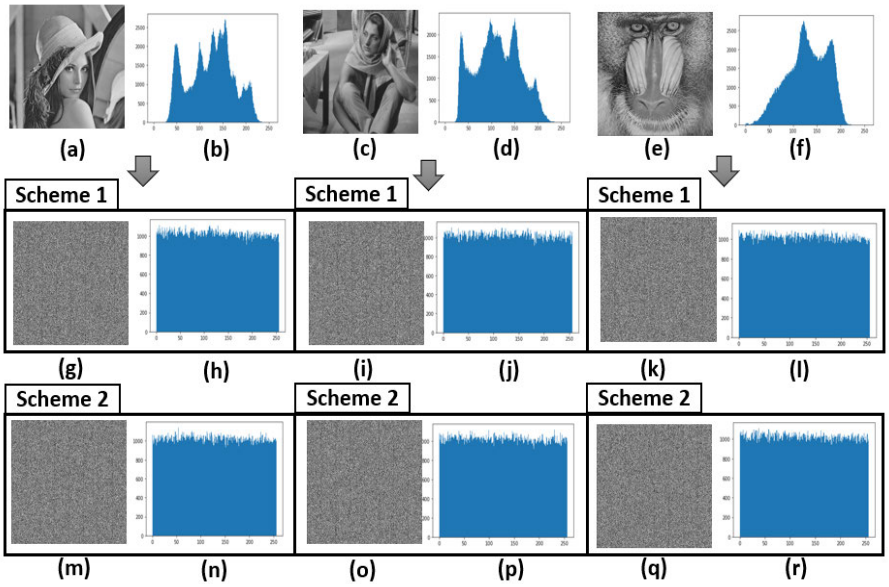


**FIGURE 6.** (a-f):Plain grayscale images with their histograms, (g-l):Cipher images with **Scheme 1** scrambling with their histograms, (m-r):cipher images with **Scheme 2** scrambling with respective histogram.

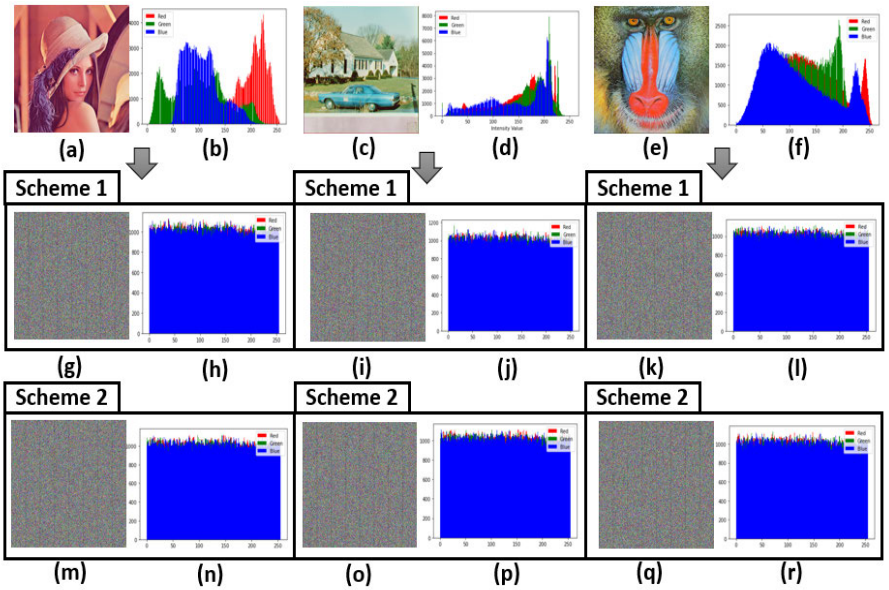


**FIGURE 7.** (a-f):Plain RGB images with their histograms, (g-l):Cipher images with **Scheme 1** scrambling with their histograms, (m-r):Cipher images with **Scheme 2** scrambling with respective histogram.

significance levels, the cipher images obtained from Scheme 1 and 2 show Chi-square values lower than the ideal values. The calculated Chi-square values satisfy the hypothesis and implies grayscale pixel uniformity in the cipher images derived from the proposed model.

### *D. KEY SPACE*

The robustness of an algorithm depends upon the key size of the cryptosystem. The proposed algorithm relies on the inability of solving the exponentially difficult Elliptic Curve Discrete Logarithm Problem(ECDLP), in feasible amount of time, to provide higher level of security with shorter key sizes. The implementation of the proposed model uses the ECC Brainpool [33] standard 512-bit Elliptic curve which can successfully withstand brute-force attacks.

### *E. SHANNON'S ENTROPY ANALYSIS*

The Shannon's theory [35] states that entropy is directly proportional to the degree of uncertainty present in the data. An encryption algorithm should ideally produce a cipher

**TABLE 2.** Variance of various grayscale images.

| Scheme | Image | Variance | |
|---|---|---|---|
| | | Plain | Cipher |
| Scheme 1 | Lena | 632097.48 | 958.04 |
| | Barbara | 576404.48 | 991.95 |
| | Mandrill | 750395.63 | 1026.14 |
| | Peppers | 555344.7 | 1003.05 |
| Scheme 2 | Lena | 632097.48 | 876.32 |
| | Barbara | 576404.48 | 977.73 |
| | Mandrill | 750395.63 | 942.47 |
| | Peppers | 555344.7 | 934.98 |
| Ref. [23] | Lena | 634734 | 980.8 |
| | Barbara | 433040 | 1013.2 |
| | Mandrill | 627520 | 1008.3 |
| | Peppers | 448850 | 950.9 |

**TABLE 3.** Chi-square analysis of proposed model.

| Scheme | Images | $\chi^2_{test}$ | Results |
|---|---|---|---|
| Scheme 1 | Lena | 275.89 | *Pass* |
| | Barbara | 263.87 | *Pass* |
| | Mandrill | 286.44 | *Pass* |
| | Peppers | 282.01 | *Pass* |
| Scheme 2 | Lena | 251.52 | *Pass* |
| | Barbara | 247.37 | *Pass* |
| | Mandrill | 266.72 | *Pass* |
| | Peppers | 241.97 | *Pass* |

image with entropy value of 8. The entropy values are computed for the cipher images obtained from both implementations of the model in Table 4 and 5. The cipher images of the tested grayscale as well as color images display better entropy values than existing image encryption schemes.

### F. RESISTANCE TO DIFFERENTIAL ATTACKS

Differential attacks are a form of cryptanalysis to find the secret key by tracing the differences in the cipher data due to minimal changes in the plain data. The Number of Changing Pixel Rate(NPCR) and Unified Average Changed Intensity(UACI) values, computed from the cipher images acquired from a pair of nearly similar plain images, are used to measure the resilience of the algorithm against such attacks. The ideal value of NPCR for an encryption is 100% with UACI value being around 33%. From Table 6 and 7, it can be ascertained that the cipher images derived from the scheme approximate near-ideal values for the NPCR and UACI parameters.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{T} \times 100\% \tag{36}$$

$$UACI = \frac{\sum_{i,j} |C(i,j) - C'(i,j)|}{I_{max} \times T} \times 100\% \tag{37}$$

where

$$D(i,j) = \begin{cases} 0 & if\ C(i,j) = C'(i,j) \\ 1 & if\ C(i,j) \neq C'(i,j) \end{cases} \tag{38}$$

T = Total number of pixels, C and C' are the two cipher images, and $I_{max}$ = Total number of Pixel Intensities.

### G. SIMILARITY MEASUREMENT

The Peak Signal-to-Noise ratio(PSNR) and Structural Similarity(SSIM) index values measure the similarity between the plain and cipher images. The PSNR value edges nearer to infinity as Mean Squared Error(MSE) approaches zero. SSIM index estimates the perceived quality of images from its structural information. Lower the PSNR and SSIM values are between plain and cipher data, better is the quality of encryption. The measured values of PSNR and SSIM for the proposed schemes are given in Table 8. The SSIM values of cipher images from the tested grayscale and RGB images approach zero with reduced values of PSNR indicating good quality of encryption. The Scheme 2 has lower similarity between original and cipher images than Scheme 1 making it a better mode of encryption.

$$PSNR = 20 \times log_{10} \frac{P_{max}}{\sqrt{MSE}} \tag{39}$$

where $P_{max}$ is the maximum pixel intensity.

### H. KNOWN-PLAINTEXT ATTACK(KPA) AND CHOSEN-PLAINTEXT ATTACK(CPA)

Known-Plaintext and Chosen-Plaintext attacks are two attack models for cryptanalysis where intruder can exploit the knowledge of one or more plaintext-ciphertext pairs from an encryption method to reveal secret information. In case of Known-Plaintext attacks, we assume the intruder has access to one or more plain images and their corresponding cipher images. The proposed algorithm generates different and unique cipher images for the same plain image due to use of the random parameter k, value adjustment, and efficient scrambling methods in each session of encryption.

In Chosen-Plaintext attacks, the intruder can choose certain plaintext images and use the respective cipher images to unveil the secret key. We assume the intruder chooses two special images i.e. all black and all white images as the plain images for the CPA attack. From Fig. 8 and Tables 9 and 10, we infer that the proposed method produces good quality cipher images for the special input images with low correlation, uniform cipher pixel distribution and high entropy

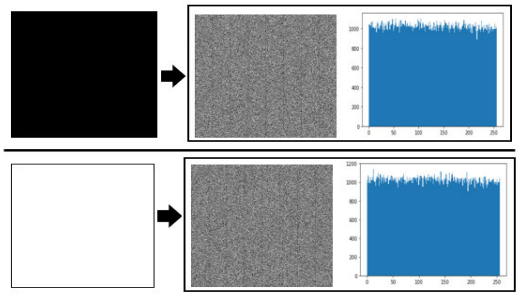

**FIGURE 8.** Plain All Black and All White images with their respective encrypted images obtained from the proposed encryption model, and the histograms of the encrypted images.

**TABLE 4.** Shannon's entropy analysis for grayscale images.

| Image | Entropy Value | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Scheme 1 | Scheme 2 | Ref. [23] | Ref. [9] | Ref. [14] | Ref. [19] | Ref. [18] | Ref. [20] |
| Lena | 7.9993 | 7.9993 | 7.9993 | 7.9993 | 7.9991 | 7.9992 | 7.9992 | 7.9991 |
| Barbara | 7.9993 | 7.9993 | 7.9993 | - | - | - | - | - |
| Peppers | 7.9993 | 7.9994 | 7.9994 | 7.9992 | - | - | - | - |
| Mandrill | 7.9993 | 7.9993 | 7.9993 | 7.9992 | - | - | - | - |

**TABLE 5.** Shannon's entropy analysis for RGB images.

| Image | Component | Entropy Value | | | | | |
|---|---|---|---|---|---|---|---|
| | | Scheme 1 | Scheme 2 | Ref. [39] | Ref. [40] | Ref. [41] | Ref. [51] |
| Lena | Red | 7.9992 | 7.9993 | 7.9992 | 7.9972 | 7.9993 | 7.9966 |
| | Green | 7.9992 | 7.9992 | 7.9993 | 7.9973 | 7.9993 | 7.9972 |
| | Blue | 7.9992 | 7.9993 | 7.9992 | 7.9972 | 7.9993 | 7.9967 |
| Mandrill | Red | 7.9993 | 7.9992 | 7.9991 | 7.9972 | 7.9923 | - |
| | Green | 7.9992 | 7.9992 | 7.9991 | 7.9972 | 7.9803 | - |
| | Blue | 7.9992 | 7.9992 | 7.9993 | 7.9972 | 7.9986 | - |
| Peppers | Red | 7.9992 | 7.9993 | 7.9989 | 7.9971 | 7.9962 | 7.9910 |
| | Green | 7.9992 | 7.9993 | 7.9991 | 7.9975 | 7.9929 | 7.9918 |
| | Blue | 7.9993 | 7.9993 | 7.9989 | 7.9974 | 7.9925 | 7.9905 |

**TABLE 6.** NPCR and UACI analysis for grayscale tested images.

| Type | Grayscale | Scheme 1 | Scheme 2 | Ref. [7] | Ref. [14] | Ref. [23] | Ref. [38] |
|---|---|---|---|---|---|---|---|
| NPCR (%) | Lena | 99.61 | 99.632 | 99.60 | 99.61 | 99.6113 | 99.59 |
| | Barbara | 99.63 | 99.62 | - | - | 99.5796 | - |
| | Peppers | 99.62 | 99.63 | | - | 99.6109 | - |
| | Mandrill | 99.62 | 99.61 | - | - | 99.6112 | - |
| UACI (%) | Lena | 33.34 | 33.34 | 33.44 | 33.32 | 33.4682 | 33.41 |
| | Barbara | 33.35 | 33.34 | - | - | 33.4296 | - |
| | Peppers | 33.31 | 33.33 | - | - | 33.4836 | - |
| | Mandrill | 33.34 | 33.34 | - | - | 33.4919 | - |

**TABLE 7.** Average values for NPCR and UACI analysis for RGB tested images.

| Type | RGB | | Scheme 1 | Scheme 2 | Ref. [49] | Ref. [50] | Ref. [51] |
|---|---|---|---|---|---|---|---|
| Average NPCR (%) | Lena | Red | 99.6200 | 99.6223 | 99.6052 | 99.6100 | 99.6001 |
| | | Green | 99.6105 | 99.6125 | 99.6060 | 99.6100 | 99.5998 |
| | | Blue | 99.6097 | 99.6185 | 99.6113 | 99.6100 | 99.5997 |
| | Mandrill | Red | 99.5937 | 99.6243 | 99.6024 | 99.6200 | 99.6099 |
| | | Green | 99.6223 | 99.6132 | 99.6252 | 99.6200 | 99.6058 |
| | | Blue | 99.6105 | 99.6059 | 99.6004 | 99.6200 | 99.5956 |
| | Peppers | Red | 99.6269 | 99.6093 | 99.6060 | 99.6100 | - |
| | | Green | 99.6028 | 99.6292 | 99.6286 | 99.6100 | - |
| | | Blue | 99.6013 | 99.6128 | 99.5874 | 99.6100 | - |
| Average UACI (%) | Lena | Red | 33.2830 | 33.3438 | 33.4280 | 32.2300 | 33.3575 |
| | | Green | 33.3327 | 33.2787 | 33.4966 | 33.9600 | 33.4287 |
| | | Blue | 33.3277 | 33.3651 | 33.3779 | 34.3500 | 33.3683 |
| | Mandrill | Red | 33.3216 | 33.3588 | 33.4311 | 33.4600 | 33.3743 |
| | | Green | 33.3115 | 33.3359 | 33.4500 | 32.2200 | 33.3829 |
| | | Blue | 33.2757 | 33.3345 | 33.4935 | 34.2300 | 33.5604 |
| | Peppers | Red | 33.3182 | 33.3151 | 33.4959 | 31.0300 | - |
| | | Green | 33.3691 | 33.3561 | 33.4874 | 34.0000 | - |
| | | Blue | 33.3692 | 33.3614 | 33.4302 | 34.7800 | - |

making it difficult for the intruder to elicit secret information from the plain-cipher image pairs.

### I. OCCLUSION ATTACK ANALYSIS

The encrypted images can suffer from data loss due to varying reasons while transmitting data between sender and receiver. The ability to recognise the original images from the distorted images signifies the strength of the proposed model against such occlusion attacks. Figures 9 and 10 depict the decrypted grayscale and color images acquired from the distorted cipher images through Scheme 1 and 2. The decrypted images show that the proposed model can resist the occlusion attacks successfully.

### J. CORRELATION COEFFICIENT ANALYSIS

Correlation coefficient is a statistical measure of strength of relationship between the original and encrypted image.

**TABLE 8.** Similarity analysis between two proposed schemes.

| Image Type | Image | PSNR | | SSIM | |
|---|---|---|---|---|---|
| | | Scheme 1 | Scheme 2 | Scheme 1 | Scheme 2 |
| Grayscale | Lena | 27.897 | 27.894 | 0.0097 | 0.0091 |
| | Barbara | 27.895 | 27.894 | 0.0094 | 0.0087 |
| | Mandrill | 27.902 | 27.898 | 0.0092 | 0.0078 |
| | Peppers | 27.903 | 27.898 | 0.0086 | 0.0084 |
| RGB | Lena | 27.899 | 27.895 | 0.0099 | 0.0098 |
| | Mandrill | 27.896 | 27.894 | 0.0097 | 0.0087 |
| | Peppers | 27.9 | 27.896 | 0.0086 | 0.0084 |

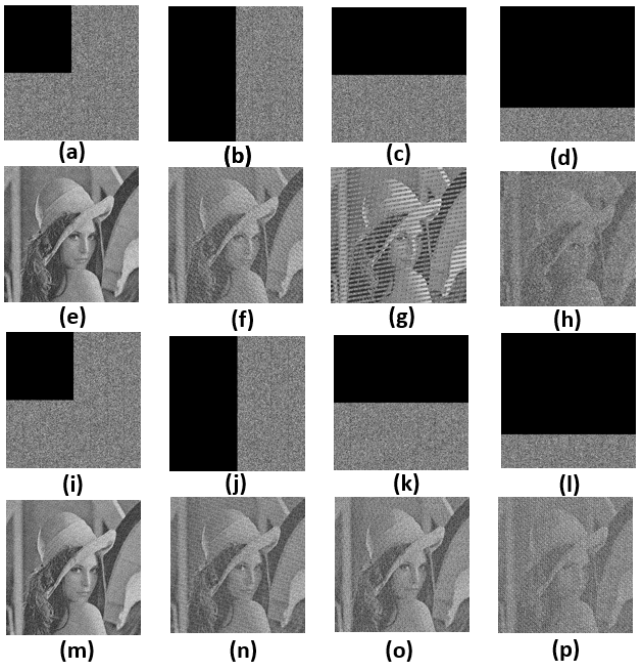


**FIGURE 9.** Decrypted grayscale images from Scheme 1 and 2 under Occlusion attack analysis. (a-d) are cipher images from Scheme 1 having 25%, 50% vertical, 50% horizontal and 75% data loss. (e-h) are the corresponding decrypted images for Scheme 1 Occlusion analysis.(i-l) are cipher images from Scheme 2 having 25%, 50% vertical, 50% horizontal and 75% data loss. (m-hp) are the corresponding decrypted images for Scheme 2 Occlusion analysis.

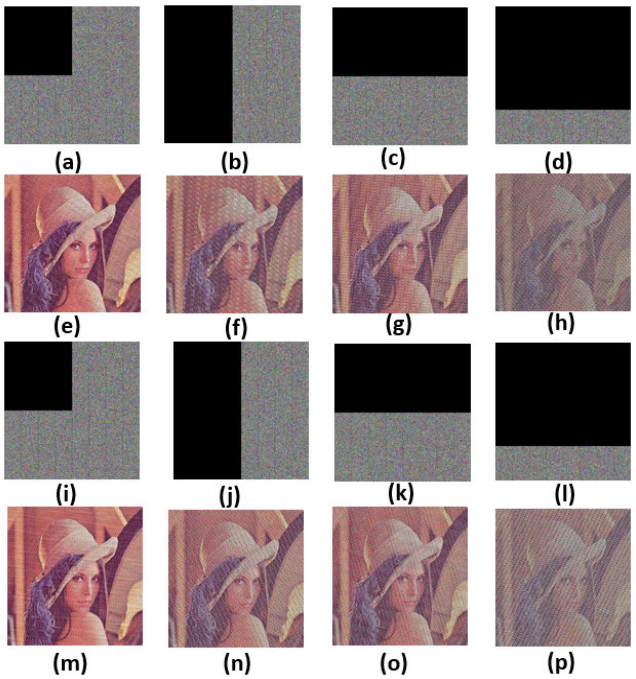


**FIGURE 10.** Decrypted color images from Scheme 1 and 2 under Occlusion attack analysis. (a-d) are cipher images from Scheme 1 having 25%, 50% vertical, 50% horizontal and 75% data loss. (e-h) are the corresponding decrypted images for Scheme 1 Occlusion analysis.(i-l) are cipher images from Scheme 2 having 25%, 50% vertical, 50% horizontal and 75% data loss. (m-hp) are the corresponding decrypted images for Scheme 2 Occlusion analysis.

**TABLE 9.** Histogram uniformity analysis for special input images.

| Image | Proposed | | Variance | $\chi^2_{test}$ | Results |
|---|---|---|---|---|---|
| All black | Scheme 1 | Plain | 267386880 | - | *Pass* |
| | | Cipher | 1000.22 | 286.54 | |
| All white | Scheme 1 | Plain | 267386880 | - | *Pass* |
| | | Cipher | 1007.16 | 260.99 | |
| All black | Scheme 2 | Plain | 267386880 | - | *Pass* |
| | | Cipher | 999.35 | 260.89 | |
| All white | Scheme 2 | Plain | 267386880 | - | *Pass* |
| | | Cipher | 883.95 | 254.62 | |

A plain image has high correlation between the adjoining pixels. The correlation graph for the plain image as a consequence is dense. A strong and desirable cipher image should have an evenly distributed graph with low correlation values between the adjoining pixels. We compute correlation coefficient between the plain and cipher images horizontally, vertically and diagonally. The correlations graph plots for the grayscale Lena image and its cipher image from the proposed model are illustrated in Fig. 11. Fig. 12 shows the correlation graph plots for the component blue of color Lena image and its cipher image. Table 11 and 12 display the comparison of correlation coefficient values obtained from Scheme 1 and Scheme 2 implementation of the tested grayscale and RGB images with those from recent image encryption algorithms. The correlation coefficient values for tested grayscale and RGB images are closer to zero in comparison to the existing encryption models.

### K. COMPUTATIONAL COST COMPARISON

A robust image encryption algorithm should perform encryption on images with minimal consumption of computing resources. The time consumption of an EC based encryption

**TABLE 10.** Performance of proposed model on special input images.

| Image | Proposed | | Entropy | Correlation Coefficient | | |
|---|---|---|---|---|---|---|
| | | | | Horizontal | Vertical | Diagonal |
| All black | Scheme 1 | Plain | 0 | - | - | - |
| | | Cipher | 7.9992 | 0.00171 | 0.00717 | -0.00133 |
| All white | Scheme 1 | Plain | 0 | - | - | - |
| | | Cipher | 7.9993 | 0.00159 | 0.0043 | 0.00082 |
| All black | Scheme 2 | Plain | 0 | - | - | - |
| | | Cipher | 7.99928 | -0.0023 | 0.0069 | -0.0025 |
| All white | Scheme 2 | Plain | 0 | - | - | - |
| | | Cipher | 7.99933 | 0.0035 | 0.00046 | 0.00057 |

**TABLE 11.** Comparison of correlation coefficient values for grayscale images.

| Algorithm | Image | Horizontal | | Vertical | | Diagonal | |
|---|---|---|---|---|---|---|---|
| | | Plain | Cipher | Plain | Cipher | Plain | Cipher |
| Scheme 1 | Barbara | 0.85973 | -0.0016 | 0.95908 | 0.0031 | 0.84181 | -0.0012 |
| | Lena | 0.97189 | 0.0019 | 0.98498 | 0.0017 | 0.95928 | 0.0011 |
| | Mandrill | 0.86652 | -0.00077 | 0.75864 | 0.0019 | 0.72613 | 0.00068 |
| | Peppers | 0.97918 | 0.0011 | 0.98264 | 0.0047 | 0.96797 | -0.00024 |
| Scheme 2 | Barbara | 0.85973 | -0.0015 | 0.95908 | 0.0016 | 0.84181 | 0.00073 |
| | Lena | 0.97189 | 0.0012 | 0.98498 | 0.0016 | 0.95928 | -0.0007 |
| | Mandrill | 0.86652 | -0.0002 | 0.75864 | 0.0036 | 0.72613 | 0.0002 |
| | Peppers | 0.97918 | -0.0012 | 0.98264 | 0.0024 | 0.96797 | 0.00021 |
| Ref. [12] | Lena | 0.9503 | -0.0226 | 0.9775 | 0.0041 | 0.9275 | 0.0368 |
| Ref. [18] | Lena | 0.9325 | 0.0074 | 0.9139 | -0.0094 | 0.9469 | -0.0054 |
| Ref. [23] | Barbara | 0.9689 | 0.0024 | 0.8956 | 0.0031 | 0.8536 | -0.0013 |
| | Lena | 0.9858 | 0.0019 | 0.9801 | -0.0024 | 0.9669 | -0.0011 |
| | Mandrill | 0.7251 | 0.0024 | 0.8558 | 0.0011 | 0.6920 | -0.0008 |
| | Peppers | 0.9807 | -0.0028 | 0.9752 | 0.0039 | 0.9636 | -0.00024 |
| Ref. [36] | Lena | 0.9771 | 0.0925 | 0.9631 | 0.0430 | 0.9469 | -0.0054 |
| Ref. [37] | Peppers | 0.9295 | 0.0048 | 0.9294 | 0.0062 | 0.8771 | 0.0030 |
| Ref. [38] | Mandrill | 0.7508 | -0.0061 | 0.8562 | 0.0130 | 0.7153 | 0.0017 |

algorithm is determined by the number of time intensive point multiplications it has. Lesser the number of point multiplications, faster is the image encryption algorithm. In Table 13,we carried out a comparative analysis of time consumption among recent EC based image encryption algorithms. The proposed model has lower computational costs with lesser number of point multiplications.

## VI. DISCUSSION

The performance of the proposed model is tested on two implementations of model, Scheme 1 using 3D Arnold Cat map and Scheme 2 using the 4D Arnold Cat map. The extended Arnold Cat maps add additional layers of value substitution after the numerous rounds of pixel scrambling which increases the security as well as quality of encryption. The model generates better-quality cipher images as evident from the uniform pixel frequency distribution in histogram analysis as can be seen in the Fig. 6 and Fig.7. The cipher images obtained are unique and distinct with high entropy, low PSNR and SSIM values and reduced correlation coefficient values between neighbouring pixels. The model has high resistance to differential attacks with an average NPCR of 99.62% and UACI of 33.3%. From the performance comparisons between the proposed model and existing encryption schemes in Tables 4–13, we infer that the proposed scheme has higher efficacy with stronger resistance against the security and statistical attacks.

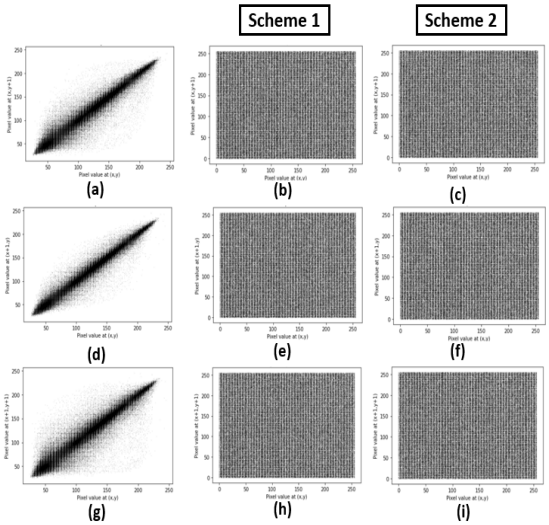


**FIGURE 11.** Correlation graphs of plain and cipher grayscale LENA images from their respective proposed Scheme 1 and Scheme 2 implementations. Here, (a - c) are horizontal correlation graphs, (c - e) are vertical correlation graphs and (f-i) are diagonal correlation graphs.

Scheme 2(4D Arnold Cat Map) performs better than Scheme 1(3D Arnold Cat Map) scrambling in comparison. The proposed algorithm is time-efficient with fewer time-consuming EC point multiplications. A lightweight digital signature algorithm using the secure SHA-256 hash

**TABLE 12.** Comparison of correlation coefficient values for RGB images.

| Scheme | Image | Type | Horizontal | | Vertical | | Diagonal | |
|---|---|---|---|---|---|---|---|---|
| | | | Plain | Cipher | Plain | Cipher | Plain | Cipher |
| Scheme 1 | Mandrill | Red | 0.92306 | 0.00046 | 0.86596 | 0.006 | 0.85434 | -0.0002 |
| | | Green | 0.86548 | 0.00037 | 0.76501 | 0.0079 | 0.73479 | -0.002 |
| | | Blue | 0.90734 | -0.00026 | 0.88089 | 0.0048 | 0.83986 | -0.0001 |
| | Lena | Red | 0.97977 | -0.00086 | 0.98932 | 0.0062 | 0.969694 | 0.0036 |
| | | Green | 0.96907 | -0.00065 | 0.98249 | 0.0053 | 0.955546 | -0.0024 |
| | | Blue | 0.93274 | -0.00154 | 0.957604 | 0.0029 | 0.918286 | -0.0009 |
| | House | Red | 0.95355 | 0.0016 | 0.95788 | 0.0077 | 0.92243 | 0.0035 |
| | | Green | 0.93909 | 0.00039 | 0.942326 | 0.0064 | 0.890085 | -0.0016 |
| | | Blue | 0.97248 | 0.0041 | 0.968604 | 0.0058 | 0.944495 | 0.0032 |
| Scheme 2 | Mandrill | Red | 0.92306 | 0.00023 | 0.86596 | 0.0027 | 0.85434 | 0.00008 |
| | | Green | 0.86548 | 0.0034 | 0.76501 | 0.00037 | 0.73479 | 0.00027 |
| | | Blue | 0.90734 | 0.0008 | 0.88089 | 0.0018 | 0.83986 | 0.0012 |
| | Lena | Red | 0.97977 | -0.0007 | 0.98932 | 0.0035 | 0.969694 | -0.00009 |
| | | Green | 0.96907 | -0.0015 | 0.98249 | 0.0047 | 0.955546 | 0.0017 |
| | | Blue | 0.93274 | -0.0009 | 0.957604 | 0.0068 | 0.918286 | 0.00103 |
| | House | Red | 0.95355 | -0.002 | 0.95788 | 0.0041 | 0.92243 | -0.0017 |
| | | Green | 0.93909 | -0.0016 | 0.942326 | 0.0008 | 0.890085 | 0.0008 |
| | | Blue | 0.97248 | 0.0012 | 0.968604 | 0.0019 | 0.944495 | 0.0031 |
| Ref. [10] | House | Red | 0.9467 | -0.0067 | 0.9310 | 0.0004 | 0.8987 | 0.0147 |
| | | Green | 0.9203 | 0.0177 | 0.9120 | 0.0175 | 0.8502 | -0.0025 |
| | | Blue | 0.9686 | -0.0153 | 0.9526 | -0.0001 | 0.9271 | -0.0207 |
| Ref. [42] | Mandrill | Red | 0.9280 | 0.0186 | 0.8650 | -0.006 | 0.8538 | -0.0013 |
| | | Green | 0.8625 | 0.0066 | 0.7697 | 0.0164 | 0.7256 | 0.0092 |
| | | Blue | 0.9087 | 0.0067 | 0.8859 | 0.0012 | 0.8427 | 0.0172 |
| | Lena | Red | 0.9326 | 0.0035 | 0.9624 | -0.004 | 0.907 | -0.0410 |
| | | Green | 0.9222 | -0.0097 | 0.9546 | 0.0053 | 0.8804 | -0.0085 |
| | | Blue | 0.8938 | 0.0185 | 0.9343 | 0.0106 | 0.8634 | -0.017 |

**TABLE 13.** Computational cost comparison analysis.

| Scheme | Number of Point Multiplications required | | | | |
|---|---|---|---|---|---|
| | Encryption | Decryption | Signature | Verification | Total |
| Proposed | 1 | 0 | 0 | 1 | 2 |
| Ref. [10] | 2 | 1 | 1 | 2 | 6 |
| Ref. [23] | 2 | 1 | × | × | 3 |
| Ref. [25] | 1 | 1 | 0 | 1 | 3 |

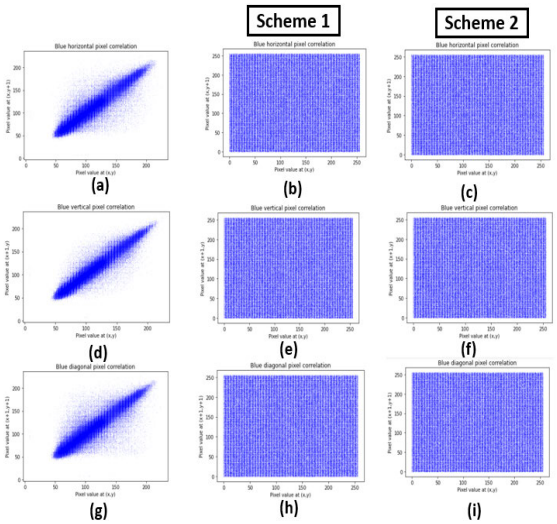


**FIGURE 12.** Correlation graphs of Blue component of plain and cipher color LENA images from their respective proposed Scheme 1 and Scheme 2 implementations. Here, (a - c) are horizontal correlation graphs, (c - e) are vertical correlation graphs and (f-i) are diagonal correlation graphs.

function is used to verify the validity of cipher image before decryption for faster decryption of correct cipher images.

## VII. CONCLUSION

The proposed image encryption and authentication model intends to enhance the quality of encryption of both grayscale and color images through the discretized chaotic 3D and 4D Arnold Cat maps. The model strengthens the quality of cipher images compared to existing schemes with higher entropy, lower correlation, higher average NPCR and UACI, lower PSNR and SSIM values along with the ability to actively thwart the Chosen-Plaintext(CPA) and Known-Plaintext attacks(KPA). The proposed model is proven to be robust, lightweight and competent against the statistical and cryptanalytic attacks. In future work, the encryption model can be amended to support other forms of real-time multimedia encryption such as audio, video and more.

## REFERENCES

[1] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004.

[2] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, Sep. 2006.

[3] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. with Appl.*, vol. 59, no. 10, pp. 3320–3327, May 2010.

[4] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Comput. Electr. Eng.*, vol. 38, no. 5, pp. 1240–1248, Sep. 2012.
[5] Y. Liu, J. Tang, and T. Xie, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map," *Opt. Laser Technol.*, vol. 60, pp. 111–115, Aug. 2014.
[6] I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, "A novel image cipher based on mixed transformed logistic maps," *Multimedia Tools Appl.*, vol. 56, no. 2, pp. 315–330, Jan. 2012.
[7] G. Ye, "A block image encryption algorithm based on wave transmission and chaotic systems," *Nonlinear Dyn.*, vol. 75, no. 3, pp. 417–427, Feb. 2014.
[8] A. S. Rajput and M. Sharma, "A novel image encryption and authentication scheme using chaotic maps," in *Advances in Intelligent Informatics*. Cham, Switzerland: Springer, 2015, pp. 277–286.
[9] Y. Luo, L. Cao, S. Qiu, H. Lin, J. Harkin, and J. Liu, "A chaotic map-control-based and the plain image-related cryptosystem," *Nonlinear Dyn.*, vol. 83, no. 4, pp. 2293–2310, Mar. 2016.
[10] L. D. Singh and K. M. Singh, "Image encryption using elliptic curve cryptography," *Procedia Comput. Sci.*, vol. 54, pp. 472–481, 2015.
[11] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017.
[12] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Opt. Lasers Eng.*, vol. 91, pp. 41–52, Apr. 2017.
[13] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Process.*, vol. 141, pp. 109–124, Dec. 2017.
[14] S. Sun, "Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules," *Opt. Eng.*, vol. 56, no. 11, 2017, Art. no. 116117.
[15] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.
[16] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 60, pp. 12–32, Jul. 2018.
[17] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.
[18] Z. Liu, T. Xia, and J. Wang, "Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes–Vanstone elliptic curve cryptosystem," *Chin. Phys. B*, vol. 27, no. 3, 2018, Art. no. 030502.
[19] D. S. Laiphrakpam and M. S. Khumanthem, "A robust image encryption scheme based on chaotic system and elliptic curve over finite field," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8629–8652, Apr. 2018.
[20] W.-K. Lee, R. C.-W. Phan, W.-S. Yap, and B.-M. Goi, "SPRING: A novel parallel chaos-based image encryption scheme," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 575–593, Apr. 2018.
[21] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-box," *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018.
[22] A. Shokouh Saljoughi and H. Mirvaziri, "A new method for image encryption by 3D chaotic map," *Pattern Anal. Appl.*, vol. 22, no. 1, pp. 243–257, Feb. 2019.
[23] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.
[24] A. Broumandnia, "The 3D modular chaotic map to digital color image encryption," *Future Gener. Comput. Syst.*, vol. 99, pp. 489–499, Oct. 2019.
[25] R. I. Abdelfatah, "Secure image transmission using chaotic-enhanced elliptic curve cryptography," *IEEE Access*, vol. 8, pp. 3875–3890, 2020.
[26] V. Kumar and A. Girdhar, "A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach," *Multimedia Tools Appl.*, vol. 80, no. 3, pp. 3749–3773, 2021.
[27] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[28] V. I. Arnol'd and A. Avez, *Ergodic Problems of Classical Mechanics*. New York, NY, USA: W. A. Benjamin, Jan. 1968.
[29] H. Liu, Z. Zhu, H. Jiang, and B. Wang, "A novel image encryption algorithm based on improved 3D chaotic cat map," in *Proc. 9th Int. Conf. Young Comput. Scientists*, Nov. 2008, pp. 3016–3021.
[30] P. N. Khade and M. Narnaware, "3D chaotic functions for image encryption," *Int. J. Comput. Sci. Issues (IJCSI)*, vol. 9, no. 3, p. 323, 2012.
[31] B. J. Saha, B. Jyoti, K. K. Kabi, and C. Pradhan, "A new approach on color image encryption using Arnold 4D Cat map," in *Computational Intelligence in Data Mining*, vol. 1. New Delhi, India: Springer, 2016. 131-138.
[32] S. Kumar and C. Pradhan, "Color image encryption technique using 4D logistic map," in *Progress in Computing, Analytics and Networking*. Singapore: Springer, 2020. 75-82.
[33] *Elliptic Curve Cryptography(ECC) Brainpool Standard Curves and Curve Generation*. Accessed: Feb. 20, 2021. [Online]. Available: https://tools.ietf.org/html/rfc5639/
[34] *USC Signal and Image Processing Insitute(SIPI) Image Database*. Accessed: Feb. 20, 2021. [Online]. Available: http://sipi.usc.edu/database/
[35] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
[36] G.-D. Ye, X.-L. Huang, L. Y. Zhang, and Z.-X. Wang, "A self-cited pixel summation based image encryption algorithm," *Chin. Phys. B*, vol. 26, no. 1, Jan. 2017, Art. no. 010501.
[37] D.-D. Liu, W. Zhang, H. Yu, and Z.-L. Zhu, "An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion," *Signal Process.*, vol. 151, pp. 130–143, Oct. 2018.
[38] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.
[39] M. Y. Valandar, M. J. Barani, and P. Ayubi, "A fast color image encryption technique based on three dimensional chaotic map," *Optik*, vol. 193, Sep. 2019, Art. no. 162921.
[40] A. Yaghouti Niyat, M. H. Moattar, and M. Niazi Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, Mar. 2017.
[41] X. Wang, X. Qin, and C. Liu, "Color image encryption algorithm based on customized globally coupled map lattices," *Multimedia Tools Appl.*, vol. 78, no. 5, pp. 6191–6209, Mar. 2019.
[42] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," *Signal Process.*, vol. 125, pp. 187–202, Aug. 2016.
[43] Y. Niu, Z. Zhou, and X. Zhang, "An image encryption approach based on chaotic maps and genetic operations," *Multimedia Tools Appl.*, vol. 79, nos. 35–36, pp. 25613–25633, Sep. 2020.
[44] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and advanced encryption system," *Signal Process.*, vol. 141, pp. 217–227, Dec. 2017.
[45] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 7, pp. 2943–2959, Jul. 2012.
[46] F. Musanna and S. Kumar, "A novel fractional order chaos-based image encryption using Fisher yates algorithm and 3-D cat map," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 14867–14895, Jun. 2019.
[47] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on hash function with only two-round diffusion process," *Multimedia Syst.*, vol. 20, no. 1, pp. 45–64, Feb. 2014.
[48] H. Liu, A. Kadir, X. Sun, and Y. Li, "Chaos based adaptive double-image encryption scheme using hash function and S-boxes," *Multimedia Tools Appl.*, vol. 77, no. 1, pp. 1391–1407, Jan. 2018.
[49] X. Wu, J. Kurths, and H. Kan, "A robust and lossless DNA encryption scheme for color images," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 12349–12376, May 2018.
[50] B. Yang and X. Liao, "A new color image encryption scheme based on logistic map over the finite field ZN," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 21803–21821, Aug. 2018.
[51] A. U. Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik*, vol. 159, pp. 348–367, Apr. 2018.

**PRIYANSI PARIDA** received the B.Tech. degree in computer science and engineering from the National Institute of Technology at Rourkela, Rourkela, India, in 2018. She is currently pursuing the M.Tech. degree in computer science and engineering with the Kalinga Institute of Industrial Technology (KIIT) Deemed to be University, Bhubaneswar, India. Her research interests include cryptography, authentication protocols, and data security.

**CHITTARANJAN PRADHAN** received the bachelor's, master's, and Ph.D. degrees from the Discipline of Computer Science and Engineering. He is currently working as an Associate Professor with the School of Computer Engineering, Kalinga Institute of Industrial Technology (KIIT) Deemed to be University, Bhubaneswar, India. He has got a total of 15 years of academic teaching experience with more than 80 publications in reputed peer reviewed journals, edited books and conferences of national and international repute. He has published few books published by publishers, like LAP Lambert, IGI Global, and Elsevier. His research interests include information security, image processing, deep learning, and multimedia systems. He is also a member of various national and international professional societies in the field of Engineering and Research, such as IET, IACSIT, CSI, ISCA, IAENG, and ISTE.

**XIAO-ZHI GAO** received the D.Sc. (Tech.) degree from the Helsinki University of Technology (now Aalto University), Finland, in 1999. In January 2004, he was appointed as a Docent (Adjunct Professor) with the Helsinki University of Technology. He is currently working as a Professor of data science with the University of Eastern Finland, Finland. He has published more than 400 technical articles on refereed journals and more than 400 technical papers on international conferences, and his current Google Scholar H-index is 33. His research interests include nature-inspired computing methods with their applications in optimization, data mining, machine learning, control, signal processing, and industrial electronics.

**DIPTENDU SINHA ROY** (Senior Member, IEEE) received the Ph.D. degree in engineering from the Birla Institute of Technology at Mesra, India, in 2010. In 2016, he joined the Department of Computer Science and Engineering, National Institute of Technology (NIT) Meghalaya, India, as an Associate Professor, where he has served as the Chair for the Department of Computer Science and Engineering. His current research interests include software reliability, distributed and cloud computing, and the IoT, specifically working on application of artificial intelligence and machine learning for smart integrated systems.

**RABINDRA KUMAR BARIK** (Member, IEEE) received the M.Tech. and Ph.D. degrees from the Motilal Nehru National Institute of Technology Allahabad, Prayagraj, India, in 2009 and 2014, respectively. He is currently working as an Assistant Professor with the School of Computer Applications, KIIT Deemed to be University, Bhubaneswar, India. He has published more than 20 international journals, like Springer, Elsevier, and IGI Global. He has also published more than 30 conference papers in various top-level conferences, like Global-SIP, CHASE, TENCON, and INDICON. He has more than 15 book chapters on his credit. Prior to this, he has edited one book named as *Cloud Computing for Geospatial Big Data Analytics: Intelligent Edge, Fog and Mist Computing* (Springer Nature) in the series of Studies in Big Data. He is doing collaborative research with The University of Texas at Dallas and the University of Rhode Island in the field of fog computing. His research interests include geospatial data science, geospatial big data infrastructure, geospatial database, geospatial cloud computing, fog computing, and IPR. He is a member of IAENG. He served as TPC and PC members in many conferences. He has received best paper awards in FICTA-2020, ICSCC-2017, and ICECE-2017 conferences. He has selected for the MHRD Scholarship during the M.Tech. and Ph.D. degrees. He has qualified GATE-2007 in information technology conducted by IIT Kanpur. He is reviewing in many journals, like Springer, Elsevier, IEEE, and IGI Global.