Adv Syst Sci Appl 2022; **01**:92–116
Published online at https://ijassa.ipu.ru.

Secure Image Cloud Storage Using Homomorphic Password Authentication with ECC Based Cryptosystem

Devipriya M., M. Brindha*

Department of Computer Science and Engineering, National Institute of Technology, Tiruchirappalli, Tamilnadu, India

Abstract: Cloud based storage gives us ease of storing large data. Cloud is a storage that can store multimedia images and other data, but what happens to the data after the storage is invisible to the user. To protect the image in the cloud and transmission to the cloud, image encryption is used. Confidentiality is the way to protect from unauthorized access while transmitting and storing medical images, military images, online banking and telecommunication. Recently, chaos has become an emerging trend towards the encryption of images. New techniques are adopted in image encryption to increase the randomness and to decrease the correlation between the pixels. In the present work, an authentication based framework and image cryptosystem has been proposed for secure storage in the cloud. Authentication is provided using SHA hash algorithm and elgamal encryption. Image cryptosystem uses chaos based scrambling using bit-matrix generated from logistic chaotic map sequence. A novel key generation for chaos is done using Fourier transform for the image cryptosystem. Bit sequence and sorting based pixel permutation are performed using the chaotic sequence. Totalistic cellular automata technique has been applied using the corner neighborhood values to diffuse the image pixels. Pixels of the image is finally diffused using the random sequence formed using elliptic curve points/ coordinates to improve the security. This encryption technique is evaluated using statistical and differential analysis. ECC gives security using the discrete logarithm problem. From the analyses, it is shown that it possesses large keyspace, sensitivity towards a small change in pixel value and also key value. It also resists pattern attacks as well as differential attacks.

Keywords: trusted agent, ElGamal encryption, Fourier transform, bit matrix based scrambling, cellular automata diffusion, elliptic curve encryption

1. INTRODUCTION

Cloud based storage is used as it is accessible anywhere using the internet facility and also does not crash like any hard disk. Managing the data in the cloud and also sharing the data with people is much comfortable. This data includes multimedia data such as images which should be encrypted before storing it in the cloud. Encryption before submitting the data to the cloud prevents leakage of information both in the transmission network as well as while stored in the cloud. Many businesses either large scale or small scale use to store the documents, images and other data in the cloud. It is easy to access the data from anywhere without a need for maintaining a storage platform. The image data and other records of the medical field can be stored and retrieved in the cloud. Similarly, different fields such as military, media, legal and even common people use the cloud to store the image and other documents. To protect the image files, there are a lot of applications available. Stingle photo is an application that encrypts the data and stores it in the cloud environment. Digilocker is a service initiated by the government of India for every citizen to store documents in the cloud securely. To provide confidentiality, data integrity and authorization, the images are

*Corresponding author: brindham@nitt.edu

encrypted before storing them in the cloud. Even though the cloud is safe, it can analyze the data for advertisement purposes which can be prevented using encryption. Authentication is used to provide credentials only to the authorized user. SHA algorithm and Elgamal encryption are used in the proposed authentication technique to serve the intended user by the trusted agent. In the proposed image encryption, in addition to the sorting based permutation, bit sequence based pixel permutation is performed to reduce the relationship between the adjacent pixels. A novel Fourier transform based key generation technique is adopted to generate new keys each time to reduce the possibility of differential attacks. Many researchers in the literature concentrate on the permutation part rather than the diffusion. Hence, in this proposed technique, the totalistic cellular automata is adopted to give strength towards the effectiveness of the diffusion. The novel combination adopted in the diffusion is totalistic cellular automata with ECC based prime field which provides high level security that can be seen from the analyses obtained. Correlation coefficient analysis shows lesser possibility to statistical attack as well as the NPCR and UACI results show that the possibility of differential attack is less.

From the study of the existing literature, it has been found that the solutions in the literature do not involve homomorphic authentication which is considered as very safe method as it does not decrypt the credentials to authenticate the user. In homomorphic encryption, the comparison for authentication is done in the encrypted value itself. In the existing literature, cryptosystems do not use plain image related key as it is used to overcome differential attacks. The following are the contributions of the proposed system:

1. Homomorphic encryption based authentication algorithm to authorize the user.

2. Initial keys for the proposed cryptosystem are formed using Fourier transform, a novel technique to overcome the differential attack depending on the plain image.

3. A novel totalistic cellular automata based diffusion is employed to avert the statistical attack.

4. ECC encryption converts the chaotic sequence into coordinates and these coordinates are reduced to random sequence for diffusion to overcome both the correlation based attacks and to improve the substitution efficacy.

The organization of the paper is as follows. Section 2 is the study of available authentication and image encryption techniques in the literature. Section 3 is the preliminary section that defines and elaborates the techniques adopted in the proposed system. The proposed authentication framework which describes the authentication technique designed using the Elgamal encryption is presented in section 4. Section 5 describes the proposed ECF image encryption scheme. Section 6 presents the results obtained from the proposed authentication and image encryption. The summary of the techniques used in the proposed authentication systems and image encryption has been provided in section 7.

2. RELATED WORKS

There are different kinds of authentication methods like passwords, biometric and smart cards etc., which are used to recognise the authenticated user. In [44], session initiation with user anonymity using ECC is developed. [3] uses three factor key agreement and authentication using ECC. Fuzzy extractor function is developed to provide authentication of the mobile user for mobile cloud computing in [35]. Authentication with user anonymity is developed using biometrics and ECC in [15]. Authentication based on the chaotic map for WSN is proposed in [17]. Different authentication schemes like [18], [16] and [13] are proposed for IoT and cloud based environments. The computations mentioned in the literature are not using homomorphic technique which is highly required when authenticated data is outsourced to non trusted environments. The main advantage of homomorphic encryption is that there is no need to decrypt the credentials to authenticate the user.

Lorenz introduced the first chaotic attractor in the year 1963 [27] from then the research in the chaotic system has started and flourished. The chaotic system is disordered in its state and shows high sensitivity towards the initial state [34]. This stimulates chaotic systems to gain attention by the researchers in image encryption [37, 46]. Confusion and diffusion structure using chaotic systems is followed by the researchers which were suggested by Fridrich [7]. Normally, permuting the pixels is done and it is followed by substitution or diffusion which changes the value of the pixel.

Elliptic curve cryptosystem (ECC) provides security using the discrete logarithm problem. The advantage of the elliptic curve system is, it uses less key space with greater security but the problem is, if it is directly applied to the image, the statistical attack might be possible. By changing it into a random irregular form and then applying ECC will prevent various kinds of attacks. Many researchers used the chaos technique and ECC technique to encrypt the images from which few of them are described in this section.

In [10], image is converted into serial bits using the steps such as transpose, reshape, to-frame and unbuffered blocks. In addition, different chaotic maps are used to create three different random sequences and these three sequences are XORed to get a new pseudo random bit generator sequence to encrypt the plain image. Even though three random sequences are involved, single diffusion is vulnerable to attacks. In [5], the image is split into three channels and it is converted to YCbCr color space. This combined YCbCr is converted into 8×8 blocks and these subblocks are scrambled. These subblocks are inverted, rotated and applied a positive negative transformation to get the encrypted image but the drawback is, block level scrambling alone cannot provide a good permutation result. Also, converting the color image into gray scale and the reverse may lead to lossy conversion. In [36], a new 3D chaotic system is realized and chaotic permutation by row wise as well as column wise is done. Diffusion using XOR with the permuted image is performed using the chaotic sequences. Here the uniformity in the encrypted pixel distribution and the efficiency of the substitution are less. In [8], bit pair level rotation is performed by converting each pixel into four pairs of bits to confuse the image. Paired bits based rotation is performed on 8×8 bit pair blocks. These 64 bit block is converted into 4 regions. Each region is rotated using the control instructions. The type of rotation, clockwise or anti-clockwise is determined by the parity. The chaotic sequence is derived from a modified pulsed coupled spiking neurons circuit map. Also, XOR and add operations are used to diffuse the image. The computational complexity for the confusion is high for bit pair level rotation.

In [23], using 2D Henon-Sine map sequences, two sequences are obtained in which one sequence is added to the pixel of the image row wise and another sequence is added to the pixel of the image in column wise. In continuation, the sine map chaotic sequence is obtained and added to the image pixel in row wise. Swapping of rows is used to interchange the place of the pixels. Previous row pixel values are XORed with the present row values. Similarly, column wise swapping, addition and XOR are done. The limitation of this work is swapping of rows alone cannot provide better permutation and also encryption has the possibility for attacks as the randomness and irregularity in encryption is less. In [28], crossover permutation is used to confuse the pixel values using the sequence obtained from the logistic-tent map and tent-sine map and the elliptic curve and Elgamal are used to get cipher points from the confused pixels. These points are then converted to a pixel like value using addition, XOR and modulo. Crossover permutation is good to confuse the pixels and it provides a good result when it is adopted in higher order bits. However, the disadvantage is, correlation between the pixels in the encryption is high in this scheme. In [19], Blake2 hash algorithm takes the plain image as input and produces two 256 bit keys. These 256 bit keys, key1 and key2 are given as input to Blake2 hash algorithm to calculate two pseudo random streams Key_{enc1} and Key_{enc2}. Plain image is converted to 8×8 blocks which undergo a single horizontal transform for 8 rows and 8 vertical different transforms for 8 columns and these blocks are quantized using a JPEG quantization table. Key_{enc1} pseudo random sequence and Fisher- Yates shuffle algorithm are used to permute these blocks and DC coefficient is changed for each block. For AC coefficient encryption, Key_{enc2} pseudo random sequence is used for key1 embedding and the entropy based encoding of AC and DC coefficients is used to produce the encrypted values. In this algorithm, the randomness in the encryption is less, hence there is a possibility of statistical attacks. In [20], the image is water marked using the discrete wavelet transform function. Josephus traversing map is generated to scramble the watermarked image. Logistic map, XOR and mod operation are used to encrypt the scrambled image. Single diffusion has the risk towards known/ chosen plain text attacks.

In [25], image is converted into blocks and converted to quantum image representation. These blocks are scrambled using quantum Arnold transform and encrypted using the sine chaotic sequence and logistic map with XOR operation. Uniformity in the pixel distribution is less in this encryption. In [32], discrete wavelet transform is applied to sparsify the image to get the sparse coefficients. It is converted to a 2D array with the 2D-LASM chaotic sequence and is used for the permutation. Compressive sensing based encryption is done using a 3D Arnold cat map and a structural random map is created using Arnold map sequence. Finally, the encrypted value is quantized in the range [0, 255]. These encrypted values are embedded in a carrier image by dividing the carrier image and the intermediate image (IM) into blocks and mapping the IM to the carrier image to produce the cipher image using a reversible color transformation but the uniformity in the distribution of pixels is less in this encryption. In [38], plain image is confused using Lorenz chaotic sequence and the permuted image is encrypted using forward and reverse diffusion. With this cipher image, the hash code of the plain image is sent to the receiver to check the data integrity. Correlation between the pixels is high in this encryption. In [43], plain image is converted into blocks and a tent sine map is used to calculate the measurement matrix to compress the image blocks. Arnold Cat map is calculated to scramble the image blocks. 2D Fractional Fourier transform and Chen hyperchaotic map are applied to diffuse the image. The initial values of the chaotic sequence are derived from the hash code of the plain image. Randomness and irregularity in the encryption are less, hence there is a possibility for the statistical attack in this encryption. In [33], 2 pseudo sets and a set of keys are produced to shift column and row of the image circularly and to diffuse the scrambled image. The pseudo set and key for permutation are produced using chaotic permutation and multi circular shrinking is applied with gradual removal of the input set. The efficiency of the substitution is less, hence there is a possibility for the differential attack in this system.

In [9], a 3D image is formed out of N different images. The initial value for chaotic maps is selected using the SHA-256 hash code. An intertwining logistic map is utilized to choose the images which is also used to select the particular row and column in selected images for scrambling. Rows and columns that are selected in the images using the intertwining logistic map are swapped. Finally, this scrambled 3D image is encrypted using an improved piecewise linear chaotic map. Swapping the whole rows cannot provide better permutation results in this work. In [14], two shared keys and nonces are produced for encryption. One key and nonce are calculated to construct an S-box whereas another key and nonce are used to construct the chaotic sequence. Each pixel value maps to an S-box value. This S-box value along with previously encrypted pixel and chaotic value are used for diffusion. To diffuse a pixel, two S-box mappings are used, that may lead to a collision if different S-boxes are mapped to the same pixel. In [29], a new random sequence is formed using ECC and XORed with the image pixel values. The permutation is done using the crossover technique which improves the efficiency of permutation only when it is performed in the high order bits. In [12], S box is created using ECC and chaotic sequence which is used to diffuse the pixel values. The efficiency of the substitution is less, hence there is a possibility for the differential attack.

In the proposed encryption scheme, the bit sequence based pixel permutation and sorting based permutation are performed to resist the statistical attacks. The totalistic cellular automata based diffusion and ECC based diffusion are employed to resist the differential attacks. Moreover, many of the existing solutions perform simple XOR based diffusion but in the proposed work complexity of the diffusion has been increased to improve the security. Adaptive plain image related key generation strategy is used in the proposed encryption technique to overcome the differential attack which is a highlight when compared with the existing solutions.

3. PRELIMINARY

This section describes the techniques used by the proposed framework such as an authentication scheme using elgamal and an encryption scheme using elliptic curve with fourier transform (ECF).

3.1. Elgamal Encryption

A prime p is chosen, a primitive root $g\ (mod\, p)$ is chosen as generator. A random number a is chosen as exponent which is the secret key. Public key is (p, g, A) and A is given by (3.1).

$$A = g^a\ (mod\, p) \tag{3.1}$$

Given, y_1 and y_2 are the two plain values, the multiplicative homomorphism of elgamal encryption is given by (3.2).

$$E(y_1 \cdot y_2) = E(y_1) \cdot E(y_2); \tag{3.2}$$

where $E(y_1)$ and $E(y_2)$ are the encrypted values of y_1 and y_2.

3.2. Fourier transform

The Fourier transform is the main tool for image processing which is used to convert an image into sine and cosine components. The result of the transformation converts the image to the frequency domain. The equation for Fourier transform is realized in Eq. (3.3).

$$z(k) = \sum_{j=0}^{L} Z_j \left[\cos\left(\frac{2\pi}{L}kj\right) - i\sin\left(\frac{2\pi}{L}kj\right)\right], \tag{3.3}$$

where $k \in [0, L-1]$.

3.3. Totalistic cellular automata

The neighborhood values of the cell are used as a whole to apply the cellular automata rules. Say, for instance, the neighborhood cell values are added or XORed or multiplied or averaged to get a totalistic value and this value is used to get the next generation value of a cell.

3.4. Finite field arithmetic

Finite field arithmetic is used in the EC cryptosystem in order to get a value bound to a finite set of numbers. Overflow in addition or multiplication makes the data insufficient to revoke at the decryption side.

3.5. Elliptic curve cryptography over prime field

The discrete logarithm problem is mainly used by the elliptic curve cryptosystem to ensure the security. An elliptic curve on a prime field F_R is realised by Eq. (3.4).

$$q^2 = p^3 + cp + d\ \ (mod\ \ R), \tag{3.4}$$

where $c, d \in F_R$, $R \neq 2, 3$ and satisfy the condition $4c^3 + 27d^2 \neq 0 \; (mod\, R)$. The points satisfy the curve equation and point at infinity O includes the order of the curve $\#E(F_R)$. Group law for the curve is

1. Identity: $A + O = O + A = Q$ for all $A \in E(k)$.

2. Negatives: If $A = (p_1, q_1) \in E(k)$, then $(p_1, q_1) + (p_1, -q_1) = O$. The point $(p_1, -q_1)$ is denoted by $-A$ and it is called the negative of A. $-A$ is a point in $E(k)$. $-O$ is equal to O.

3. Point Addition: Let $A = (p_1, q_1)$ and $B = (p_2, q_2) \in E(k)$, where $A \neq \pm B$. Then $A + B = (p_3, q_3)$. Taking into account Eq. (3.5), we have

$$
\begin{aligned}
p_3 &= \left(\frac{q_2 - q_1}{p_2 - p_1}\right)^2 - p_1 - p_2 \;\; (mod \;\; R), \\
q_3 &= \left(\frac{q_2 - q_1}{p_2 - p_1}\right)^2 (p_1 - p_3) - q_1 \;\; (mod \;\; R).
\end{aligned}
\tag{3.5}
$$

4. Point Doubling: Let $A = (p_1, q_1) \in E(k)$, where $A \neq -A$. Then $2A = A + A = (p_3, q_3)$. Taking into account Eq. (3.6), we have

$$
\begin{aligned}
p_3 &= \left(\frac{3p_1^2 + c}{2q_1}\right)^2 - 2p_1 \;\; (mod \;\; R), \\
q_3 &= \left(\frac{3p_1^2 + c}{2q_1}\right)^2 (p_1 - p_3) - q_1 \;\; (mod \;\; R).
\end{aligned}
\tag{3.6}
$$

3.6. Chaos based encryption

Chaotic systems are preferred in image encryption for their randomness, periodicity, sensitivity to initial values and ergodicity. It is not only dynamic but also has the property to generate the values depending on the initial value for effective decryption. In this paper, logistic map is used to derive random sequences for permutation and diffusion.

3.6.1. Logistic map The logistic map is a chaotic function to calculate pseudo random sequence using equation (3.7).

$$a_{n+1} = \alpha a_n (1 - a_n), \tag{3.7}$$

where $0 < a_n < 1$ and $\alpha = [0, 4]$ are used to get chaotic behaviour.

4. PROPOSED AUTHENTICATION FRAMEWORK

The classical method of storing the image in the cloud does not encrypt the image and hence there can be possibility of attacks to steal the information from the cloud. Fig. 4.1 shows the classical method of storing the image in the cloud. In order to overcome this limitation, a novel authentication based cryptosystem has been developed. The authentication protocol is designed using SHA 256 hash and Elgamal encryption. The proposed cryptosystem is based on chaos, totalistic cellular automata and ECC. The framework consists of three levels such as user, trusted agent and cloud server. The user who wants to store images in the cloud will register with the trusted agent with user id and password. The trusted agent stores the hash

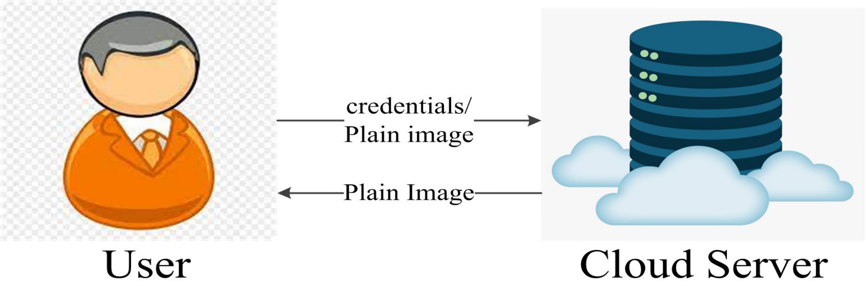


Fig. 4.1. classical Framework

value of user id and the encrypted hash value of the password. Whenever the user has images to be stored in the cloud, the user will login into the trusted agent and this trusted agent checks the hash value of the user id for equality. The encrypted hash password stored in the database is divided by the encrypted hash of the password entered by the user which leads to a value of 1 since the encryption is homomorphic. Subsequently, the trusted agent authenticates the user, encrypt the images and pass them to the cloud. On the other way, the trusted agent rejects the user whose user id or password does not match. Fig. 4.2 shows the proposed authentication framework.

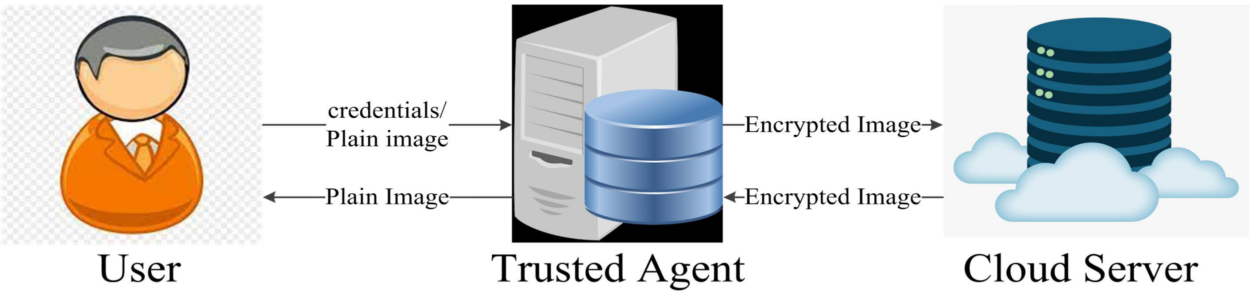


Fig. 4.2. Proposed authentication framework

4.1. Authentication System Entities

The proposed authentication system consists of User (U), Trusted agent (T) and cloud server (CS).

1. User: This entity is the one which owns the images and wants to store the images in the cloud server.

2. Trusted agent: This entity is the server that authenticates the user and encrypts the images. For authentication, Elgamal homomorphic encryption has been used and for image encryption, the proposed ECF cryptosystem has been used.

3. Cloud server: The cloud server stores the images encrypted by the trusted agent. The images in the cloud are retrieved by the trusted agent whenever there is a request raised by the user to access the images.

4.2. Proposed framework design

This section presents the sequence of the key generation process, user registration in T, authentication and encryption process done in T.

Table 4.1. Hashed userid

Userid	Hashed userid
user	0F96A6BA6B08E076EFA346DB1D1C59FF
user@123	DB9A02F4E902587F2B5BF34B4C774D84

Table 4.2. Encrypted password values

Password	Hashed encrypted value
authen	131B3309235535EA00002E5338CB2 DCD103A00C938452FE51DD62A23 1FEE2E100BC727852CC12D4707DA 2C3B1AF51682330933090C903B263 2C60C0A010C25F3
authen@123	170830AE103A0DDF2D4735EA0F2 E16823ED01CCA2D8A14AD2ED93 0F12E96025B05F39510FB41F680B4 1252A096CC27423A5D3BEF163F37 391AF5170841F42679

4.2.1. Key generation In key generation, only one private key a is chosen. The generator raised to a is multiplied with the message to get the encrypted result. As the system is homomorphic, multiplicative homomorphism is utilized to test the equality between the passwords.

4.2.2. User registration The user registration is a process of creating user id and password with T. The created user id is hashed using SHA algorithm and the created password is hashed and encrypted using the SHA and Elgamal encryption. Fig. 4.3 depicts the user registration. Table 4.1 and Table 4.2 show the hashed user id and hashed encrypted password.

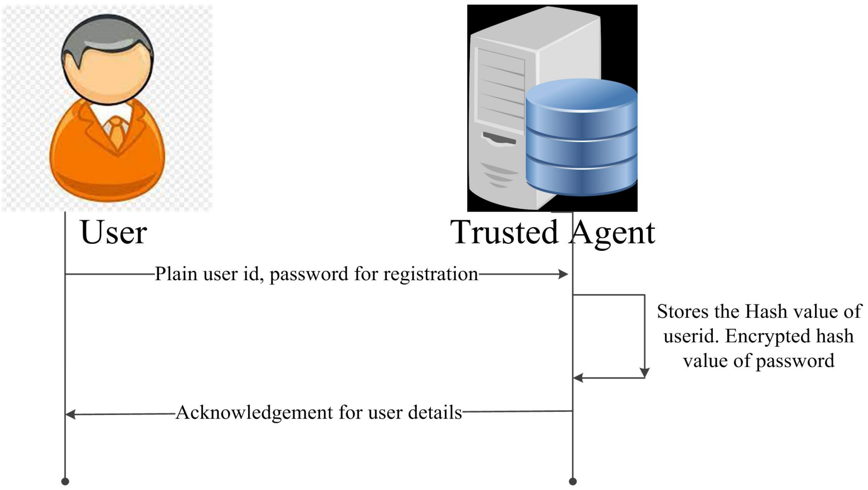

User
Trusted Agent
Plain user id, password for registration
Stores the Hash value of userid. Encrypted hash value of password
Acknowledgement for user details

Fig. 4.3. User registration

4.2.3. Authentication and image encryption The authentication is performed by a trusted agent.

1. User enters the user id and password.

2. The hash value of the user id is compared with the authentication table.
3. If the user id in the authentication table matches with the entered user id, the hash value for password entered is created and it is encrypted using Elgamal encryption.
4. The password in the authentication table is divided by the encrypted password. The authentication is said to be successful if the result is 1. Otherwise, it fails.
5. If the authentication is successful, then the images of U are encrypted using the proposed ECF cryptosystem by T and stored in the CS.
6. Whenever the image is needed, T is queried by U and T, in turn query the cloud server to retrieve the image and send it to U after decryption. Figures 4.4 and 4.5 show the user authentication and storage of encrypted image to CS using T and retrieval of decrypted image from CS using T, respectively.

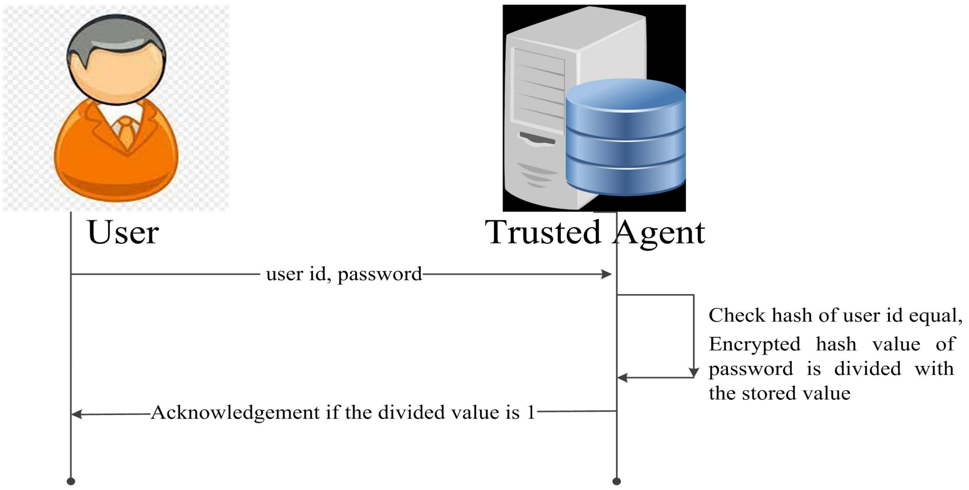

User
Trusted Agent
user id, password
Check hash of user id equal, Encrypted hash value of password is divided with the stored value
Acknowledgement if the divided value is 1

Fig. 4.4. User authentication

5. PROPOSED ENCRYPTION SCHEME

The proposed elliptic curve with Fourier transform based key (ECF) system starts with the generation of key value for the chaotic system. The initial key value is generated using Fourier transform based equation. It takes the unique pixels from each color plane R, G and B. These pixel values are multiplied with the sine and cosine functions to get the initial keys which are used to generate the logistic map sequences. These sequences are used to scramble the pixels of each plane. The chaotic sequence is sorted and its index values are used to scramble the pixel values. The same chaotic sequence is diffused with the scrambled pixels using totalistic cellular automata technique. These image pixel values are diffused using the random sequence formed by the coordinates of an elliptic curve, given a prime number R. In this ECC encryption, R value and curve points (c and d in Eq. (3.4)) are also considered as the secret values in addition to the private key. Fig. 5.6 shows the diagram of the encryption process.

5.1. Proposed approach

This section elaborates the encryption and decryption process of ECF.

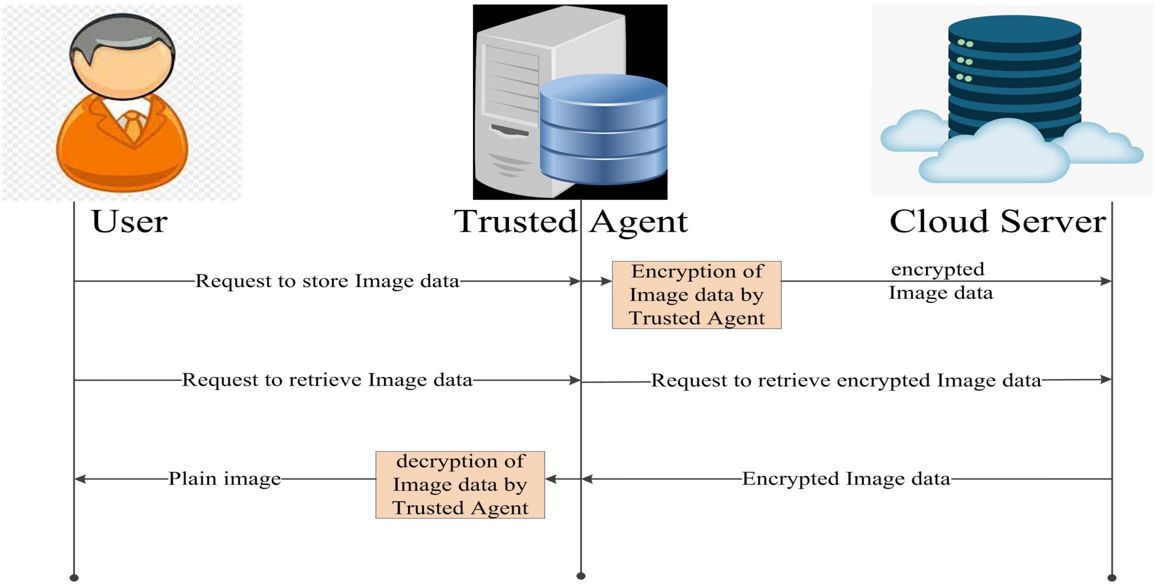

User
Trusted Agent
Cloud Server
Request to store Image data
Encryption of Image data by Trusted Agent
encrypted Image data
Request to retrieve Image data
Request to retrieve encrypted Image data
Plain image
decryption of Image data by Trusted Agent
Encrypted Image data

Fig. 4.5. Store and retrieval

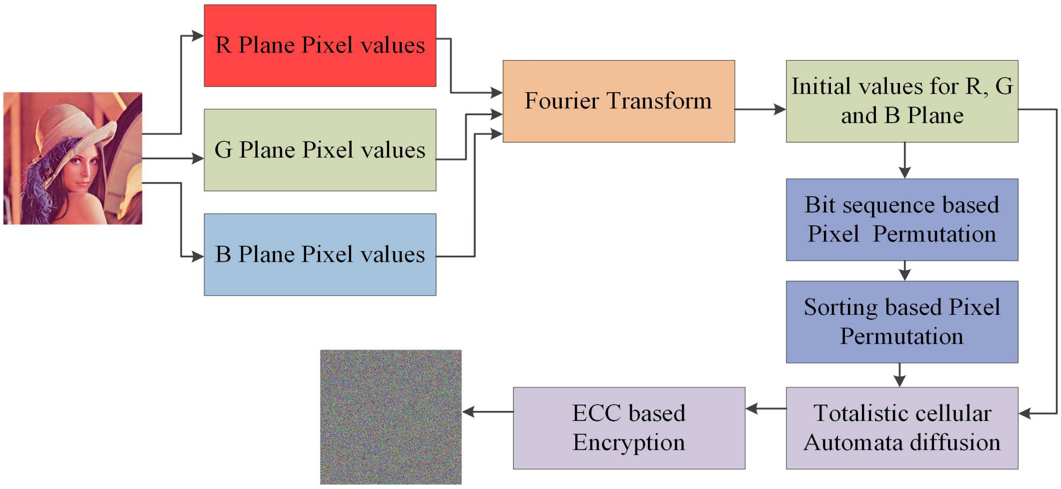

R Plane Pixel values
G Plane Pixel values
B Plane Pixel values
Fourier Transform
Initial values for R, G and B Plane
Bit sequence based Pixel Permutation
Sorting based Pixel Permutation
Totalistic cellular Automata diffusion
ECC based Encryption

Fig. 5.6. Encryption Process

5.1.1. Encryption process

1. Key Generation for Chaotic Map
   Fourier transform function is used to calculate the initial values for the chaotic map. Equation (5.8) is used to calculate initial value for chaos.

$$K = \sum_{j=0}^{L} z_j \left[\cos\left(\frac{2\pi}{L} j^2\right) \sin\left(\frac{2\pi}{L} j^2\right)\right], \tag{5.8}$$

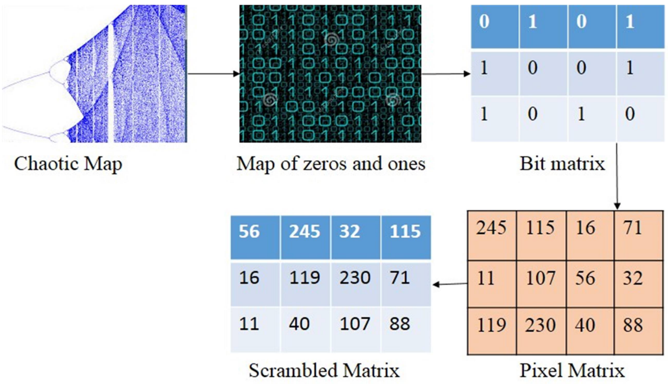
   where α and $x(1)$ for logistic map are derived from K. z_j is the pixel and L is the number of unique pixels in color plane R. Similarly, K for G and B planes are calculated.

2. Chaotic sequence
   The chaotic sequence is generated using the initial values derived from Fourier function.

The random chaotic sequence is generated using Eq. (5.9).

$$a(n+1) = \alpha a(n)(1 - a(n)) * 10^4 \ \ mod \ \ 1 \tag{5.9}$$

3. Permutation using bits sequence and sorting
The chaotic sequence is converted to bits and these bits act as a control parameter to jumble the image. The image pixel values are substituted sequentially in the places of ones. The remaining pixel values are substituted with zeros. The chaotic sequence is sorted and the index values are used to permute the pixels. Figures 5.7 and 5.8 show the permutation using bit sequence and sorting, respectively.



Bit matrix

0	1	0	1
1	0	0	1
1	0	1	0

Pixel Matrix

245	115	16	71
11	107	56	32
119	230	40	88

Scrambled Matrix

56	245	32	115
16	119	230	71
11	40	107	88

Fig. 5.7. Permutation using bit sequence

1	2	3	4	5	6	7
0.2211	0.5115	0.4114	0.3136	0.1142	0.7129	0.6127

Unsorted chaotic sequence

5	1	4	3	2	7	6
0.1142	0.2211	0.3136	0.4114	0.5115	0.6127	0.7129

Sorted chaotic sequence

1	2	3	4	5	6	7
102	104	151	160	161	140	131

Pixel values before scrambling

5	1	4	3	2	7	6
161	102	160	151	104	131	140

Pixel values after scrambling

Fig. 5.8. Permutation using sorting

4. Diffusion using totalistic cellular automata
Chaotic sequence is converted to a matrix and the corner neighborhood values are added with the corresponding $(i, j)^{th}$ value. This sum value is added to the pixel value and it is

reduced to 0 to 255 values. Fig. 5.9 represents the function of totalistic cellular automata.

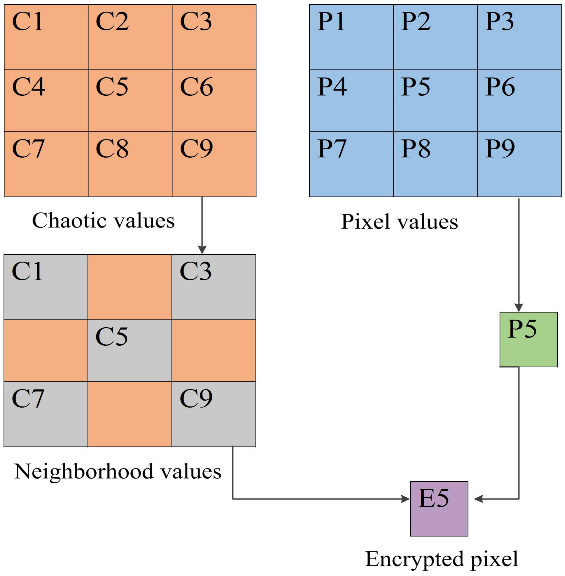


Fig. 5.9. Totalistic Cellular Automata

5. ECC based diffusion
   In this diffusion, pixels are diffused using values obtained from ECC coordinates.
   (a) Let R be 643, $a = 1$, $b = 19$;
   (b) Let private key value of user A be $k_a = 148$.
   (c) $G = (14, 89)$ is the generator.
   (d) Public key of user B, $P_b = k_b.G = (276, 203)$.
   (e) CE is coordinate points calculated using Eq. (5.10).

$$CE = C.G + P_b.k_a \tag{5.10}$$

   (f) C is the chaotic sequence and the elliptic curve coordinate points formed using C is shown in Table 5.3.

Table 5.3. Elliptic curve coordinates using C

	1	2	3	4	....	512
1	(159,204)	(193,620)	(174,346)	(555,272)	....	....
2	(479,179)	(425,237)	(469,600)	(370,525)	....	....
3	(437,628)	(466,22)	(76,487)	(309,156)	....	....
4	...	...	...	...	....	....
...	...	...	...	...	....	....
512	...	...	...	...	....	....

   (g) These coordinate points, x and y are added and reduced to $[0, 255]$ in order to get a new random sequence for diffusion. Finally, this random sequence is diffused with the pixel values. Results of encryption are shown in Fig. 5.10. Fig. 5.10(a) shows the plain image, Fig. 5.10(b) shows the permuted image and Fig. 5.10(c) shows the encrypted image.

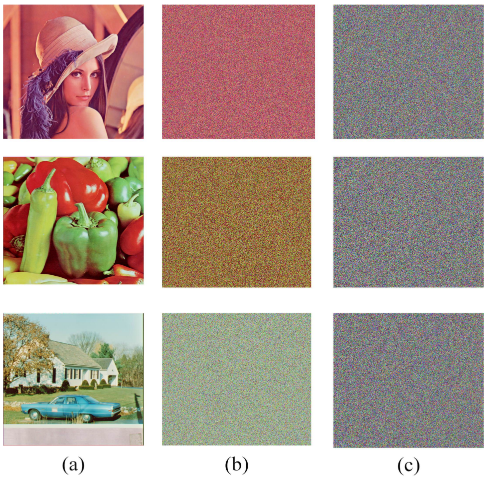


Fig. 5.10. Results of encryption process

5.1.2. Decryption process

1. Public key of B and private key of A and generator G is used to generate the random sequence using the chaotic sequence with ECC. This random sequence is diffused with the image.

2. It is followed by the diffusion using totalistic cellular automata.

3. The image is permuted to its original position using chaotic bit sequence and sorted index to get the original image I.

4. Results of decryption are shown in Fig. 5.11. Fig. 5.11(a) shows the encrypted images and Fig. 5.11(b) shows the decrypted images, respectively.

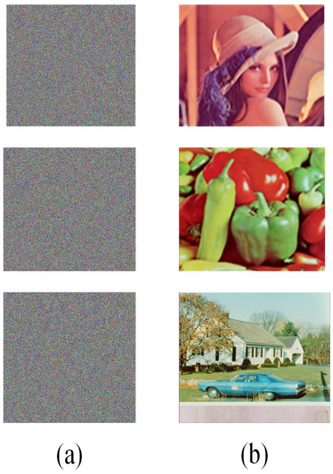


Fig. 5.11. Results of decryption process

6. RESULTS AND DISCUSSION

The hardness of the authentication system and simulation results of the color image with the performance of the encryption algorithm are evaluated and presented in this section. The simulation has been done using Matlab R2020a on 64 bit OS Windows 7 professional, Intel core i5-3380M processor with operating frequency 2.90GHz and 8GB RAM.

6.1. Analysis of authentication system

Hash is a one way function and its hardness towards the computation of the same hash value i.e., collision with the available hash value makes the system safer. The encryption function is hard as it uses the discrete logarithm problem to encrypt the hash value of the password.

The following subsections analyse the proposed cryptosystem using statistical and differential analyses to show the strength of the encryption.

6.2. Analysis of key space

In this algorithm, α and a_1 values are taken as keys for chaotic diffusion. Three different α and a_1 values are used as there are three different planes in the color image. For ECC encryption, it uses 16 bit key. If the floating point accuracy of the system is 10^{-15} then the key space is $10^{93} > 2^{100}$. Thus, the proposed encryption technique is strong enough to resist brute force attack.

6.3. Key sensitivity analysis

A small difference in the key should give a significant change in the encrypted image. The difference between the pixels of the encrypted image with the original key and the encrypted image with a very negligible change in the key gives a new scrambled image if they are completely different. If any negligible change in the key does not allow the decryption algorithm to decrypt the message, then the algorithm is said to be effective. key1 and key2 are changed by adding 0.0000001 and 0.0000002 to the keys, respectively. In Fig. 6.12, Fig. 6.12(a) presents plain image, Fig. 6.12(b) is the image encrypted with original key, Fig. 6.12(c) and Fig. 6.12(d) are images encrypted with slight change in the keys, Fig. 6.12(e) and Fig. 6.12(f) are the images obtained as a result of the difference between Fig. 6.12(b) & Fig. Fig. 6.12(c) and Fig. 6.12(b) & 6.12(d), respectively. In Fig. 6.13, Fig. 6.13(a) is the image decrypted with the original key whereas, Fig. 6.13(b) and Fig. 6.13(c) are the images decrypted with a slight change in the key.

6.4. Histogram analysis

The histogram is one of the analyses to test the resistivity towards statistical attack. It shows how pixel values in an image are distributed. If the graph shows the flat histogram then it is assumed that the algorithm can resist statistical attack. Fig. 6.14 shows the histogram of the plain image and the cipher image of Lena. Fig. 6.14(a), Fig. 6.14(c) and Fig. 6.14(e) are the histogram of the R, G and B planes of plain image whereas, Fig. 6.14(b), Fig. 6.14(d) and Fig. 6.14(f) are the histogram of the R, G and B planes of cipher image. The flat histogram of the cipher image in Fig. 6.14 conveys that the attack using the histogram is not possible.

6.5. Correlation coefficient analysis

The correlation coefficient ($Corr$) is used to determine the degree of connectivity between the pixels. If the $Corr$ value is nearer to 1, it shows the high similarity between the pixel values. If the $Corr$ value is nearer to 0, it shows less similarity between the pixel values. It is

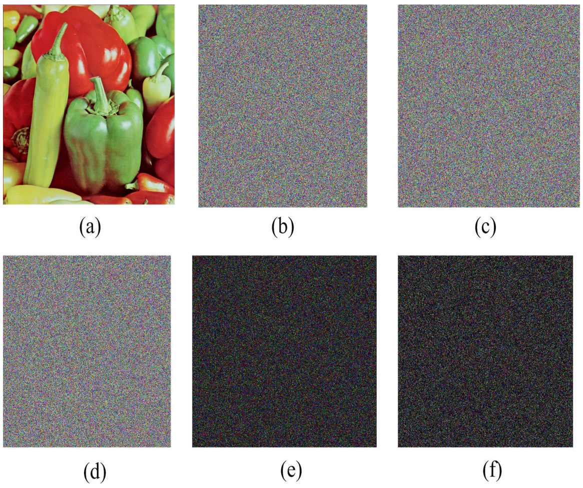


Fig. 6.12. Key Sensitivity results for encryption

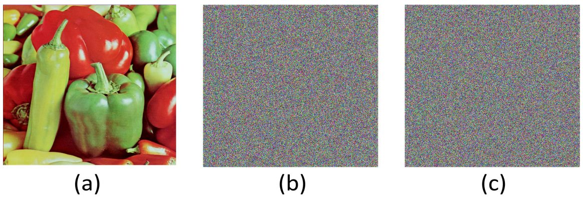


Fig. 6.13. Key Sensitivity results for decryption

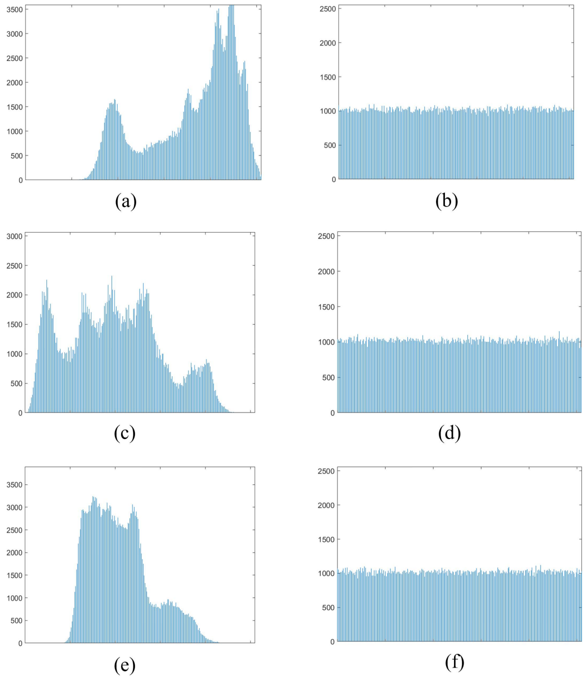
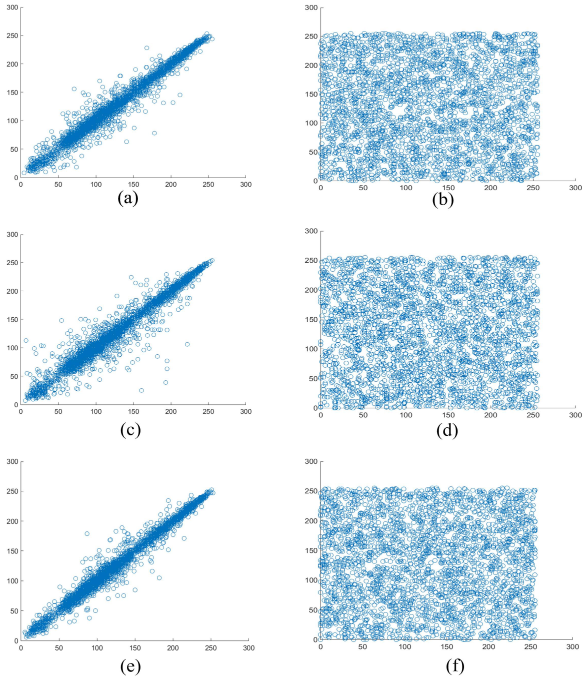


Fig. 6.14. Histogram of plain and cipher image

calculated using Eq. (6.11).

$$Corr = \frac{D_1((p - D_1(p))(q - D_1(q)))}{\sqrt{U_1(p)(U_1(q))}}, \tag{6.11}$$

where $D_1(p)$ and $U_1(p)$ are the p gray level expectation and variance. $Corr$ of the proposed ECF scheme is nearer to 0 and proves that the cipher has less similarity between adjacent pixel values. Fig. 6.15 shows the correlation distribution of Lena plain image and cipher image. Fig. 6.15(a), Fig. 6.15(c) and Fig. 6.15(e) are horizontal, vertical and diagonal correlation distribution of the plain image, respectively. Fig. 6.15(b), Fig. 6.15(d) and Fig. 6.15(f) are the horizontal, vertical and diagonal correlation distribution of cipher image, respectively. Table 6.4 conveys the correlation coefficient values of cipher image. Table 6.5 conveys the comparison of average correlation coefficient values of the proposed solution with the existing solutions. Lena image is taken for comparison. The obtained correlation coefficient values and correlation distribution in Fig. 6.15 conveys that the correlation between the adjacent pixel values is less.



(a) (b)

(c) (d)

(e) (f)

Fig. 6.15. Correlation distribution of plain and cipher image

Table 6.4. Correlation Co-efficient values for cipher images

Image	Horizontal	Vertical	Diagonal
Lena1	0.0014	0.0094	0.0042
peppers1	0.0097	0.0119	0.0051
house1	0.0053	0.0043	0.0035
boat1	0.0067	0.0042	0.0050
baboon1	0.0111	0.0059	0.0072

Table 6.5. Comparison of Correlation Co-efficient of Proposed with existing solutions

Encryption Scheme	Horizontal	Vertical	Diagonal
ECF	0.0014	0.0094	0.0042
[24]	0.0119	0.0087	0.0045
[40]	0.0082	0.0128	0.0012
[31]	0.0265	0.0044	0.0625

6.6. Entropy analysis

The quality of the confused image is determined by the entropy. If the entropy value is high, it means that the image is irregular. It is calculated using Eq. (6.12).

$$E(I) = \sum_{i=1}^{2N-1} p(I_i) \log_2 p(I_i), \tag{6.12}$$

where I is the image, N is the length of the pixel in binary, $p(I_i)$ denotes the probability of occurrence of I_i. Table 6.6 shows the Entropy values of the cipher image for all three planes. Table 6.7 compares the proposed entropy result with existing solutions and from the comparison, it is inferred that the proposed solution outperforms the existing solutions.

Table 6.6. Entropy analysis of proposed Solution

Image	plane	Entropy
Lena1	R G B	7.9994 7.9992 7.9993
Peppers1	R G B	7.9993 7.9993 7.9994
House1	R G B	7.9993 7.9993 7.9993
Boat1	R G B	7.9993 7.9993 7.9993
Baboon1	R G B	7.9993 7.9994 7.9993

6.7. Chi Square analysis

This is also one of the tests to analyse the distribution of pixel values in an image which can be calculated using Eq. (6.13).

$$\chi = \sum_{i=0}^{255} \frac{(c_i - c_0)^2}{c_0}, \qquad c_0 = (M \times N)/256, \tag{6.13}$$

where c_i and c_0 are the real and expected frequencies of pixel value i. Chi square value for $\alpha = 0.05$ is 293.24783. Table 6.8 shows the chi square value of the cipher images and all the values are less than 280. If the values are less than 293, the possibility of statistical attack is less.

Table 6.7. Comparison of Entropy value of proposed with existing solutions

Algorithm	plane	Entropy
ECF	R	7.9994
	G	7.9992
	B	7.9993
[24]	R	7.9892
	G	7.9902
	B	7.9896
[40]	R	7.9892
	G	7.9896
	B	7.9896
[30]	R	7.9972
	G	7.9972
	B	7.9976
[31]	R	7.9972
	G	7.9973
	B	7.9972
[22]	R	7.9874
	G	7.9872
	B	7.9866

Table 6.8. Chi square analysis of ECF

Image	Chi square value
Lena1	271.3691
Peppers1	272.7402
Baboon1	255.9316
House1	251.8164
Boat1	250.4531

6.8. Maximum deviation

This is a measure to convey the quality of the encryption which can be calculated using Eq. (6.14). For larger values of maximum deviation, the encryption is efficient. The deviation between the plain and ciphertext should be higher to ensure that the image is random and irregular.

$$ME = \frac{t_0 + t_{255}}{2} + \sum_{l=1}^{254} t_l \tag{6.14}$$

1. Histogram of plain image h_{ip} and cipher image h_{ic} is calculated.
2. The absolute difference of the cipher and plain histogram is the value t which is calculated using (6.15).
$$t = |h_{ip} - h_{ic}| \tag{6.15}$$
3. The difference value t with specified intensity is t_l.

6.9. Irregular deviation

This is a statistical measure of the uniform distribution of pixel values. If the irregular deviation is smaller, the uniformity in pixel distribution is high. It is calculated using the following steps,

1. The image p_n and its cipher c_n is subtracted and the absolute value d_n is calculated using (6.16).
$$d_n = |p_n - c_n| \tag{6.16}$$
2. The difference image d_n is used to find the histogram h_l using (6.17).
$$h_l = Histogram(d_n) \tag{6.17}$$
3. h_{avg} is calculated from each h_l and the total intensity value 256 using (6.18).
$$h_{avg} = \frac{1}{256}\sum_{l=0}^{255} h_l \tag{6.18}$$
4. IS_l is calculated using the absolute difference between the individual histogram and the the average value as given in (6.19).
$$IS_l = |h_l - h_{avg}| \tag{6.19}$$
5. The irregular deviation is calculated by IS_{avg} using Eq. (6.20).
$$IS_{avg} = \sum_{l=0}^{255} IS_l \tag{6.20}$$

The maximum and irregular deviation are tabulated in Table 6.9. The maximum deviation of the ECF cipher gives larger values and shows that the quality of encryption is high. Irregular deviation of the ECF cipher is lesser than maximum deviation which implies an equal distribution of pixel values.

Table 6.9. Maximum deviation and irregular deviation

Image	Maximum deviation	Irregular deviation		
		R	G	B
Lena1	352876	129498	160072	190006
peppers1	308224	174436	120152	122900
Baboon1	356369	166722	176616	148552
House1	516702	156870	145676	145726
Boat1	292957	186676	112830	110884

6.10. Deviation from uniform histogram

Deviation from uniform histogram is a measure to determine the uniformity in the distribution of pixel values. It is measured using Eq. (6.22) and the deviation values are tabulated in Table 6.10.

1. The ideal value calculated using the dimensions r and s of the image is Hj which is expressed in (6.21).
$$Hj = \frac{r \times s}{256} \tag{6.21}$$
2. Using Hj and the individual histogram value of the cipher HD_u, h_e is calculated.
$$h_e = \frac{\sum_{u=0}^{255} |HD_u - Hj|}{r \times s} \tag{6.22}$$

Table 6.10. Deviation from uniform histogram

Image	Deviation from uniform histogram		
	R	G	B
Lena1	0.0246	0.0253	0.0247
peppers1	0.0250	0.0245	0.0230
Baboon1	0.0249	0.0224	0.0250
House1	0.0265	0.0253	0.0261
Boat1	0.0251	0.0239	0.0239

6.11. Differential attack analysis

This is used to test the quality of diffusion by comparing two cipher images where one cipher produced using the original plain image, another cipher produced using single bit value change in the original plain image. This single bit value change should produce a vast difference in the cipher image. Number of pixel change rate (NPCR) and unified average changing intensity (UACI) are the measures used to determine the efficiency of the diffusion which are calculated using Eq. (6.23) and Eq. (6.24), respectively.

$$NPCR = \frac{1}{M_1 \times N_1} \sum_{i_1=0}^{M_1-1} \sum_{j_1=0}^{N_1-1} E_1(i_1, j_1) \times 100,$$
$$E_1(i_1, j_1) = \begin{cases} 1, & if D_a(i_1, j_1) \neq D_b(i_1, j_1) \\ 0, & otherwise \end{cases}, \tag{6.23}$$

$$UACI = \frac{1}{M_1 \times N_1} \sum_{i_1, j_1} \frac{|D_a(i_1, j_1) - D_b(i_1, j_1)|}{256} \times 100, \tag{6.24}$$

where D_a and D_b are cipher images with only single bit change. M_1 and N_1 are the image dimensions. NPCR and UACI values are tabulated in Table 6.11. Table 6.12 shows the comparison of NPCR and UACI values of proposed solution with existing solutions. For comparison, Pepper image is used and the results obtained convey that the proposed solution has high substitution efficiency than existing solutions.

Table 6.11. NPCR and UACI values

Image	Plane	NPCR	UACI
Lena1	R	99.6349	33.4528
	G	99.5815	33.4553
	B	99.6014	33.4137
Peppers1	R	99.6395	33.4835
	G	99.6098	33.5218
	B	99.6040	33.4457
House1	R	99.6193	33.4858
	G	99.5991	33.4465
	B	99.6113	33.4762
Baboon1	R	99.6189	33.4233
	G	99.6208	33.4453
	B	99.6151	33.4773
Boat1	R	99.6002	33.4625
	G	99.6063	33.4307
	B	99.6220	33.4085

Table 6.12. Comparison of Average NPCR and UACI value of ECF with existing solution

Algorithm	NPCR	UACI
ECF	99.6177	33.4836
[24]	99.61	32.20
[1]	99.62	28.62
[6]	99.29	33.18
[21]	99.63	31.87
[4]	99.60	33.45
[45]	99.58	33.44

6.12. Overall comparison using metrics

The image encryption scheme is compared with the available different encryption schemes in the literature. The correlation coefficient, entropy, NPCR and UACI are the metrics used for comparison in which the proposed scheme outperforms the encryption scheme already in existence. Few works perform well in the efficiency of substitution and lack in the correlation coefficient. Some of the works lack randomness and uniform distribution of pixel values. The proposed scheme has consistency in the performance and there is no skewed performance like performing well in one metric and very poor in another metric. Table 6.13 shows the comparison of the proposed scheme with the existing solution using the above mentioned metrics.

Table 6.13. Overall comparison of proposed solution with existing solutions using metrics

Algorithm	Correlation Coefficient			Entropy	NPCR	UACI
	H	V	D			
ECF	0.0014	0.0094	0.0042	7.9993	99.6177	33.4836
[24]	-0.0119	-0.0087	-0.0045	7.9896	99.61	32.20
[37]	0.0054	0.0064	0.0046	-	99.60	33.79
[10]	-	-	-	-	99.43	21.97
[36]	-0.0423	0.0202	0.0212	7.9974	99.55	33.61
[39]	-0.0331	0.0057	0.0169	7.9972	99.61	33.40
[11]	-0.0070	0.0151	0.0003	7.8963	99.60	33.36
[26]	0.0074	-0.0094	-0.0054	7.9992	99.61	33.46
[42]	0.0925	0.0430	0.0533	-	99.65	33.50
[41]	-0.0226	0.0041	0.0368	7.2072	99.61	33.53
[2]	-0.0061	0.0130	0.0017	7.9992	99.60	33.49

6.13. Overall comparison using features

The features compared are key derivation, strong diffusion, one time key and decryption complexity. Even though few encryption schemes have strong diffusion property and decryption complexity, it has drawback such as it does not use an adaptive key for each plain image. Encryption scheme [2] has all features like the adaptive key, strong diffusion and decryption complexity but its computational overhead is high as it uses both CA and DNA. The proposed encryption has all the features such as plain image related key, strong diffusion, high decryption complexity and less computational overhead. Table 6.14 compares the proposed scheme and the existing schemes using the features used for encryption.

Table 6.14. Overall comparison of proposed solution with existing solutions using features

Algorithm	Plain image related key	Strong diffusion	One time key	Decryption complexity
ECF	Yes	Yes	No	Initial key for chaos and a private keys for ECC
[24]	No	Yes	No	Initial key for chaos
[37]	No	Yes	No	Initial key for chaos
[10]	No	Yes	No	Non chaotic encryption
[36]	Yes	No	No	Initial key for chaos
[39]	No	No	No	Initial key for chaos
[11]	No	No	No	Initial key for chaos
[26]	No	Yes	No	Initial key for chaos using ECC
[42]	Yes	No	No	Initial key for chaos
[41]	Yes	No	No	Initial key for chaos
[2]	Yes	Yes	No	Initial key for chaos

7. CONCLUSION

The authentication system is proposed using SHA hash and Elgamal encryption scheme using the homomorphic property. The proposed ECF cryptosystem uses the logistic map to permute and diffuse the image. Three iterations of logistic map are used for each plane to improve the security. Initial values are derived from the image using Fourier transform based equation. The permutation is performed using bit values obtained from the chaos sequence. Additionally, sorting based chaotic permutation is also performed. Finally, the image is diffused using totalistic cellular automata and encrypted using elliptic curve encryption. The performance is analyzed using cipher image. Statistical and differential attacks can be reduced using the conversion of pixels with the random values obtained from ECC coordinates. Overall, the proposed system achieves better performance and has good resistance against statistical and differential attacks.

REFERENCES

[1] Çavuşoğlu, Ü., Kaçar, S., and Pehlivan, Ihsan & Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based s-box. *Chaos, Solitons & Fractals*, **95**:92–101.

[2] Chai, X., Gan, Z., Yang, K., and Chen, Yiran & Liu, X. (2017). An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and dna sequence operations. *Signal Processing: Image Communication*, **52**:6–19.

[3] Challa, S., Das, A. K., Odelu, V., Kumar, N., Kumari, S., and Khan, Muhammad Khurram & Vasilakos, A. V. (2018). An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. *Computers & Electrical Engineering*, **69**:534–554.

[4] Chen, J., Zhu, Z.-l., Zhang, L.-b., and Zhang, Yushu & Yang, B.-q. (2018). Exploiting self-adaptive permutation–diffusion and dna random encoding for secure and efficient image encryption. *Signal Processing*, **142**:340–353.

[5] Chuman, T. and Sirichotedumrong, Warit & Kiya, H. (2018). Encryption-then-compression systems using grayscale-based image encryption for jpeg images. *IEEE Transactions on Information Forensics and security*, **14**(6):1515–1525.

[6] Enayatifar, R. and Abdullah, Abdul Hanan & Isnin, I. F. (2014). Chaos-based image encryption using a hybrid genetic algorithm and a dna sequence. *Optics and Lasers in Engineering*, **56**:83–93.

[7] Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, **8**(06):1259–1284.

[8] Ge, R., Yang, G., Wu, J., Chen, Y., and Coatrieux, Gouenou & Luo, L. (2019). A novel chaos-based symmetric image encryption using bit-pair level process. *IEEE Access*, **7**:99470–99480.

[9] Hanif, M., Naqvi, R. A., Abbas, S., and Khan, Muhammad Adnan & Iqbal, N. (2020). A novel and efficient 3d multiple images encryption scheme based on chaotic systems and swapping operations. *IEEE Access*, **8**:123536–123555.

[10] Hasan, Fadhil Sahib & Saffo, M. A. (2020). Fpga hardware co-simulation of image encryption using stream cipher based on chaotic maps. *Sensing and Imaging*, **21**(1):1–22.

[11] Huang, L., Cai, S., and Xiong, Xiaoming & Xiao, M. (2019). On symmetric color image encryption system with permutation-diffusion simultaneous operation. *Optics and Lasers in Engineering*, **115**:7–20.

[12] Ibrahim, Saleh & Alharbi, A. (2020). Efficient image encryption scheme using henon map, dynamic s-boxes and elliptic curve cryptography. *IEEE Access*, **8**:194289–194302.

[13] Ibrahim, M. H., Kumari, S., and Das, Ashok Kumar & Odelu, V. (2018). Attribute-based authentication on the cloud for thin clients. *The Journal of Supercomputing*, **74**(11):5813–5845.

[14] Ibrahim, S., Alhumyani, H., Masud, M., Alshamrani, S. S., Cheikhrouhou, O., Muhammad, G., and Hossain, M Shamim & Abbas, A. M. (2020). Framework for efficient medical image encryption using dynamic s-boxes and chaotic maps. *IEEE Access*, **8**:160433–160449.

[15] Kumari, Saru & Renuka, K. (2020). A provably secure biometrics and ecc-based authentication and key agreement scheme for wsns. *International Journal of Communication Systems*, **33**(3):e4194.

[16] Kumari, S., Karuppiah, M., Das, A. K., Li, X., and Wu, Fan & Kumar, N. (2018). A secure authentication scheme based on elliptic curve cryptography for iot and cloud servers. *The Journal of Supercomputing*, **74**(12):6428–6453.

[17] Kumari, S., Li, X., Wu, F., Das, A. K., and Arshad, Hamed & Khan, M. K. (2016). A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps. *Future Generation Computer Systems*, **63**:56–75.

[18] Kumari, S., Li, X., Wu, F., Das, A. K., and Choo, Kim-Kwang Raymond & Shen, J. (2017). Design of a provably secure biometrics-based multi-cloud-server authentication scheme. *Future Generation Computer Systems*, **68**:320–330.

[19] Li, Peiya & Lo, K.-T. (2017). A content-adaptive joint image compression and encryption scheme. *IEEE Transactions on Multimedia*, **20**(8):1960–1972.

[20] Li, L., Xie, Y., Liu, Y., Liu, B., Ye, Y., Song, T., and Zhang, Yushu & Liu, Y. (2019). Exploiting optical chaos for color image encryption and secure resource sharing in cloud. *IEEE Photonics Journal*, **11**(3):1–12.

[21] Liao, X., Hahsmi, M. A., and Haider, R. . o. (2018). An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using dna and chaos. *Optik-International Journal for Light and Electron Optics*, **153**:117–134.

[22] Liu, H. and Wang, Xingyuan & Kadir, A. (2013). Color image encryption using choquet fuzzy integral and hyper chaotic system. *Optik-International Journal for Light and Electron Optics*, **124**(18):3527–3533.

[23] Liu, L. and Lei, Yuhang & Wang, D. (2020). A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation. *IEEE Access*, **8**:27361–27374.

[24] Liu, Qian & Liu, L. (2020). Color image encryption algorithm based on dna coding and double chaos system. *IEEE Access*, **8**:83596–83610.

[25] Liu, X., Xiao, D., and Huang, Wei & Liu, C. (2019). Quantum block image encryption based on arnold transform and sine chaotification model. *Ieee Access*, **7**:57188–57199.

[26] Liu, Z. and Xia, Tiecheng & Wang, J. (2018). Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and menezes–vanstone elliptic curve cryptosystem. *Chinese Physics B*, **27**(3):030502.

[27] Lorenz, E. N. (1963). The mechanics of vacillation. *Journal of Atmospheric Sciences*, **20**(5):448–465.

[28] Luo, Y., Ouyang, X., and Liu, Junxiu & Cao, L. (2019a). An image encryption method based on elliptic curve elgamal encryption and chaotic systems. *IEEE Access*, **7**:38507–38522.

[29] Luo, Y., Ouyang, X., and Liu, Junxiu & Cao, L. (2019b). An image encryption method based on elliptic curve elgamal encryption and chaotic systems. *IEEE Access*, **7**:38507–38522.

[30] Mollaeefar, M. and Sharif, Amir & Nazari, M. (2017). A novel encryption scheme for colored image based on high level chaotic maps. *Multimedia Tools and Applications*, **76**(1):607–629.

[31] Niyat, A. Y. and Moattar, Mohammad Hossein & Torshiz, M. N. (2017). Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Optics and Lasers in Engineering*, **90**:225–237.

[32] Ping, P., Fu, J., Mao, Y., and Xu, Feng & Gao, J. (2019). Meaningful encryption: generating visually meaningful encrypted images by compressive sensing and reversible color transformation. *IEEE Access*, **7**:170168–170184.

[33] Ramli, K., Suryanto, Y., and Hayati, N. . o. (2020). Novel image encryption using a pseudoset generated by chaotic permutation multicircular shrinking with a gradual deletion of the input set. *IEEE Access*, **8**:110351–110361.

[34] Rohith, S. and Bhat, KN Hari & Sharma, A. N. (2014). Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of linear feedback shift register. In *International Conference on Advances in Electronics Computers and Communications*, pages 1–6. IEEE.

[35] Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., and Kumar, Neeraj & Vasilakos, A. V. (2017). On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services. *IEEE Access*, **5**:25808–25825.

[36] Sambas, A., Vaidyanathan, S., Tlelo-Cuautle, E., Abd-El-Atty, B., Abd El-Latif, A. A., Guillén-Fernández, O., Hidayat, Y., and Gundara, G. . o. (2020). A 3-d multi-stable system with a peanut-shaped equilibrium curve: Circuit design, fpga realization, and an application to image encryption. *IEEE Access*, **8**:137116–137132.

[37] Souyah, Amina & Faraoun, K. M. (2016). An image encryption scheme combining chaos-memory cellular automata and weighted histogram. *Nonlinear Dynamics*, **86**(1):639–653.

[38] Wang, N., Di, G., Lv, X., Hou, M., Liu, D., and Zhang, Jun & Duan, X. (2019). Galois field-based image encryption for remote transmission of tumor ultrasound images. *IEEE Access*, **7**:49945–49950.

[39] Wang, X. and Wang, Qian & Zhang, Y. (2015). A fast image algorithm based on rows and columns switch. *Nonlinear Dynamics*, **79**(2):1141–1149.

[40] Wu, X., Wang, K., Wang, X., and Kan, Haibin & Kurths, J. (2018). Color image dna encryption using nca map-based cml and one-time keys. *Signal Processing*, **148**:272–287.

[41] Xu, L., Gou, X., and Li, Zhi & Li, J. (2017). A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. *Optics and Lasers in Engineering*, **91**:41–52.

[42] Ye, G.-D., Huang, X.-L., and Zhang, Leo Yu & Wang, Z.-X. (2017). A self-cited pixel summation based image encryption algorithm. *Chinese Physics B*, **26**(1):010501.

[43] Zhang, M., Tong, X.-J., Liu, J., Wang, Z., Liu, J., and Liu, Baolong & Ma, J. (2020). Image compression and encryption scheme based on compressive sensing and fourier transform. *IEEE Access*, **8**:40838–40849.

[44] Zhang, Z., Qi, Q., Kumar, N., and Chilamkurti, Naveen & Jeong, H.-Y. (2015). A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography. *Multimedia Tools and Applications*, **74**(10):3477–3488.

[45] Zhen, P., Zhao, G., and Min, Lequan & Jin, X. (2016). Chaos-based image encryption scheme combining dna coding and entropy. *Multimedia Tools and Applications*, **75**(11):6303–6319.

[46] Zhou, G., Zhang, D., Liu, Y., and Yuan, Ying & Liu, Q. (2015). A novel image encryption algorithm based on chaos and line map. *Neurocomputing*, **169**:150–157.