Hybrid Method of Document Image Encryption using ECC and Multiple Chaotic Maps

Revanna C R, Keshavamurthy C

Abstract: Document imaging is one of the most important technology used to preserve, retrieve and to transmit old documents over the internet. Since open network threatens the security of such documents from being intercepted, the proposed scheme intends to provide enhanced security for such documents. The proposed hybrid algorithm includes Elliptic Curve Cryptography (ECC), and mixed chaotic system. The ECC encrypts the plain image based on the elliptic points generated by selecting a prime number. The mixed chaotic map includes two-dimensional logistic map and three-dimensional Lorenz map. The 2D logistic map is used for confusing the ECC encrypted image and 3D Lorenz map is used for diffusing the confused image. The two levels of confusion, first with byte level and second with bit level are introduced. The two levels of diffusion, first level with Lorenz map and second level with Fibonacci sequences are introduced. Better net pixel change rate and unified average change intensity with flat histogram and low correlation are achieved in this method. The key Sensitivity, Entropy, Mean Square Error, and Peak Signal to Noise Ratio analysis reveal that the proposed method is resistant to any external invasion. The encryption and decryption speed is increased by using programming techniques. The robustness of the algorithm is also checked and found to be robust against noise and loss of information.

Key words: Elliptic Curve Cryptography; Chaotic map; Logistic map; Lorenz map.

I. INTRODUCTION

The instances where certain documents have to be shared individual-to-many, the symmetric encryption is not appropriate since sharing of the secret key between the sender and receiver is not secure as private key can be intercepted in an open network resulting in loss of confidentiality. The public key cryptography is more appropriate since the sharing of secret key is not involved. Most of the existing public key cryptosystems do not apply the public key cryptosystems to encrypt an image, instead they use symmetric encryption to encrypt the image and a public key cryptosystems is applied as a key exchange protocol. Usage of asymmetric key over the network applications is not practical, since each participating entity requires storing the keys of all other entities. Usually, in most of the existing public key cryptosystems, the ECC is not used for encryption. Rather, the symmetric cipher schemes are used. But, for the exchange of secret key ECC is used. Rarely, Elliptic curve is used for encryption since it is more useful in message authentication, key distribution and is based on mathematical functions.

ECC is fast since it uses addition operations instead of multiplications and multiplications instead of exponentiation. It is more suitable for real time and the band limited applications. The advantage of using the ECC method is due to its small key size and faster execution with low randomness. The proposed work uses ECC with mixed/multiple chaotic systems to increase the randomness, speed, security level, robustness to noise and loss of information.

II. THE RELATED WORK

[1] Gives basic idea of elliptic curves and its point generation for data encryption. Elliptic operations like point addition, point multiplication etc. are discussed in detail for secure communication. In [2] authors discussed about Elliptic curve cryptography (ECC) and its performance in terms of execution speed and security in comparison to the traditional cryptographic algorithms like RSA etc. The ECC points are generated by selecting the Prime number P. In [3] the authors discussed about ECC image encryption in which the elliptical points are generated using prime number and its security level in comparison with RSA encryption technique. In [4] the authors proposed an Elliptic curve cryptography (ECC) for color image encryption and decryption. Further they include digital signature to the encrypted image for enhanced authenticity. In order to reduce the computation time they performed operation by grouping the pixels and pairing of the grouped pixels. This yields an entropy of 7.99986 for the Lena image. In [5] authors introduced a new technique combining both image compression and encryption techniques. An Elliptic curve cryptography encryption technique is deployed during and before traditional JPEG compression technique for more security and size reduction. The image pixel values are converted into ECC points by using Koblitz’s method. A data hiding concept which includes secret message encryption using Elliptic curve cryptography (ECC) is presented in [6]. The secret image is encrypted by using ECC points and using SVD and DWT the encrypted image is watermarked for secret communication. In [7] an ECC mapping table method is used to encrypt the image. The ECC points are generated by selecting the Larger Prime number P. The mapping table is constructed using the points generated by the Elliptic curve. The generated points are mapped to the image pixels to perform encryption. An elliptic curve –Elgamal method is proposed in [8] for the transmission of a coded image over an open channel. A new additive homomorphism for elliptic curve –Elgamal is introduced for better security.
This yields a shorter key length. In [9] the cyclic elliptic curve points over Galois field are generated. The chaotic map is used to generate random sequence. A binary sequence obtained using the Threshold function is applied for chaos sequence. The ECC points are selected depending on the binary sequence. The obtained points are used as key to encrypt the medical images for security. In [10] the authors proposed a new technique which uses a non-symmetric partition to generate N-phase pseudorandom sequences by using zero-mean logistic maps with a fast algorithm to generate N-phase sequences. This algorithm yields NPCR of 99.57 and UACI of 33.22 and Entropy of 7.9972 for the Lena image. [11] Details an image encryption scheme in a transformed domain using discrete wavelet transform. This work uses two dimensional logistic map as key and haar wavelet transform in order to obtain sub bands. The obtained sub bands are encrypted using the chaotic sequence. A new ciphering technique is proposed in [12] including a 2D logistic sine for image encryption. The generated sequence from single sine map is used for two operations namely pixel permutation and pixel substitution. In [13] the authors proposed a new image encryption scheme using 3D Lorenz chaotic map. This chaotic sequence is highly sensitive to the initial conditions which results in high level security. In [14] a 3D chaos based nonlinear encryption scheme is implemented. The chaos sequence is used for confusion as well as for diffusion to increase the complexity. The proposed system include five steps in encryption process namely 3D chaotic map generation, chaos Histogram equalization, Row rotation, Column rotation and XOR operation. A modified mixed chaotic system is proposed in [15] using 2D baker map and two logistic map. Baker map is used for diffusion and the logistic map is used for confusion process. At the end the cipher image is generated by XOR operation using the sequence generated by the logistic map. A symmetric image encryption method using multi-chaotic system is proposed in [16]. The proposed scheme adopts 1D logistic map and 2D chaotic map for image encryption. A multi chaotic system applied for color image encryption is proposed in [17]. The system comprises two chaotic system namely logistic map and cubic chaotic map to achieve confusion and diffusion. In [18] the authors propose an enhanced Data encryption standard (DES) technique for increased security which includes the Elliptic curve cryptography (ECC) and chaotic logistic map for efficient image encryption ensuring secure communication. In [19] a hybrid image encryption scheme which combines logistic chaotic system and cyclic elliptic curves which generates key stream by using chaotic map is proposed. The generated keys are mixed with sequence obtained from ECC points. The proposed system yields Entropy of 7.9973 for the Lena image. Hybrid algorithms includes advanced encryption standard and elliptic curve digital signature which are introduced in [20] to encrypt the medical images for teledicine application. Two crypto systems are introduced to encrypt the DICOM images. In [21] an image encryption scheme is proposed by combining hybrid chaotic method and cyclic elliptic curve method. The pseudorandom key sequence is generated by chaotic system and cyclic ECC points. Sequence generated is used to encrypt the image. Chaos-Driven Elliptic Curve Pseudo-random Number Generator is proposed in [22]. The key sequences are generated based on Elliptic curve points driven by the chaotic map. The generated points are used to encrypt the image. The proposed method yields maximum entropy of 7.9973. From the literature, the ECC is a kind of encoding of the information. Therefore the document images encrypted elliptically are prone to statistical and dynamical attacks. The randomness produced by the ECC depends on the prime number selected to create and map the ECC points on the curve using the mapping table. For greater randomness, a very large prime number needs to be selected. As prime number is larger, searching and processing of the ECC points from the table requires more encryption time. With the small prime number generating a statistic ECC mapping table and usage of fast searching technique will significantly reduce the encryption time, but to improve the randomness, the ECC encrypted image is subjected to confusion and diffusion processes. There is a need of increasing the randomness, robustness and reducing the encryption time with a smaller prime number and provide the security against statistical and dynamical attacks is a research challenge in our proposed work. The need arises to develop a hybrid encryption algorithm and improve the performance with respect to the dynamical attacks by subjecting the elliptically encrypted document image to confusion and diffusions. More rounds of confusion and diffusion with multiple chaotic maps possessing higher dimensions increase the performance. In this proposed system, ECC is used with multiple chaotic system to provide better security over a simple ECC method. ECC is used for generating the elliptic points based on the prime number selected. The generated points are used to create static mapping table in order to encrypt the image pixels. The Multiple chaotic encryption system consists of 2D Logistic map and the 3D Lorenz maps. The Confusion process consists of two steps namely Byte level confusion and Bit level confusion. The byte level confusion is achieved by shuffling the pixels based on the random sequence generated by the 2D Logistic map. The bit level confusion is achieved by shuffling 8-bits within a pixel based on the same 2D Logistic chaotic sequences. The diffusion process is conducted in two steps where, the first step modifies the pixel values based on the sequence generated by the 3D Lorenz map, while the second step modifies the pixel value based on the Fibonacci series generated by the input original image pixel values. The establishment of the interdependency between the neighboring pixels increases the robustness against the noise and against loss of information. The encryption complexity of the proposed system is increased by combining ECC with two level chaotic encryption. Due to this, our proposed scheme yields a highly random cipher image. The NPCR and UACI values are close to their theoretical one, a flat histogram, very low correlation, high encryption speed values in all directions are expected to be achieved.
III. BRIEF REVIEW OF ELLIPTIC CURVE CRYPTOGRAPHY AND CHAOTIC MAPS

A. Elliptic Curve Cryptography

Elliptic curve cryptography is a cubic polynomial equation given by

\[ y^2 = x^3 + ax + b. \]  

(1)

Considering a and b as two positive integers whose values are less than P with x and y the two variables whose values are between zero and P \((0 < x < P)\) respectively. The values of a and b are chosen such that they satisfy the condition of discriminant

\[ 4a^3 + 27b^2 \mod P \neq 0. \]  

(2)

The value of P is chosen to be a very large prime number \(P > 3\).

The shape of the elliptic curve varies with different values of a and b.

Elliptic curves are used for the public key cryptosystems (asymmetric encryption) where two different keys one each for encryption (public key) and decryption (private key) are used. The Public key cryptosystems used with ECC are ideal under circumstances of low processing, narrower Bandwidth, smaller storage and low power consumption. ECC are used to convert plain image into a ciphered image and considered for finite prime field in which all the arithmetic is performed with a modulo P. The elliptic group includes the points for fixed values of a and b with a variable x \((x < P)\). For the sample values of (a and b) which satisfies the equation (2), the quadratic residues are obtained for different values of x. The number of points in the quadratic residue is equal to \(\frac{P-1}{2}\). For the existing value of residue, there are two different points in the \(E_P(a, b)\) group.

In ECC, each pixel in the plain image is mapped into a point from the elliptic group. Then for each value of x, determine if \(y^2\) belongs to the set of quadratic residues. If it belongs then mark two points in the elliptic group one with \((x_1, y_1)\) and another with \((x_2, y_2)\). The Fig. 1 shows how the points of the elliptic group are scattered. The total number of points in the EC together with the point at infinity ‘O’ (both x and y are \(\infty\)) is the order of the elliptic curve denoted by M. The smallest integer value N for which the product of N and P is equal to point at ‘O’ \((NP = O)\) is the order of point P such that \(N \leq M\). Then the points P, 2P, 3P… \((N-1)P\) are distinct on the Elliptic Curve. The public key is a point on the curve, while a private key is a random number generated by the owner. User A selects private key \(n_A < N\). The public key \(P_A\) is calculated as \(P_A = n_AG\) and \(P_B = n_BG\) where \(n_A\) and \(n_B\) are the private keys of party A and B respectively. G is a generator point belonging to an elliptic group, the product of n and G yields a very large prime number P. E P (a, b) and G are made public in the ECC.

In the encryption of a pixel value of the plain image, the sender chooses a random number \(K\) and determines the cipher image pair of points \(P_C\).

\[ P_C = \{(K), (P_M + KP_B)\}. \]  

(3a)

Where \(P_M\) is the plain image pixel and \(P_B\) is the receiver’s public key. The encryption process in ECC also includes the summation and product of elliptic points on the elliptic curve.

The plain image pixel can be obtained by performing the following operation.

\[ (P_M + KP_B) \cdot (n_B (KG)). \]  

(3b)

Addition and Multiplication of Elliptic Points

Assuming P and Q be two points on \(E_P(a, b)\) and O, the infinity point. The addition method used is

1. \(P + O = P\).
2. If \(Q = -P\), i.e. \(P (x_1, y_1), Q(x_2, y_2) = (x_1, -y_1) = -P\), then \(P + Q = O\).
3. If \(Q \neq -P\), then \(P + Q = (x_3, y_3)\)

Where \(X_3 = \lambda^2 - x_1 - x_2, \) \(\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \)

\(Y_3 = \lambda(x_1 - x_3) - y_1 \mod P. \)

Where \(\lambda \equiv \frac{y_2 - y_1}{x_2 - x_1}, \) if \(P \neq Q, \)

The multiplication, KG in the above equation is repeating the addition of the point G for \(K\) number of times using the equations (4) and (5). The initial value for a and b are -1 and 188 respectively. Whereas the prime number P is equal to 751.

\[ x_{i+1} = r(3y_i + 1)x_i(1 - x_i), \]  

(6)

\[ y_{i+1} = r(3x_i + 1)y_i(1 - y_i), \]  

(7)

Where \(r\) is the system parameter and \(x_i, y_i\) are the pair wise points. The map depends on three values namely \(x_0, y_0\) and \(r\) whose corresponding initial values are \(r = 1.19, x_0 = 0.8909\) and \(y_0 = 0.3342\).

B. Chaotic Maps

The Two Dimensional Logistic Map

The 2D Logistic map is distinct for its complicated chaotic nature in comparison with the mono dimensional Logistic map [23]. It takes the input \(x_i, y_i\) and \(r\) in a plane and locates it to a new position. Mathematically it can be defined as

\[ x_{i+1} = r(x_i(1 - x_i)), \]

\[ y_{i+1} = r(y_i(1 - y_i)). \]

The Three Dimensional Lorenz Map

The Lorenz equation can be represented in differential equations having chaotic behavior for certain parameters with initial conditions. Mathematically it can be defined as

\[ \frac{dx}{dt} = s(X - Y), \]  

(8)

\[ \frac{dy}{dt} = Y(r - Z) - Y, \]  

(9)

\[ \frac{dz}{dt} = X \times Y - b \times Z. \]  

(10)

The System exhibits chaotic behavior when the parameters are having values \(s = 10, r = 28\) and \(b = \frac{8}{3}\).
IV. PROPOSED METHODOLOGY

The proposed algorithm consists of three phases. The first phase includes public key cryptography called Elliptic curve encryption. While, the next two phases includes chaos based confusion and diffusion process. The complete encryption process is as shown in Fig. 2.

A. ECC Encryption

The grey scale image of size \( M \times N \) with pixel values ranging from 0 to 255 will be the input plain image. As aforementioned the elliptic points are generated by selecting a large prime number \( P \). The generated points are arranged in the form of a table called the mapping table, Table [A]. The size of the mapping table will be \( 256 \times T \), where the number of rows will be 256. The rows are numbered from 0 to 255. Each row value represents the intensity value of pixels. \( T \) represents \( S^p(a,b) \) if the last column \((T-1)\) elements in the mapping Table[A] are left free, the unfilled elements should be filled with zeroes. The ECC method of encryption, maps a pixel value from the input plain image into a point on the Elliptic Curve. For a pixel value, the first column element in the corresponding row of the mapping table is mapped, if it appears for the first time. If the same valued pixel appears for the next time, then an adjacent column element in the same row is mapped. For any pixel value after mapping the \((T-1)\) column points, the procedure repeats from the first column of the mapping table. Once, the mapping of all pixel values in the plain image is completed, the mapped points are encrypted using the public key of the receiver. The encryption of a mapped point yields in two points of which one point is common for all the pixels, whereas the other point is different. For each encrypted elliptic point, the corresponding row index is marked in the mapping table which represents the complete ECC encryption. The encryption steps are described below

1. The plain image I of size \( M \times N \) depicts pixel intensities.
2. Pixels are mapped to the elliptic curve points \( E_p(a,b) \) using mapping Table[A]. The obtained mapping points are represented in matrix J.
3. Applying the receiver’s Public key, mapping points are encrypted and R matrix deduced.
4. For each element of matrix R, the corresponding row index is marked and achieved matrix S, which is of same size as that of original plain image.

B. Confusion Process

The confusion process is achieved in two stages namely, stage 1 and stage 2. In stage 1, the byte level confusion in which the pixels of the ECC encrypted image are permuted according to the 2D Logistic pseudorandom sequences. In stage 2, the bit level confusion in which the bit positions of each pixel is permuted according to the pseudorandom sequences generated from the 2D Logistic map.

Stage 1: Byte Level Confusion

A byte level confusion is done by interchanging the rows and columns of the ECC encrypted image based on the chaotic sequence generated by 2D Logistic map. The following steps are used for the byte level confusion.

1. The ECC encrypted image S of size \( M \times N \) is taken as input for confusion.
2. The chaotic sequence is generated by 2D Logistic map and arrange them in a row matrix of size \( M \times 1 \). Sort the obtained chaotic sequence in the ascending order and the index values are obtained in L1.
3. The rows of matrix X are shuffled based on the index values of L1 to achieve matrix Y.
4. Generate chaotic sequence from the same map of size 1 x N and sort them in the ascending order. The index values of the sorted matrix are L2.
5. The columns of matrix Y are shuffled based on the index values of L2 to achieve matrix Z. The matrix Z contains the result of byte level confusion.

**Stage 2: Bit Level Confusion**
In bit level confusion, the individual bits within a byte are interchanged. The bit level confusion is achieved by shuffling 8-bits within a pixel based on the same 2D Logistic chaotic sequence as shown in Fig. 3.

1. Generate the two dimensional logistic sequence of length that is equal to number of bits in a pixel.
2. Convert the obtained sequence into integer value G.
3. Choose a pixel value E of the Z matrix and convert it into binary bits F.
4. The resultant bits are interchanged based on the integer values obtained in step 2 to achieve H.
5. Repeat the steps 3 to 4 for all the pixels in matrix Z.

### Table A. Mapping Table

| Index | 1st Mapping | 2nd Mapping | 3rd Mapping |
|-------|-------------|-------------|-------------|
| 0     | (0,375)     | (263,397)   | (274,422)   |
| 1     | (0,376)     | (264,337)   | (278,241)   |
| 2     | (1,375)     | (264,414)   | (278,510)   |
| 3     | (1,376)     | 265,76      | (279,83)    |
| 4     | (2,378)     | (265,675)   | (283,697)   |
| 160   | (187,701)   | 266,244     | (291,735)   |
| 161   | (188,94)    | (266,507)   | (295,110)   |
| 162   | (188,657)   | (267,352)   | (296,657)   |
| 240   | (205,590)   | (264,224)   |             |
| 241   | (207,215)   | (269,527)   | (299,568)   |
| 242   | (207,536)   | (260,589)   |             |
| 255   | (263,354)   | (272,675)   |             |

Retrieval Number: C4457098319/2019©BEIESP
DOI:10.35940/ijrte.C4457.118419

Published By: Blue Eyes Intelligence Engineering & Sciences Publication

International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

1619
Hybrid Method of Document Image Encryption using ECC and Multiple Chaotic Maps

C. Diffusion
It is achieved in two levels; the first level diffusion includes logical XOR operation between the confused image Z and the matrix containing the chaotic sequences obtained from the 3D Lorenz map. The second level diffusion includes logical XOR of first level diffused image and Fibonacci series obtained from the original plain image.

First Level Diffusion
1. Generate chaotic sequences from the 3D Lorenz map.
2. Convert the obtained sequences into integer value ranges from 0 to 255 and store them in a matrix Z1.
3. Logical XOR is performed between the confused image H with the matrix Z1 obtained from Lorenz map to achieve matrix H1 of size M \times N.

Second Level Diffusion
1. Take the input plain image of size M \times N and arrange them in a vector V of length 1 \times M \times N using progressive scan method.
2. Generate a new Fibonacci vector D of length 1 \times M \times N with its first element as the sum of zero and the first element of V.
3. The second element of D is sum of second element of V and the first element of D.
4. The next element of D is the sum of its previous element and the next element of V. Repeat this step until the all the elements of D are obtained
5. Convert the elements of the vector D whose value range from 0 to 255.
6. Reverse the sequence D.
7. Generate a new Fibonacci vector D1 of length 1 \times M \times N with its first element as the sum of zero and the first element of D.
8. The second element of D1 is sum of second element of D and the first element of D1.
9. The next element of D1 is the sum of its previous element and the next element of D. Repeat this step until the all the elements of D1 are obtained
10. Convert the elements of the vector D1 into a matrix of size M \times N whose value range from 0 to 255.
11. Logical XOR is performed between matrix H1 and matrix D1 which results in final cipher image C.

Decryption Process
The steps followed to extract the original plain image from the cipher image are,
1. The final encrypted image C is XORed with matrix D1 obtained during encryption which result in matrix H1 (First level diffused image).
2. The resultant H1 matrix is XORed with matrix Z1 obtained from Lorenz map to obtain matrix H.
3. The pixel’s bit positions of H are rearranged using sequence G and obtain matrix Z.
4. The rows of the matrix Z are permuted using L1 and get Y.
5. The columns of the matrix Y are permuted using L2 to get matrix S.
6. For each element of the matrix S, find the elliptical points which will map the original pixel from the elliptical mapping table using equation (3b) and store them in matrix I.

V. SECURITY ANALYSIS

A. Statistical Analysis

Entropy
The information entropy is a measure of randomness in the image. The randomness of the image is based on the probability of occurrence of the various gray levels in the image. An image whose pixel gray levels are equally probable represents highest randomness. Randomness of an image represents the confidentiality and the leakage of information. Entropy also finds the strength of the cryptosystem. Information entropy is calculated using the equation (1) in chapter 3. The entropy obtained for different images when encrypted using ECC alone are tabulated in the Table [4]. Similarly, the entropy values of different document images when encrypted using Hybrid scheme are tabulated in Table [5]. The entropy of the cipher image for the input Lena image with ECC alone is 7.5984, while for the same image with hybrid scheme is 7.9997.
The entropy for the Lena image using the proposed Hybrid method is compared with the existing methods in Table [7]. This reveals that the proposed method has higher randomness than other methods. This represents the effectiveness with respect to certainty of the document and proves its capability of resisting the entropy based attacks.

**PSNR**

It is an assessment metric to measure the visual degradation in an encryption system. The PSNR indicates the quality of the image and is also a measure of the amount of information present in the cipher (noisy) image. The proposed encryption scheme is fed with the noise free document images of different types. The PSNR is calculated using the equation (2) in chapter 3. While finding the PSNR, the cipher image is considered as a noisy image.

The PSNR values obtained for different document images are tabulated in Table [4, 5] against the ECC scheme and the hybrid scheme. It is observed that the PSNR for all document images is lesser than 10dB using the proposed method. However, the cipher image with its PSNR less than 33dB is very difficult to extract the original plain image from the cipher image. It is also observed that the PSNR obtained for the Lena image using hybrid method is lesser than that of the ECC method. Hence the hybrid method is more secure than the ECC alone.

**MSE**

A small change in the initial value of the key leads to a large change in the cipher. These changes can be measured by finding the Mean Square Error between the two cipher images. The MSE is calculated by using the equation (3) in chapter 3. The proposed encryption scheme is fed with a set of different document images for the system with ECC and the hybrid system. The MSE obtained for different images using ECC and Hybrid schemes are tabulated in Table [4, 5]. The results show that the MSE is more in the case of hybrid encryption scheme than in the case of ECC alone. It is observed that the MSE is more for a small change in the initial conditions. The smaller values of MSE enables the interceptor to visualize the original image. The larger results of MSE in Table [5] ensures that the algorithm is resistant against the statistical attacks. The system is more resistant in the case of the hybrid scheme of encryption than the scheme with ECC alone.

**Histogram**

It is a pictorial representation of the distribution of pixels of different intensity levels as against their numbers. The histograms of plain and cipher images are also used to correlate them. The histogram of the proposed encryption scheme for the input Lena image and its corresponding cipher image are shown in Fig. 4. The histogram of the plain image is shown in Fig. 4(a) has spikes in it. The histogram of the cipher image obtained from the scheme ECC alone is shown in Fig. 4(b) also has spikes. By analyzing the spikes and its statistics, the Fig. 4 [(a), 4(b)] also shows that the gray levels of the cipher images are distributed with almost equal probability and hence it indicates that a small amount of information may be predicted by an interceptor. So it is possible to predict the original image. Hence the encrypted image with ECC is predictable and less secure. The histogram of the plain image has spikes in it but no spikes are found in the corresponding cipher image obtained from the hybrid scheme. It is observed from the Fig. 4(c) that the histogram of the cipher image is perfectly flat. This indicates that all the gray levels in the cipher image are equally distributed. It also depicts that the image is truly in disorder and uniformly distributed. The uniform pixel level distribution reveals no leakage of information. It also shows that the cipher image do not indicate any clues to extract the original plain image. The hybrid scheme shows that they are not correlated. Hence the proposed encryption scheme protects information from all statistical and cipher-only attacks.

**Key Space Analysis**

When the key space is maximum, it is difficult for the interceptor to crack the algorithm using brute force attack. The proposed scheme includes ECC encryption and mixed chaotic system with two dimensional Logistic map and three dimensional Lorenz map. The initial conditions for ECC are the public keys, private keys, a, b, and P. Whereas for the 2D Logistic map, the initial conditions and control parameters are \(x_0, y_0\) and \(r\) and for the 3D Lorenz map, the initial conditions and control parameters are \(X_0, Y_0, Z_0\) and step size \(h\). It is referred that the ECC alone is resistible for the brute force attack. But in this method, along with ECC, a mixed chaotic system is also added to increase the strength of the security of the ECC encrypted image. The secret key used in the proposed scheme is shown in Table [1]. The key size is calculated using the equation (4) in chapter 3. It is approximated for the proposed method as \(2^{202}\). This secret key size is far more than \(2^{200}\) and hence the proposed method is more secret key resistant against the Brute force attack.
The key sensitivity assesses how effective the encryption algorithm is for a small change in the secret key. It represents the change in the cipher image for a small change in the key. In this proposed system of encryption, we obtain an unrecognizable cipher image for an incremental change (in the order of $10^{-15}$) in the secret key. The two cipher images obtained for the keys $K_1$ and $K_2$. The difference ratio is calculated using equation (11). This represents how many number of pixels are different for a small change in

| Map       | Sub Keys | Control Parameters | Initial Conditions                |
|-----------|----------|--------------------|-----------------------------------|
| Logistic | $K_r$    | $r = 1.9$          | $x_0 = 0.8909, y_0 = 0.3342, s = 10, r = 18, b = \frac{8}{3}$, $X_0 = 0.000000000000778899, Y_0 = 0.0000000000123654, Z_0 = 0.00000000000657789$ |
| Lorenz   | $K_s$    | $s = 10$           | $X_0 = 0.00000000000000778899$ |
| ECC      | $P = 751$|                    | $a = -1, b = 188, k = 6$ |

The low correlation coefficient between the two adjacent pixels indicates that the pixels of equal levels are distributed one adjacent to the other in an in haphazardly across the cipher image signifies the confusion and diffusion properties of the encrypted image. The pixel gray levels distribution of the plain image, cipher image from the scheme ECC alone and the cipher image obtained from the hybrid scheme are shown in Fig. 6. It is observed that the pixels in the plain image are distributed densely along the 45° in the Cartesian co-ordinate system. This indicates that the pixels of equal levels are distributed one adjacent to the other in an intelligent plain image and the human visual system could understand it. The pixel distribution is denser along the 45° in the Cartesian system and less random in the case of the cipher image obtained from the scheme ECC alone as seen in Fig. 6(e), 6(h)). This depict that the information is in intelligent form to some extent and hence it is perceptible to human visual system.

### Table 1. The Secret Key used for Encryption and Decryption

| Key Sensitivity Analysis |
|--------------------------|
| **Map** | **Sub Keys** | **Control Parameters** | **Initial Conditions** |
| Logistic | $K_r$ | $r = 1.9$ | $x_0 = 0.8909, y_0 = 0.3342, s = 10, r = 18, b = \frac{8}{3}$, $X_0 = 0.000000000000778899, Y_0 = 0.0000000000123654, Z_0 = 0.00000000000657789$ |
| Lorenz | $K_s$ | $s = 10$ | $X_0 = 0.00000000000000778899$ |
| ECC | $P = 751$ | | $a = -1, b = 188, k = 6$ |

The key sensitivity analysis indicates that the pixels of equal levels are distributed one adjacent to the other in an in haphazardly across the cipher image signifies the confusion and diffusion properties of the encrypted image. The pixel gray levels distribution of the plain image, cipher image from the scheme ECC alone and the cipher image obtained from the hybrid scheme are shown in Fig. 6. It is observed that the pixels in the plain image are distributed densely along the 45° in the Cartesian co-ordinate system. This indicates that the pixels of equal levels are distributed one adjacent to the other in an intelligent plain image and the human visual system could understand it. The pixel distribution is denser along the 45° in the Cartesian system and less random in the case of the cipher image obtained from the scheme ECC alone as seen in Fig. 6(e), 6(h)). This depict that the information is in intelligent form to some extent and hence it is perceptible to human visual system.
The pixel distribution for the cipher image obtained from the hybrid scheme is random in nature as seen from Fig. 6(c, f, i) and this depict that the information is in unintelligent form and could not be perceptible to human visual system.

B. Dynamical Analysis

Number of Pixel Change Rate (NPCR)

It’s a measure used to find the resistance of the encryption for the minute changes in plain image. The NPCR is calculated using the equation (11) in chapter 3. The differential attack is also known as the chosen plain text attack. A small change in the plain image should cause to change all the pixels in the cipher image with no changes in the key. It represents how much effective is the diffusion method used. The ideal value of the NPCR is 100%. The NPCR value for the different document images using the proposed hybrid scheme are calculated and tabulated in Table [5]. The NPCR obtained for the Lena image using the hybrid scheme is compared in Table [7]. The results of comparison indicates that the proposed method yields a larger value of NPCR. The proposed encryption scheme yields the NPCR more closely to the ideal value. Hence the proposed hybrid system of encryption is more resistant against the dynamical attacks.

Unified Average Change Intensity (UACI)

It assesses the difference in mean pixel level between two cipher images owing to minute change in the plain image. It also indicates the sensitivity of the encryption algorithm for changes in the plain image. The UACI is calculated by using the equation (12) in chapter 3. It is calculated for the different input plain images using the proposed hybrid scheme and their results are tabulated in Table [5]. The UACI for the input Lena image is compared with the existing methods in Table [7]. The UACI obtained for the Lena image using the proposed encryption algorithm is close to the ideal value 33.33%. Hence the proposed algorithm is resistant to dynamical attacks.

Structural Similarity Index Measure (SSIM)

It is a measure of structural similarity between plain image and the encrypted image. It is calculated by using the equation (13) in chapter 3. The SSIM is calculated for different document images using ECC and hybrid scheme are recorded in Table [4, 5]. The values obtained are close to the ideal value 0. This indicates that the encrypted images are visually highly degradable and hence no intelligent information can be predicted. Therefore the proposed hybrid scheme is resistant enough for dynamical attacks.

Universal Image Quality Index (UIQ)

Let \( x = \{x_i|i = 1,2, \ldots, M \times N\} \) be the original and cipher images respectively, then the quality index is calculated using the equation (19) in chapter 3. The UIQ calculated using the proposed encryption scheme for different types of document images using ECC and hybrid scheme are tabulated in Table [4, 5]. The UIQ values obtained for different types images lie within the theoretical range of values [-1, 1]. Hence the proposed encryption algorithm is efficient to sustain the dynamical attacks.

C. NIST Test Analysis

There are different complexity measurement techniques to measure the randomness of a given chaotic sequence. In this scheme, the NIST (National Institute of Statistical Test) Analysis has been conducted to quantitatively estimate the complexity of different dimensional (2D and 3D) chaotic maps. The complexity of the proposed scheme can be assessed by making use of NIST special publication 800-22 (SP 800-22) [24]. There are 16 different statistical test of special publication SP 800-22 [25]. The details on the NIST test suite are described in chapter 3. The results of randomness tests conducted on 2D Logistic map and the 3D Lorenz map are recorded in Table [2]. The test results ensures perfect randomness in all the NIST test suite.
Hence these random sequences are used for the encryption and decryption scheme.

### Table 2. NIST Test Analysis

| Statistical Analysis                          | 3D chaotic Map | 2D chaotic Map | Status          |
|-----------------------------------------------|----------------|----------------|-----------------|
| Mono Bit Frequency Test                       | 0.863775403633| 0.32652543384 | Success         |
| Block Frequency Test                          | 0.784243891129| 0.209620646602| Success         |
| Run Test                                      | 0.145169651362| 0.047760364749| Success         |
| Longest Run Ones                              | 0.874200174367| 0.299225122695| Success         |
| Binary Matrix Rank Test                       | 0.536891444943| 0.078500615631| Success         |
| Spectral Test                                 | 0.763297124216| 0.755338578368| Success         |
| No over Lapping Template Matching Test        | 0.389258576742| 0.966652786198| Success         |
| Overlapping Template Matching Test            | 0.264571775094| 0.477735602427| Success         |
| Universal Statistic Test                      | 0.973452527457| 0.387744833019| Success         |
| Linear Complexity Test                        | 0.863878207016| 0.916669104285| Success         |
| Serial Test                                   | 0.999999999999| 1.000000000000| Success         |
| Approx. Entropy Test                          | 0.999869306864| 0.997751055158| Success         |
| Cumulative Sums Test Forward                  | 0.975361188055| 0.567739751712| Success         |
| Cumulative Sums Test Reverse                  | 0.633545750229| 0.543327656132| Success         |
| Random Excursion Test                         | 0.748945710199| 0.866433877605| Success         |
| Random Excursions Variant Test                | 0.984763202196| 0.984523538855| Success         |

### D. Encryption Speed Analysis

It is a measure of encryption and decryption time. The encryption and decryption time for different document images are recorded in Table [3]. The encryption and decryption speed is basically depending on storing and searching of elliptical points in the mapping table, Table [A]. The encryption speed can be reduced by using the advanced Programming technique for storing and searching the elliptical points on the mapping table. The encryption/decryption time taken for the Lena image by the proposed hybrid encryption scheme is recorded in Table [3]. The results shows that the proposed method encrypts and decrypts the document images in lesser time. The proposed technique uses static elliptical point generation and arranging them in an ascending order as and when they are generated. The binary searching technique used for an elliptical point in the mapping table for a given pixel significantly reduces the encryption and decryption time. The encryption time taken by the proposed algorithm for different document image types are recorded in Table [3a]. The encryption and decryption time for the input Lena image using the proposed scheme is compared with the other existing methods in Table [3b]. The results indicate that the encryption and decryption time taken by the proposed scheme is lesser than the existing methods on ECC alone. Hence this hybrid method is faster than the other methods.

### Table 3a. Results of Encryption Time for Different Types of Document Images

| Document Image Type             | Encryption Time (m sec) | ECC alone | Hybrid System using ECC and 2D Logistic Map | Hybrid System using ECC, 2D Logistic Map and 3D Lorenz Map |
|---------------------------------|-------------------------|-----------|---------------------------------------------|----------------------------------------------------------|
| Lena (Picture) Image            | 575.61                  | 1387.782  | 968.909                                     |
| Text Image                      | 692.11                  | 1400.327  | 901.899                                     |
| Text with Picture Image         | 701.11                  | 1411.431  | 1002.44                                     |
| Text Surrounding Picture        | 589.09                  | 1424.39   | 1101.67                                     |
| Text + Picture Image            | 571.89                  | 1368.676  | 971.89                                      |
| DOC1                            | 612.56                  | 1304.567  | 989.12                                      |
| DOC2                            | 620.76                  | 1397.422  | 997.9                                       |
| DOC3                            | 642.11                  | 1454.886  | 972.45                                      |
E. Robustness Analysis

When images are sent via open networks, they may be accumulated with some noise or there may be some loss of data. An effective algorithm is the one which will recover the plain image from the affected cipher image; this is referred to as the robustness of the algorithm. The input cipher image with loss of information and with added noise are fed to the decryption algorithm. The results of the decrypted images are shown in Fig. 7. The result depicts that the decryption can recover the original image against the loss of information in the cipher image as shown in Fig. 7(d). But, for the salt and pepper noise added during the transmission of information, the proposed algorithm is found robust as it could recover the perceivable original plain image but with some noise as shown in Fig. 7.

![Fig. 7. Robustness: (a) The Cipher Image with Loss of Information, (b) The Cipher Image Decrypted against Loss of Information, (c) The Cipher Image with Salt and Pepper Noise and (d) The Cipher Image Decrypted against Noise with a Variance of 0.1](image)

VI. SIMULATION, RESULTS AND DISCUSSION

A. Simulation

To determine how much efficient the proposed encryption method to provide the security, the performance analysis was developed in MATLAB R2014a software using a Laptop having 4GB RAM and 80GB Hard disc. For the simulation, the proposed algorithm is fed with various gray scale document images of different sizes (512 × 512 and 256 × 256) as the input plain image. The plain Lena image and the corresponding cipher image obtained from the ECC alone is shown in Fig. 8. The other plain images and their corresponding cipher images obtained from the hybrid scheme are shown in Fig. 9. The Table [4-7] shows the results of various security parameters for different images. The Lena image decrypted with the correct decryption key, \( K = [r = 1.19, x_0 = 0.8909, y_0 = 0.3342, s = 10, r = 18, b = 8/3], X_0 = 0.000000000778899, Y_0 = 0.000000000123654, Z_0 = 0.000000000657789 \) is shown in Fig. 5. The proposed scheme is simulated for the Lena picture image using single chaotic system with the same dimensional map and the multiple chaotic system with different dimensional maps for various security parameters and the results are recorded in Table [9].

B. Results of Encryption

![Fig. 8. Results of ECC Scheme for the Lena Image: (a) Plain Lena Image and (b) ECC Encrypted Lena Image](image)
Table 4. Results of ECC Encryption on various Document Images

| INPUT IMAGE         | PSNR    | MSE      | CORRELATION | ENTROPY | SSIM  | UIQ  |
|---------------------|---------|----------|-------------|---------|-------|------|
|                     |         |          | Hori | Verti | Diag |      |      |      |
| LENA                | 9.7511  | 6.88×10³ | -0.0165 | 0.0575 | 0.0202 | 7.5984 | 0.071624 | 0.071633 |
| BABOON              | 10.0308 | 6.456×10³ | 0.00864 | 0.0426 | 0.0426 | 7.4496 | 0.060444 | 0.06033  |
| PEPPER              | 9.5020  | 7.292×10³ | 0.0434  | 0.0144 | 0.0832 | 7.6233 | 0.066619 | 0.06671  |
| PLANE               | 9.648   | 8.87×10³  | 0.0215  | 0.0141 | 0.14257 | 7.2019 | 0.109899 | 0.10872  |
| Text                | 10.867  | 6.212×10³ | 0.0755  | 0.0472 | 0.0786 | 7.3239 | 0.057624 | 0.05783  |
| Text Embedded over Picture | 9.5203 | 7.196×10³ | 0.00534 | -0.0013 | 0.00234 | 7.5232 | 0.055219 | 0.05533  |
| Text + Picture      | 9.7261  | 8.68×10³  | 0.0072  | 0.00121 | 0.01677 | 7.3426 | 0.053999 | 0.05488  |
| Text Surrounding Picture | 9.9765 | 5.88×10³  | -0.0768 | -0.0645 | 0.0163 | 7.4771 | 0.009728 | 0.00986  |
| DOC1                | 10.676  | 6.108×10³ | -0.0098 | 0.0083 | 0.0118 | 7.4209 | 0.100388 | 0.10045  |
| DOC2                | 10.201  | 6.211×10³ | 0.0011  | -0.0009 | 0.0122 | 7.1032 | 0.002759 | 0.00286  |
| DOC3                | 9.745   | 8.11×10³  | -0.05401 | 0.0335 | 0.0734 | 7.3098 | 0.035666 | 0.03422  |

Fig. 9. Results of Hybrid Encryption Scheme: (a) Plain DOC1, (b) Encrypted DOC1, (c) Plain DOC2, (d) Encrypted DOC2, (e) Plain DOC3, (f) Encrypted DOC3, (g) Plain Lens Image, (h) Encrypted Lens Image, (i) Plain Text Image, (j) Encrypted Text Image, (k) Plain Text Embedded over Picture Image, (l) Encrypted Text Embedded over Picture Image, (m) Plain Text Surrounding Picture Image, (n) Encrypted Text Surrounding Picture Image, (o) Plain Picture + Text Image, (p) Encrypted Picture + Text Image, (q) Plain Baboon Image, (r) Encrypted Baboon Image, (s) Plain Baboon image, (t) Encrypted Baboon Image, (u) Plain Plane Image and (v) Encrypted Plane Image
Table 5. Results of Encryption from Hybrid Scheme for various Document Images

| INPUT IMAGE | NPCR (%) | UACI (%) | ENTROPY | Correlation (Plain Image) | Correlation (Cipher Image) | MSE | PSNR | SSIM | UIQ |
|-------------|----------|----------|---------|---------------------------|---------------------------|-----|------|------|-----|
|             |          |          |         | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |       |       |       |       |
| LENA        | 99.641   | 33.57    | 7.9997  | 0.9698 | 0.9859 | 0.9578 | -0.0242 | -0.0171 | -0.0119 | 7.7651x10^3 | 8.881 | 7.692x10^-4 | 7.701x10^-4 |
| PEPPER      | 99.6304  | 33.458   | 7.9992  | 0.9953 | 0.9971 | 0.9917 | -0.0380 | -0.0447 | -0.0400 | 7.7643x10^3 | 8.882 | 6.882x10^-4 | 6.821x10^-4 |
| PLANE       | 9.6098   | 33.5215  | 7.9991  | 0.9835 | 0.9844 | 0.9678 | -0.0213 | -0.0129 | -0.0264 | 7.7674x10^3 | 8.882 | -0.0122x10^-4 | -0.013x10^-4 |
| BABOON      | 99.6162  | 33.3969  | 7.9992  | 0.9631 | 0.9497 | 0.9268 | -0.00085 | -0.0051 | -0.0120 | 7.7403x10^3 | 8.895 | 7.811x10^-4 | 7.808x10^-4 |
| Test Image  | 99.632   | 33.432   | 7.9991  | 0.7612 | 0.6751 | 0.8671 | -0.00067 | -0.0486 | 0.0345 | 6 | 1.8124x10^0 | 5.878 | 3.881x10^-4 | 3.781x10^-4 |
| Test Embedded over Picture | 99.6411 | 33.342  | 7.9991  | 0.9732 | 0.8782 | 0.7562 | 0.00023 | 0.00047 | 0.0123 | 1.7224x10^1 | 6.102 | 2.896x10^-4 | 2.965x10^-4 |
| Test + Picture | 99.611 | 33.464  | 7.9992  | 0.8334 | 0.8211 | 0.7862 | 0.00086 | 0.03784 | 0.0011 | 2 | 7.4480x10^0 | 8.910 | 5.756x10^-4 | 5.868x10^-4 |
| Test Surrounding Picture | 99.6127 | 33.4599 | 7.9993  | 0.8421 | 0.8951 | 0.6337 | -0.0067 | -0.0166 | -0.0262 | 7.7560x10^1 | 8.871 | 6.441x10^-4 | 6.391x10^-4 |
| DOC1        | 99.632   | 33.5102  | 7.9992  | 0.9824 | 0.7956 | 0.8622 | -0.0028 | 0.00278 | 0.0312 | 1 | 1.8034x10^0 | 5.986 | 9.886x10^-4 | 9.796x10^-4 |
| DOC2        | 99.6012  | 33.3892  | 7.9991  | 0.9012 | 0.9532 | 0.8044 | -0.0564 | -0.0552 | 0.0864 | 1.8141x10^0 | 5.867 | -0.0118x10^-4 | -0.0118x10^-4 |
| DOC3        | 99.642   | 33.5034  | 7.9993  | 0.7229 | 0.9125 | 0.7849 | 0.07101 | 0.00733 | -0.0064 | 1.8854x10^0 | 5.646 | 5.112x10^-4 | 5.501x10^-4 |

Table 6. Comparison of Results of Encryption for the Lena Image using the ECC Scheme with Existing Encryption Scheme

| Reference | NPCR (%) | UACI (%) | Entropy | Correlation |
|-----------|----------|----------|---------|-------------|
|           |          |          |         | Horizontal | Vertical | Diagonal |
| [Proposed] | NA       | NA       | 7.9997  | Red         | -0.0123   | -0.00032  | 0.0192 |
|           |          |          |         | Green       | -0.00026  | -0.0332   | -0.0756 |
|           |          |          |         | Blue        | 0.0078    | 0.0012    | -0.0056 |
| [4]       | NA       | NA       | 7.99986 | Red         | -0.00672293 | 0.000402062 | 0.0147189 |
|           |          |          |         | Green       | 0.0177625  | 0.0175243  | -0.00258394 |
|           |          |          |         | Blue        | -0.0153138 | -0.00015259 | -0.0207352 |
| [8]       | NA       | NA       | 7.9973  | NA          | NA         | NA       | NA       |

Table 7. Comparison of Results of Encryption for the Lena Image using the Proposed Hybrid Scheme with Existing Encryption Schemes

| Reference | NPCR (%) | UACI (%) | Entropy | Correlation |
|-----------|----------|----------|---------|-------------|
|           |          |          |         | Horizontal | Vertical | Diagonal |
| [Proposed] | 99.641   | 33.57    | 7.9997  | Red         | -0.0184   | -0.0327   | 0.0017 |
|           |          |          |         | Green       | -0.0051   | -0.0099   | -0.0117 |
|           |          |          |         | Blue        | 0.0056    | 0.0020    | -0.0208 |
| [10]      | 99.57    | 33.22    | NA      | NA          | NA        | NA       | NA       |
| [19]      | NA       | NA       | 7.9973  | NA          | NA        | NA       | NA       |
| [22]      | NA       | NA       | 7.9972  | NA          | NA        | NA       | NA       |

NA ➔ Not Applicable
C. Discussion

In this proposed hybrid encryption scheme, the documents are protected at two levels: At the first level using ECC and at the second level using Hybrid system. The ECC encrypted Lena image is perceptible to human visual system in Fig. 8(b). This is due to the small prime number used in ECC causing to repeat the same ECC mapping point in the pixel mapping Table [A] for the pixel level. Hence the cipher image obtained from it is predictable. The results obtained at the first level of encryption for the Lena image in Table [4, 6] reveals that less randomness, minute similarity, less noise level. This indicates that, the encrypted image may be predictable for a smaller Prime number and the ECC encryption system is insecure. At the second level, the significantly higher disorder ensures more randomness and unpredictability with the larger value of entropy in Table [5, 7]. When compared with the existing methods, the proposed system yields higher level of sensitivity and greater resistance to small changes in the plain image with a high NPCR and UACI as in Table [5, 7]. The smaller values of correlation coefficient in all directions Table [5, 7] ensures the hybrid cipher image has no redundancy and more confidentiality. The experimental results shows that it is difficult to extract the plain image from the cipher image as more noise level is achieved. The complex interdependency established between the neighboring pixels resulted in more robustness against noise and loss of information as depicted from Fig. 7. The Table [3a, 3b] reveals that, less encryption time is achieved by employing the improved programming technique. The Table [8] reveals that the hybrid system is more secure with multiple chaotic system with different dimensional maps than compared to single chaotic system with the same dimensional maps. This scheme also ensures the NIST compliance for the multiple chaotic systems and hence enables more security. Since this scheme involves no exchange of secret key, it has high level of confidentiality and integrity. Hence the proposed system is resistant to statistical and dynamical attacks, high speed and robust to noise and loss of information.

REFERENCES
1. Dr Jean-Yves Chouinard, “Design of Secure Computer Systems CSI4138/CEG4394 Notes on Elliptic Curve Cryptography”, (2002).
2. Moncef Amara and Ammar Sia, “Elliptic Curve Cryptography and its Applications”, IEEE 7th Int. Workshop on Systems, Signal Processing and their Applications, (2011), 247-250.
3. Kamlesh Gupta and Sanjay Silakari, “Performance Analysis for image Encryption using ECC”, IEEE Int. Conference on Computational Intelligence and Communication Networks,(2010), 79-82.
4. Laiphrakpam Dolendro Singh and Kumantham Manglem Singh, “Image Encryption using Elliptic Curve Cryptography”, ELSEVIER, Procedia Computer Science,11th Int.Multi-Conference on Information Processing-2015 (IMCIP-2015), Vol.54, 472-481.
5. Saied Bakhtairi, Subaraiuh Ibrahim, Mazheena Salleh, Majid Bakhatairi, “JPEG Image Encryption with Elliptic Curve Cryptography”, IEEE Int. Symp. On Biometrics and Security Technologies (ISBAST) (2014), 144-149.
6. Ritu Gupta, Pulkit Mundra, Shikha Karwal, Abhilasha ASingh, “DWT-SVD based Watermarking Scheme of JPEG images using Elliptic Curve Cryptography”, IEEE 5th ICRITO, (2016), 359-365.
7. Ali Soleyamani, Md Jan Nordin,Zulkarnain Md Ali, “A Novel Public Key Image Encryption based on Elliptic Curves over Prime Group Field”, Journal of image and Graphics, (2013), Vol. 1 No.1, 43-49.
8. Li, Ahmed A. Abd El-Latif., Xiamu Niu, “Elliptic Curve ElGamal based homomorphic image encryption scheme for sharing secret images”, ELSEVIER Signal Processing, (2012), Vol.92, 1069-1078.
9. Sovmya S and Dr S.V.Sathyararayanaya : “Symmetric Key image Encryption Scheme with key sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)”,IEEE, Int. Conference on Contemporary Computing and Informatics, (2014), 1345-1350.
10. Lingfeng Liu, Suoxia Miao, Hanping Hu, Mengfan Cheng, “N-phase logistic chaotic sequence and its application for image encryption”, IET, Signal Processing,(2016), Vol.10 No. 9, 1096-1104.
11. Ramin Mojtabah Saffri and Sattar Mirzakuchaki, “A Novel image encryption algorithm based on Discrete wavelet transform using Two dimensional Logistic map”, IEEE, 24th Iranian Conference on Electrical Engg. (2016), 1785-1790.
12. Zhongyun Hua, Vicong Zhou, Chi-Man Pun, C.L. Philip Chen, “Image encryption using 2D Logistic-Sine Chaotic map”, IEEE, Int. Conf. on Systems, Man, and Cybernetics, (2014), 3229-3234.
13. Kayhan CELIK and Erol KURT, “A New Image Encryption Algorithm based on Lorenz System”, IEEE, Int. Conf. on Electronics, Computers and Artificial Intelligence, (2016), SW. 23-28.
14. Md.Billal Hossain, Md.Toufikau Rahman, A B M Saadmaan, Syeed Islaam, “A new Approach of Image encryption using 3D chaotic map to enhance security of Multimedia Component”, IEEE, 3rd Int. Conf. on Informatics, Electronics and Vision, (2014).
15. Rashidah Kadir, Rosdiana Shahril, Mohd Azizaini Maroof, “A modified image encryption scheme based on 2D chaotic map”, IEEE, Int. Conf. on Comp and Comm.Engg, (2010).
16. Sahar Mazlooom and Amir-Masud Eftekhari-Moghadam, “Color Image Cryptosystem using chaotic maps”, IEEE Conf, (2011).
17. N.F.Elebady, H.M.Abdalkader, M.I Moussa, S F Benha, Egypt, “Image Encryption based on New One-Dimensional Chaotic map”, IEEE Conf, (2014).
18. Mohammed A. Seif Eldeen, Dr Abdellatif A. Elkouny, Prof Dr. Salwah Elramly, “DES Security Reinforcement Using Chaotic Logistic map and Elliptic Curve Cryptography”, IEEE Conf, (2015).
19. Ahmed A. Abd El-Latif and Xiamu Niu, “A hybrid chaotic system and cyclic elliptic curve for image encryption”, ELSEVIER, Int. Journal of Electronics and Communications, (2013), Vol.67, 136-143.
20. Ali Al-Haj, Gheith Abandah, Noor Hussein, “Crypto-based algorithms for secured medical image transmission”, IET, Information Security, (2015), Vol. 9, No.6, 365-373.
21. Hong Liu and Yanbing Liu, “Cryptanalyzing an Image encryption scheme based on hybrid chaotic system and cyclic elliptic curve”, ELSEVIER, Optics and Lase Tech, (2014), Vol.56, 15-19.
22. Omar Reyad, Zbigniew Kotulski et.al: “Image Encryption using Chaos-Driven Elliptic Curve Pseudo-Random Number Generators”, (2016), Appl. Math. Inf. Sci. Vol. 10, No. 4, 1283-1292.
23. Yue Wu, Gelan Yang Huixia Jin,et.al, “Image encryption using the two-dimensional logistic chaotic map”,Journal of Electronic Imaging, Vol. 21 (1), (2012).
24. Meleo, A., Bezerra, P. and Ahlem, A., et al. Priority QoE: a tool for Improving the QoE in Video Streaming, Intelligent Multimedia Technologies for Networking Applications: Techniques and Tools, chapter 11. (2013).
25. Liu, H. and Wang, X. (2011). Color image encryption using spatial bit-level permutation and High-dimension chaotic system’, Optical Communication,284, pp. 3895–3903.

AUTHORS PROFILE

DR C Keshavanurthy is B.E. and M.E. in Electronics and Communication Engineering and received his Ph.D in the area of C A N. His academic interests include Computer Communication Networks, Ad-hoc Wireless Networks and Multimedia Communication. He has a research experience of over 20 years and has published many research articles on image encryption. Served as the Principal at YDIT, Bangalore. Currently working as a Professor of Electronics and Communication Engineering at SRSIT, Bangalore.

Mr C R Revanna is a B.E. in Electronics and Communication Engineering, M.E. in Electronics at UVCE from Bangalore University, Bangalore, India. His research interest includes Encryption, Image Processing and Cryptography, and published research articles on document image encryption. Currently working as Assistant Professor in Electronics and Communication Engineering at Government Engineering College, Ramanagaram, India. He is also pursuing his Ph. D. research work at Jain University, Bangalore, India.