Journal of Theoretical and Applied Information Technology
15th May 2024. Vol.102. No 9
© Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COLOR IMAGE ENCRYPTION BASED ON ARNOLD CAT MAP- ELLIPTIC CURVE KEY AND A HILL CIPHER

DESAM VAMSI[1], PRADEEP REDDY CH[2]
[1]School of Computer Science and Engineering, VIT-AP University, AP, India.
[2]School of Computer Science and Engineering, VIT-AP University, AP, India.
E-mail: [1]d.vamsi1@gmail.com, [2]pradeep.ch@vitap.ac.in

ABSTRACT

The role of Image encryption in communication over the internet is gaining a lot of interest in recent days with the increased use of the internet. Transfer of crucial images over the internet is prone to attack and stealing when shared on an unsecured medium. To avoid these attacks and theft of image data, encryption is the best process to be used. In this paper, a novel approach of sub- image shuffled Arnold cat followed by an elliptic curve is used for encryption and decryption. The RGB planes of the color image are extracted, and each plane is divided into four sub-images that undergo the Arnold cat transformation that effectively scrambles and shuffles the image values, and four sub-images are combined back. The Arnold transformed RGB planes are combined into a single image that is further processed with an Elliptic curve key to compute a self-invertible key matrix and perform Hill cipher operation for encryption and decryption. The proposed method generates good quality cipher images with an entropy value of 7.9, low correlation, and can resist statistical and differential attacks.

Keywords: *Encryption, Arnold Cat, Elliptic Curve, Self-Invertible Key Matrix, Hill Cipher, RGB Planes*

1. INTRODUCTION

The means of communication have changed drastically over the years due to significant advancements in internet technology. Moreover, digital media transmission such as text, audio, and video files has become easier and more convenient. This has improved the lifestyle of people; however, these advancements also bring various threats. Once the information is transmitted digitally on the internet, it may encounter internet security threats such as hacking, malicious software, and identity threats.

Cryptography [1] is the practice of encrypting information to make it unintelligible to unauthorized individuals. Cryptography relies on mathematical principles, particularly number theory and arithmetic, to establish authenticity, integrity, and confidentiality for messages under specific circumstances. Its primary objective is to safeguard information during transmission, making it inaccessible to unauthorized individuals and preventing unauthorized tampering or interception. It is imperative to acknowledge that cryptography does not possess a singular universal technique for message encryption. Rather, there exist numerous approaches, each with its own set of benefits and drawbacks. Presently, the most prevalent encryption methods are symmetric and asymmetric key cryptography.

In Symmetric cryptography, a secret key is used for encryption (single key), examples are AES, Triple DES, DES, and IDEA. In asymmetric cryptography two keys are used for encryption (public, secret key), examples are RSA, ECC, DSA, and homomorphic [35]. Various cryptographic techniques are used to encrypt data which are in different formats like text [2,3,4], image [5,6,7,13,15], video [8,9], and audio [10,11] files.

Digital images have become increasingly important, as a type of data often containing sensitive information such as fingerprints, medical scan reports, pattern recognition, satellite military imagery, and more. As a result, there is a growing need to protect these images from access highlighting the importance of implementing image security measures. Notably, researchers have focused on image encryption due to its challenges compared to encrypting text. These challenges arise from the characteristics specific to images, including their data capacity and the presence of correlations between adjacent pixels. Due to these properties, encryption methods such as AES, DES, 3DES, and RSA are not well suited for encrypting the images effectively. To effectively address this problem, it is recommended to encrypt an image by transforming it from a coherent, understandable image into an incomprehensible, encrypted version using two distinct processes: confusion and diffusion.

In today's digital landscape, many image encryption techniques leverage the unique properties of chaotic maps and systems. These properties encompass essential characteristics like non-periodicity, ergodicity, and a strong sensitivity to initial conditions and control parameters. Notably, even minor adjustments to these parameters can lead to significant differences in the output of a chaotic map. Chaotic dynamical systems fall into two primary categories, namely, continuous, and discrete systems. Discrete systems are composed of various chaotic maps that operate iteratively, whereas continuous chaotic are dynamical systems that are described using differential equations.

Within the realm of chaotic systems, they can be further classified into two categories, namely, one-dimensional, and high-dimensional systems. One-dimensional chaotic systems are characterized by having just one or a few parameters, making them relatively simple to implement. However, using a one-dimensional chaotic system has limitations. If any of its variables are compromised, the predictability of its chaotic behavior increases, and it operates within a restricted range. Therefore, one-dimensional chaotic systems may not always be the most suitable choice for image encryption.

On the other hand, high-dimensional chaotic maps involve at least two or more variables and exhibit a higher degree of complexity. This increased complexity makes their behavior significantly more challenging to predict, even if one of the variables is compromised. Consequently, high-dimensional chaotic maps offer enhanced security performance when compared to their one-dimensional counterparts**.**

1.1 Present problem statement:

The implementation of the novel algorithm in this paper uses an Elliptic curve (EC), shuffled Arnold cat map and hill cipher. Figure 1 represents the block diagram of the novel algorithm. Initially separate the R, G, and B channels from the original 256*256-pixel color image (I_{RGB}). Then divide each channel into four equal sub-images. Perform the Arnold cap map function on each sub-image and reconstruct the sub-images into single planes. The obtained three planes are reconstructed into one image (Arn_{RGB}) and perform shuffle operation the obtained image is stored in As_{RGB}. Later perform a hill cipher operation with a self-invertible matrix which is generated from ECC keys. Finally, the encrypted image (Ash_{RGB}) is obtained, and it is resistant to several attacks.

2. LITERATURE SURVEY

The authors in [12] present an innovative 2-D trigonometric mapping technique, highlighting its chaotic characteristics. The authors employed established dynamic analysis tools such as bifurcation diagrams, phase space trajectories, and Lyapunov exponent to demonstrate the chaotic nature of the map. Additionally, they established that the mapping exhibits an infinite equilibrium point. The proposed encryption/decryption scheme for color images incorporates four key components: the aforementioned trigonometric map, the Mandelbrot Set, the Bit-XOR operation, and a new Conditional shift operation. The focus of the paper [12], centers around the introduction of a chaotic-cryptographic system designed to effectively counter various forms of intrusions while simultaneously improving the Shannon entropy measure of the cipher images.

The author in [14] introduces a novel approach to encrypt and decrypt the data in different formats like text, image, and sound using a fractional order Rossler chaotic system. At the outset, a Master-Slave synchronization mechanism is developed for the fractional-order Rossler utilizing Lab view, enabling the encryption and decryption processes. Equations for the Master-Slave mechanism of fractional-order Rossler are formulated to facilitate synchronization. Subsequently, the designed fractional order Rossler chaotic system is employed for the encryption and decryption of image, sound, and text data separately.

In paper [5], a new image encryption method is introduced, utilizing a 2DSalomon map. This scheme incorporates a hyperchaotic map characterized by extensive randomness and a wide range. The system's exceptional performance is verified through various reliable metrics, including bifurcation analysis, Lyapunov exponent, phase space trajectory diagrams, Kolmogorov entropy, Shannon entropy, and correlation dimension. Through the integration of the 2D Salomon map, the image encryption method entails bit-level pixel splitting and subsequently disturbing the pixels while altering their values.

The paper [16] introduces a new 2D hyperchaotic system called the Schaffer map, tailored for applications that demand high complexity. Drawing inspiration from the Schaffer function, widely recognized as a benchmark in optimization due to its unique oscillation properties, this system is developed. The chaotic behavior of the 2D Schaffer map has been thoroughly assessed using various chaos indicators like sample entropy, Kolmogorov entropy, correlation dimension, Lyapunov exponent,0-1 test, permutation entropy, phase space trajectory, and bifurcation diagrams.

3. PRELIMINARIES

3.1. Arnold Cat Map

In 1968, V. Arnold discovered a system that performs stretch and fold mapping using the image of a cat. A matrix with determinant 1 is used for this 2D mapping which makes it reversible using inverse properties. The image is transformed using Arnold cat [17] mapping that generates a randomized image. If the mapping is iterated several times, the original image will finally appear again. Arnold's period is defined as the number of iterations required for the reconstruction of the original image through continuous mapping.

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = B \begin{bmatrix} X_m \\ Y_m \end{bmatrix} (mod\ M) = \begin{bmatrix} 1 & r \\ s & rs+1 \end{bmatrix} \begin{bmatrix} X_m \\ Y_m \end{bmatrix} (mod\ M) \qquad (1)$$

Where $det(B) = 1, r$ and s are the positive integers, and M is the image size. (X_m, Y_m) is the sample pixel position of the image size $M \times M$, $(X_m, Y_m), r, s \in \{0,1,2,3, \dots M-1\}$, (X', Y') is the new position obtained after performing Arnold transform.

This map performs the chaotic transformation using two factors namely tension (enlarging the coordinates $x\ and\ y$ using multiplication) and folds (constraining it to a unit matrix using mod). The pixels of the image are transformed using equation (1), the resultant image is called a scrambled image. While repeating the transformation process for certain iterations, the output image meets the expected result (i.e. until the secret key) the scrambled image will be obtained as per requested. The 2D chaotic Arnold's Cat Map is generated by interchanging the original image pixel positions without deleting any image data. The resultant chaotic image after certain random iterations includes all pixel values of the original image in random. So, the number of iterations depends on the parameters (r, s, and M) of the original image that are used as secret keys. The transformation of the Arnold is periodical in nature because the original image is obtained after a specific number of iterations. The time taken to transform the image for Arnold is given as:

$$Arnold\ Period = min[i: \{Arnold\ transform(f(X_m, Y_m), M)\}^i = f(X_m, Y_m)]$$

The image decryption process depends on the period of transformations. Here, (Arnold period – secret key) calculates the number of iterations involved in the decryption process.

3.2. *Elliptic Curve Definition*

$E_p(a, b)$ is the representation of an elliptic curve. Since p is a prime number, a and b are limited to mod p . $y^2 = x^3 + ax + b$ is the equation that represents the curve. Elliptic curves are not ellipses; however, the equation of elliptic curve can be understood as the result of calculating the elliptic curve's circumference, or as a cubic equation with a maximum degree of 3.

The Elliptic curve is symmetric. This yields a value of x represented as $\pm x$. Therefore, each curve demonstrates symmetry around $y = 0$. ECC can be characterized as an elliptic curve over Z_p (prime curve) and an elliptic curve over GF(2^m) (binary curve). The use of ECC [18] extends to key exchange and encryption.

The security of various elliptic curve ciphers is evaluated based on the number of points present in a finite abelian group defined over an elliptic curve. The number of points N in the instance of the finite group $E_p(a, b)$ is limited by: $p + 1 - \sqrt{p} \leq N \leq p + 1 + 2\sqrt{p}$

The number of elements in Z_p, or p elements, is roughly equal to the number of points in $E_p(a, b)$.

3.3. *Algorithm for Key Exchange Using Elliptic Curves in Diffie-Hellman Protocol*

ECDH, also known as Elliptic-curve Diffie–Hellman, is a protocol for key agreement. It enables two parties, each possessing an elliptic-curve public–private key pair, to establish a shared secret while transmitting in an unsecured channel. This shared secret can be utilized directly as a key or can be used to derive another key. Subsequent communications can then be encrypted using a symmetric-key cipher, with the key or derived key. ECDH is a variation of the Diffie–Hellman protocol [19] that incorporates EC cryptography.

Suppose sender C desires to establish a mutual key with receiver D, however, the sole communication channel accessible to them is susceptible to eavesdropping by an unauthorized third party. At first, consensus must be reached on the domain parameters, which include (p, a, b, G, n, h) in the prime case where, $a, b \in E_p(a, b)$, n is subgroup size, and ‘ h' is the cofactor.

In addition, it is essential for every party involved to possess a key pair that is appropriate for elliptic curve cryptography [20]. This key pair comprises a private key, denoted as $'d'$, which is a randomly chosen integer within the range of $[1, n-1]$. Furthermore, there is a corresponding public key represented by a point $'P'$, where $P = d.G$ is obtained by adding the point $'G'$ to itself $'d'$times. Before the execution of the protocol, it is essential for each party to possess knowledge of the other party's public key. The Sender key pair is denoted as (d_C , P_C), while the receiver key pair is represented as (d_D,P_D).

3.4. *Hill Cipher*

Lester Hill introduced the Hill cipher [21] in 1929 as a symmetric block cipher method. The encryption and decryption process are done by using the same key matrix. This technique assigns numerical values to each alphabet, where 'a' is represented as 0, 'b' as 1, 'c' as 2, and so forth, up to 'z' represented as 25. The plaintext is segmented into blocks of dimensions n×n, where n is determined by the size of the key matrix. For instance, if the key matrix (W) is 2×2, then each plaintext block (H_P) should also be 2×1 in size. Both matrices W and H_P are utilized in the encryption process, generating a ciphertext block (H_C) of dimensions 2×1 consisting of numeric values [22]. To decrypt the ciphertext, the receiver calculates the inverse of the key matrix (W), denoted as W^{-1}, where $W^{-1} \times W = I$ (Identity matrix).
The mathematical notation:
Encryption is,
$H_C = W \times H_P (mod 26)$, and
Decryption is,
$H_p = W^{-1} \times H_C (mod 26)$

Sender computes the point (x_k,y_k)= $d_C . P_D$
Receiver computes the point (x_k,y_k)=$d_D . P_C$

The symmetric key is derived from the x-coordinate of the point, which is denoted as X_k . Many standardized protocols that rely on the Elliptic Curve Diffie-Hellman (ECDH) utilize a hash-based key derivation function to generate this symmetric key.
The shared secret $X_k = (a, b)$ computed by both parties are identical, as

$$d_C . P_D = d_C . d_D . G = d_D . d_C . G = d_D . P_C$$

The sender initially reveals the public key, ensuring that no one else can discover the private key unless they can solve the discrete logarithm problem for an elliptic curve. The receiver’s private key has equal security. The shared secret key can only be computed by sender and receiver unless someone else can solve the Diffie-Hellman problem using elliptic curves.
Then X_1 and $X_2$are calculated as:

$$X_1 = a * G = (x_{11}, x_{12})$$
$$X_2 = b * G = (x_{21}, x_{22})$$

By applying the ECDH exchange protocol, the users C and D generate the keys X_1 and X_2.

3.5. *Generating Self-Invertible Matrix*

Encryption and decryption rely on the key matrix, and if the inverse of the key matrix does not exist, decryption becomes impossible. To address this issue a self-invertible matrix [23] is generated by taking the points from the Elliptic Curve Diffie-Hellman Key Exchange AlgorithmX_1 and X_2. The matrix $S_n (4 \times 4)$ is used by both the sender and receiver for encrypting and decrypting the image.

The self-invertible matrix is $S_n = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \\ x_{41} & x_{42} & x_{43} & x_{44} \end{bmatrix}$
It is subdivided as $S_n = \left[\begin{array}{c|c} S_{11} & S_{12} \\ S_{21} & S_{22} \end{array}\right]$
Where, $S_{11} = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$ and the values of S_{12} , S_{21},S_{22} of key matrix are generated as $S_{12} = I - S_{11}$, $S_{21} = I + S_{11}$, and$S_{11} + S_{22} = 0$, here$I$= identity matrix.
The pixels of the image (As$_{RGB}$) are segmented into blocks of size 4, where each block is transformed into a vector with dimensions 4 rows and 1 column (4×1). Subsequently, a multiplication operation is performed with the key

matrix $S_n(4 \times 4)$ for each vector. To get the encrypted vectors take modulo 256 and reconstruct the encrypted image from the vectors to send to the receiver.

4. PROPOSED METHOD

The implementation of the novel algorithm in this paper uses an Elliptic curve (EC), shuffled Arnold cat map, and hill cipher. Initially separate the R, G, B channels from the original color image (I_{RGB}) with 256×256 pixels. Then divide each channel into four equal sub-images. Perform the Arnold cap map function on each sub-image and reconstruct the sub-images into single planes. The obtained three planes are reconstructed into one image (Arn_{RGB}) and perform shuffle operation the obtained image is stored in As_{RGB}. Later perform a hill cipher operation with a self-invertible matrix which is generated from ECC keys. Finally, the encrypted image (Ash_{RGB}) is obtained, and it is resistant to several attacks.

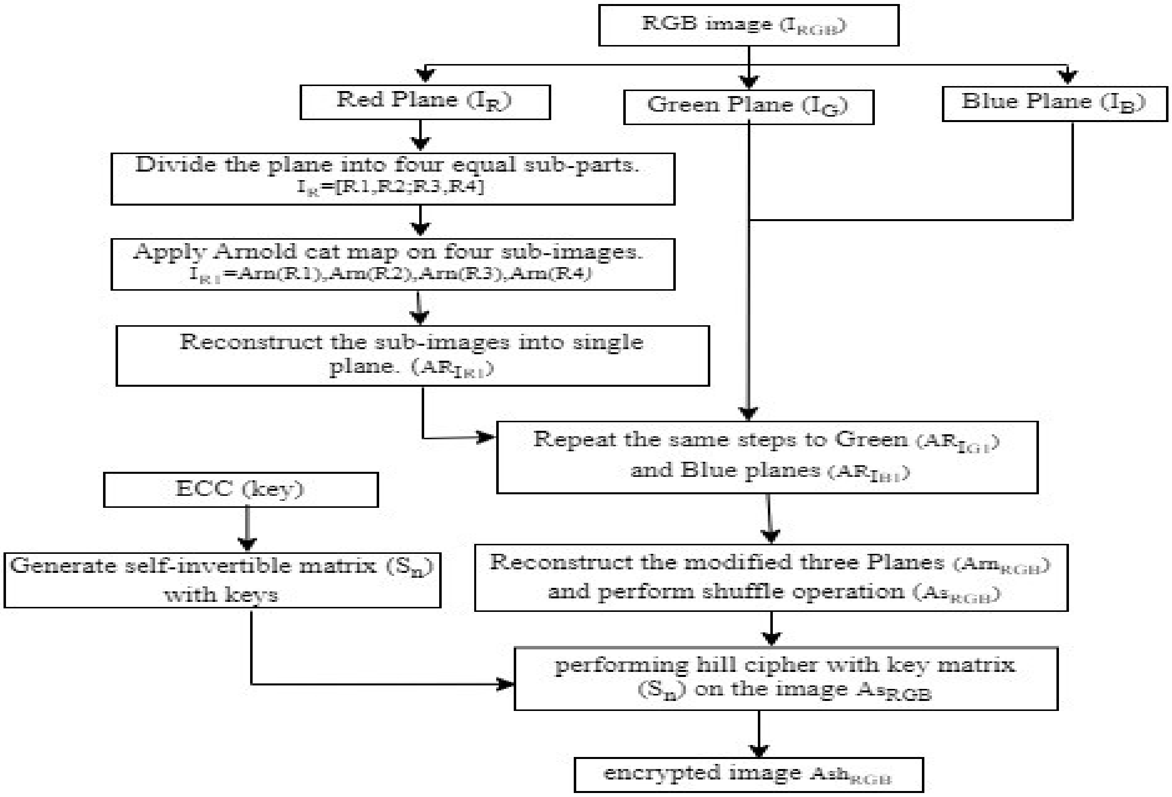

RGB image (I_{RGB})
Red Plane (I_R)
Green Plane (I_G)
Blue Plane (I_B)
Divide the plane into four equal sub-parts.
I_R=[R1,R2;R3,R4]
Apply Arnold cat map on four sub-images.
I_{R1}=Arn(R1),Arn(R2),Arn(R3),Arn(R4)
Reconstruct the sub-images into single plane. (AR_{IR1})
Repeat the same steps to Green (AR_{IG1}) and Blue planes (AR_{IB1})
ECC (key)
Generate self-invertible matrix (S_n) with keys
Reconstruct the modified three Planes (Arn_{RGB}) and perform shuffle operation (As_{RGB})
performing hill cipher with key matrix (S_n) on the image As_{RGB}
encrypted image Ash_{RGB}

Figure 1: Flowchart of proposed encryption algorithm

4.1. Proposed Algorithm

Step 1: Select an image (I) of size (m, n, 3)
Step 2: Separate the image to planes R, G, B. Where, I->I_R, I_G, I_B
Step 3: For each plane I_R, I_G, I_B
Divide the plane into four sub-images, where
I_R = [R1, R2; R3, R4]
I_G = [G1, G2; G3, G4]
I_B = [B1, B2; B3, B4]
Step 4: Apply the Arnold cat map on the four sub-images of each plane.
I_{R1} =Arn(R1),Arn(R2),Arn(R3),Arn(R4)
I_{G1}=Arn(G1),Arn(G2),Arn(G3),Arn(G4)
I_{B1}= Arn(B1),Arn(B2),Arn(B3),Arn(B4)
Step 5: Reconstruct the Arnold mapped sub-images into single planes of I_{R1}, I_{G1}, I_{B1}.
For each plane I_{R1}, I_{G1}, I_{B1}.
$AR_{I_{R1}}$= [Arn(R1),Arn(R2);Arn(R3),Arn(R4)]
$AR_{I_{G1}}$= [Arn(G1),Arn(G2);Arn(G3),Arn(G4)]
$AR_{I_{B1}}$= [Arn(B1),Arn(B2);Arn(B3),Arn(B4)]

Step 6: Reconstruct the modified three planes R, G, B into a single image.

Arn$_{\text{RGB}}$= [$AR_{I_{R1}}$, $AR_{I_{G1}}$,$AR_{I_{B1}}$]

Step 7: Shuffle the image (Arn$_{\text{RGB}}$) to obtain As$_{\text{RGB}}$. Randomly, shuffle the linear indexes of images into 1 to m*n, and rearrange the shuffled index into original rows and columns of Arn$_{\text{RGB}}$ to obtain As$_{\text{RGB}}$.
Wa=Arn$_{\text{RGB}}$; Si=size (Wa)
Pa=reshape (randperm (numel (Arn$_{\text{RGB}}$)),Si)
As$_{\text{RGB}}$= Wa(Pa)

Step 8: Generate a self-invertible matrix (4*4) from the EC keys.

Step 9: Perform hill cipher operation with the self-invertible matrix and shuffled Arnold image (As$_{\text{RGB}}$).
Step 10: The final encrypted image Ash$_{\text{RGB}}$ is obtained.

4.2. Algorithm Divide

In step 3 the division operation is performed as:

```
Procedure: Div (image I)
Input: image I of size (m, n, 3)
Output: Each plane is divided into four sub-images
Initiate: $I_R = (m, n, 1)$
          $I_G = (m, n, 2)$
          $I_B = (m, n, 3)$
For every channel $I_R, I_G, I_B$
$R_1 = I_R(1{:}m/2\,,1{:}n/2\,,1)$
$R_2 = I_R(1{:}m/2\,,n/2+1{:}n,1)$
$R_3 = I_R(m/2+1{:}m,,1{:}n/2\,,1)$
$R_4 = I_R(m/2+1{:}m,n/2+1{:}n,1)$
$G_1 = I_G(1{:}m/2\,,1{:}n/2\,,2)$
$G_2 = I_G(1{:}m/2\,,n/2+1{:}n,2)$
$G_3 = I_G(m/2+1{:}m,,1{:}n/2\,,2)$
$G_4 = I_G(m/2+1{:}m,n/2+1{:}n,2)$
$B_1 = I_B(1{:}m/2\,,1{:}n/2\,,3)$
$B_2 = I_B(1{:}m/2\,,n/2+1{:}n,3)$
$B_3 = I_B(m/2+1{:}m,,1{:}n/2\,,3)$
$B_4 = I_B(m/2+1{:}m,n/2+1{:}n,3)$
End
```

5. ANALYSIS OF SECURITY AND EFFICIENCY

The simulations of the proposed image encryption method are implemented in MATLAB R2019a with a 2.40GHz Intel® Core™ i7 processor with USC-SIPI database [24] color images with 256*256 size. The images that are used in the simulation are "Female", "Couple", "House", "Tree", "Lena"," Mandrill", and "Peppers" as shown in Figure 2.

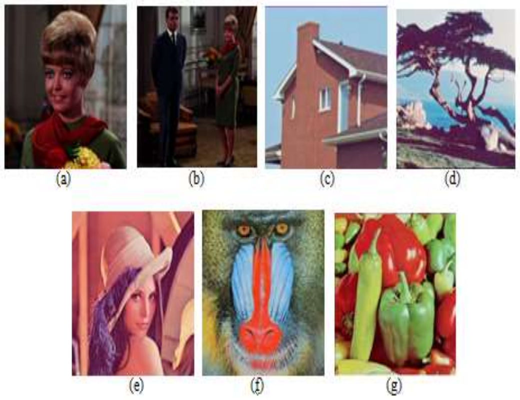


Figure2.Plain images (a) "Female", (b) "Couple", (c) "House", (d) "Tree", (e) "Lena", (f) "Mandrill", (g) "Peppers"

5.1 Histogram analysis and chi-square analysis

Histogram and Chi-square are two commonly known techniques used to test the robustness of a cryptosystem against unauthorized access (third parties). In this context, uniform distribution of pixels is the characteristic of encrypted data, whereas the pixels in original data are non-uniformly distributed. Figure 3 shows the histograms of the output images which indicate a uniform distribution, while the histograms of input images are completely distinct from the ones seen before. This uniformity is further verified through Chi-square analysis [25]. Table 1 presents the Chi-square results, which include their corresponding p-values, considering a significance level of 0.05 for the histograms of the cipher images. A valid Chi-square (i.e., a uniform histogram) is obtained if the score obtained is less than $\chi 2^{th}(255,\ 0.05) = 291.2546$, this indicates the corresponding p-value is greater than 0.5. As per the result presented in Table 1, the histograms of the images that are encoded exhibit the characteristics of uniformity in the pixel distribution. This provides evidence that the crypto-system under analysis can resist any form of histogram-based attack.

5.2. Entropy Analysis

A system's information entropy is a numerical measure of uncertainty and irregularity concerning the original structure of data. In Table 2 the average entropy of cipher image (RGB) is shown, and the result makes it clear that the proposed encryption method produces extremely random cipher images.
The entropy $H(E)$of a source E:

$$H(E) = \sum_{i=0}^{w} P(x_i).log2\ \frac{1}{P(x_i)} \qquad (2)$$

Where x_i is the gray level with the probability of $P(x_i)$. The average of three channels entropy values of the images are shown in Table 2 which are near to 8. The comparison is given in Table 3 which shows that our method is better than the methods [26] [27]. Color images encrypted with proposed algorithm are seen to exhibit a high degree of randomness.

Table 1: Chi-square test of the histogram

Image	Components	χ2-test	
		Score	Result
Female	R	292.254	Pass
	G	258.358	Pass
	B	245.966	Pass
Couple	R	237.458	Pass
	G	264.357	Pass
	B	225.684	Pass
House	R	235.145	Pass
	G	228.624	Pass
	B	248.259	Pass
Tree	R	275.568	Pass
	G	214.456	Pass
	B	258.268	Pass
Lena	R	278.365	Pass
	G	258.358	Pass
	B	247.685	Pass
Mandrill	R	258.568	Pass
	G	275.689	Pass
	B	238.458	Pass
Peppers	R	268.745	Pass
	G	277.235	Pass
	B	283.568	Pass

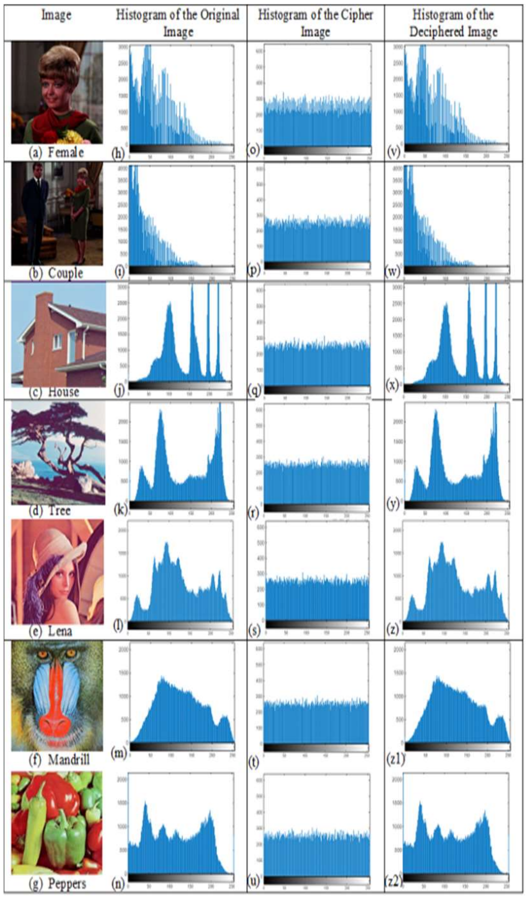
Table 2: Entropy of cipher images

Image	Cipher image Entropy$_{avg}$
Female	7.9985
Couple	7.9965
House	7.9875
Tree	7.9978
Lena	7.9989
Mandrill	7.9982
Peppers	7.9794

Table 3: Comparison of encrypted Lena image entropy values with proposed algorithm and algorithms in [26] [27]

Methods	Entropy$_{avg}$
Proposed	7.9989
[26]	7.9957
[27]	7.9973
[34]	7.9986

Figure 3: (a)-(g) Original Images; (h)-(n) Histograms of original images;(o)-(u) Histograms of cipher images;(v)-(z2) Histograms of deciphered images



5.3. Correlation Analysis

When the correlation is minimized, the cryptosystem can resist statistical intrusion. The equations to achieve correlation values are:

$$Cor_{pq} = \frac{E\{[p - E(p)] \quad [q - E(q)]\}}{\sqrt{F(p)}\sqrt{F(q)}}$$

$$with \quad E(p) = \frac{1}{N}\sum_{i=1}^{N} p_i$$

$$and \quad F(p) = \frac{1}{N}\sum_{i=1}^{N}[p_i - E(p)]^2 \qquad (3)$$

The variables p and q represent the pixel values found at corresponding positions in images I and I`. The variances $E(p)$ and $F(p)$ along with N representing the total pixel count, are crucial in computing correlation coefficients. These coefficients, obtained for the color images randomly selecting 2000 pairs of adjacent pixels in the horizontal (H), vertical (V), and diagonal (D) directions for R, G, B planes are organized in Table 4. The comparisons with other algorithms are shown in Table 5. Simultaneously, Figure 4 provides an overview of the distribution of neighboring pixels of “Lena” image. Upon examination of Figure 4, it becomes evident that minimal correlation values are achieved in three directions: vertical, horizontal, and diagonal. This observation is significant as it underscores the encryption scheme's resilience against potential attackers, particularly in terms of the correlation coefficient. Essentially, the encryption scheme proves highly secure due to the minimal correlations among neighboring pixels, making it exceptionally challenging for attackers to decipher the information based on correlation analysis.

Figure 4. Correlation distribution of plain and cipher image of “Lena”.

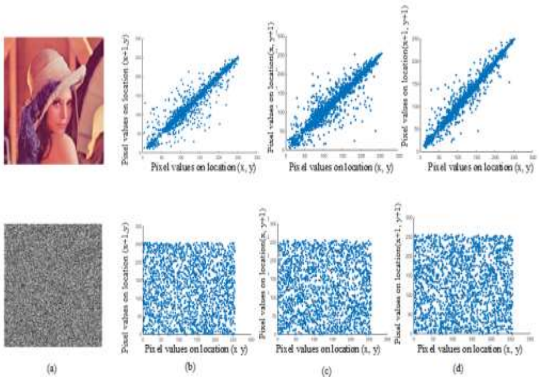


Table 4. Correlation coefficients of test images

Image	Direction	R	G	B
Female	H	-0.0023	0.0020	-0.0041
	V	-0.0013	0.0019	0.0021
	D	0.0024	-0.0013	-0.0009
Couple	H	-0.0054	-0.0028	0.0010
	V	-0.0027	0.0008	-0.0005
	D	0.0019	0.0020	-0.0026
House	H	-0.0047	-0.0010	0.0013
	V	-0.0028	-0.0005	-0.0024
	D	0.0016	0.0026	0.0027
Tree	H	-0.0034	-0.0013	-0.0019
	V	-0.0026	0.0022	0.0013
	D	-0.0031	-0.0007	-0.0027
Lena	H	0.0015	-0.0024	-0.0019
	V	0.0012	0.0031	-0.0027
	D	-0.0035	-0.0008	0.0008
Mandrill	H	-0.0028	-0.0029	0.0019
	V	-0.0027	-0.0021	-0.0032
	D	-0.0018	0.0015	-0.0005
Peppers	H	-0.0032	-0.0021	0.0024
	V	0.0017	-0.0006	0.0031
	D	-0.0024	-0.0018	-0.0007

Table 5: Correlation coefficient comparison of Lena image with proposed algorithm and algorithms in [26] [27] [28].

Image	Direction	R	G	B
Proposed	H	0.0015	-0.0024	-0.0019
	V	0.0012	0.0031	-0.0027
	D	-0.0035	-0.0008	0.0008
[26]	H	- 0.0095	-0.0055	0.0015
	V	- 0.0009	0.0025	- 0.0021
	D	- 0.0074	0.0011	- 0.0018
[27]	H	- 0.0029	0.0039	- 0.0037
	V	0.0001	-0.0005	0.0003
	D	0.0002	-0.0045	0.0018
[28]	H	0.0111	- 0.0132	- 0.0016
	V	- 0.0109	0.0175	0.0025
	D	- 0.0101	0.0021	0.0150

5.4. NPCR and UACI Analysis

NPCR and UACI are the primary measures used to certify whether a cryptosystem can resist differential attacks [29]. NPCR calculates the proportion of pixels with different intensities between two cipher images of $\mathrm{B}_1(i,j)$ and $\mathrm{B}_2(i,j)$,whereas UACI calculates the average intensity of difference between the encrypted versions of B_1 and B_2.

$$NPCR_{RGB} = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} Q_{RGB}\,(i,j) \times 100 \qquad (4)$$

$$Q_{RGB}(i,j) = \begin{cases} 0 \ if \ B_1(i,j) = B_2(i,j) \\ 1 \ if \ B_1(i,j) \neq B_2(i,j) \end{cases}$$

$$UACI_{RGB} = \frac{1}{M\times N\times 255}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|B_1(i,j) - B_2(i,j)| \times 100 \qquad (5)$$

NPCR and UACI values range from 0 to 100. An effective cryptosystem is expected to aim for an NPCR close to 100%. Generally, the UACI for well-designed encryption algorithms is around 33.6% [30]. In Table 6, the average of three channels NPCR and UACI values for the images are obtained by modifying the data at distinct positions. In Table 7, the comparisons with other algorithms are shown. Based on these results, the proposed encryption algorithm is highly secure and unbreakable.

Table 6: NPCR and UACI values.

Image	$NPCR_{avg}$	$UACI_{avg}$
Female	99.6541	33.4572
Couple	99.6124	33.3845
House	99.6421	33.4186
Tree	99.5024	33.5112
Lena	99.7834	33.4875
Mandrill	99.6127	33.4271
Peppers	99.6387	33.4023

Table 7: NPCR and UACI values comparison with other algorithms.

Image	$NPCR_{avg}$	$UACI_{avg}$
Proposed	99.7892	33.4875
[26]	99.7566	32.6766
[27]	99.6129	33.4627
[28]	99.6102	33.4675
[34]	99.7862	34.6213

5.5. PSNR

Assessing the algorithm's performance involves a comparison of distortion between the original image with both encrypted and decrypted image. The measurement used to play out this encryption quality check is PSNR.

$$PSNR = 10\ log_{10} \frac{{MAX_H}^2}{MSE} \quad (6)$$

$$MSE = \frac{1}{M \times N} \sum_{r=1}^{M} \sum_{s=1}^{N} (R(r,s) - R'(r,s))^2 \ (7)$$

where $\mathrm{R}(\mathrm{r},\mathrm{s})$ and $\mathrm{R}'(\mathrm{r},\mathrm{s})$ are the original and encrypted image pixel values, *MSE* is mean square error. In Table 8, the PSNR values are less for the encrypted image, it shows that our algorithm has high performance.

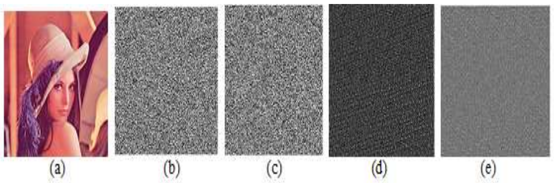
Table 8: PSNR values

Image	PSNR
Female	8.2541
Couple	8.3554
House	8.5746
Tree	8.3524
Lena	8.2875
Mandrill	8.3654
Peppers	8.3564

5.6. Key space and Sensitive Analysis

The effectiveness of image encryption scheme depends on the robust security level of the secret key. In order to ensure protection from brute-force attacks, the size of the key must be larger than 2^{100}. Our proposed technique has a secret key with a length of 256 bits, which is efficient to protect from brute-force attacks. Furthermore, the secret key demands an elevated sensitivity to changes in its values to avert any attempts at size reduction. To measure the sensitivity of key we generate key(K1) and modify one bit to get the key value (K2). Encrypting the same image with both K1 and K2 allows us to compare the results. The findings, illustrated in Figure 5, show that the ciphered images D1 and D2 using K1 and K2 exhibit dissimilarity. Notably, decrypting C1 using K2 results in a random-like image. These outcomes emphasize the high security and sensitivity of the secret key in our proposed encryption scheme, ensuring robust protection against potential attacks.

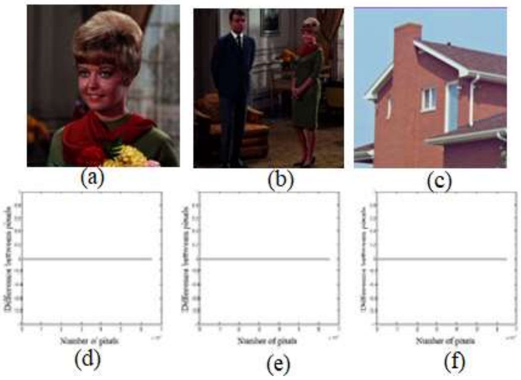
Figure 5: a) The plain "Lena" image; b) using K1 the obtained cipher image D1; c) using K2 the obtained cipher image D2; d) D1-D2; e) using K2 the deciphering image.



5.7. Image restoration

Upon completing the decryption process, an image restoration technique is implemented to scale whether the cipher image is accurately decrypted without losing any data. In Figure 6, the X-axis stores the values of image pixels, and the y-axis stores the values which are difference between corresponding pixels of the plain and decrypted image. Figure 6 illustrates that both decrypted and original or plain images ("Female", "Couple" and "House") are lookalike by plotting restoration results.

Figure 6: Image restoration of images a) Female, b) Couple, c) House



5.8. Noise and data Loss

During the transmission of ciphered images, there are various threats causing risks to integrity of data. The digital image data is susceptible to corruption and errors arising from analog to digital conversion. Productively, the ciphered image becomes vulnerable to data loss and noise effects [31]. In the process of safeguarding from these threats, the pixels shuffling, scrambling and value manipulation plays a vital role in image encryption. Figure 7 provides the decryption outcomes of ciphered images along with various noise effects of a noise effects test. Interestingly, the recovered images maintain recognizability even with the noise effects. Figure 8 gives the outcomes of the data loss test. We analyze that the data loss, the recovered images are visually recognizable up to 50%. This means that our proposed image encryption scheme has high resistance against both data loss and noise effects.

Figure 7: Noise effect on encrypted and decrypted and images with a) 1% salt and pepper noise, b) 5% salt and pepper noise, c) 10%salt and pepper noise.

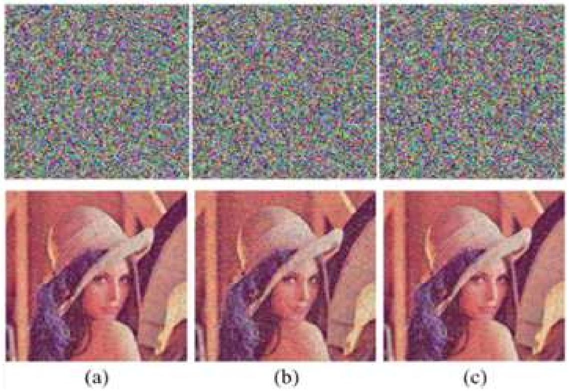
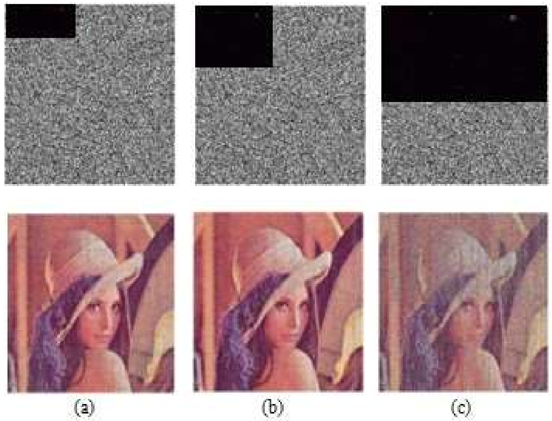


Figure 8: Data Loss effect on encrypted decrypted images with a) 12.5% data loss, b) 25% data loss, c) 50%data loss.



5.9. Computational speed

The algorithm is executed in Intel(R) Core i7-5500U processor with 12GB of RAM and MATLAB R2019a software. The algorithm gives utmost priority if its execution time is less. The comparative analysis with other algorithms is given in Table 9.

Table 9: Execution Time

Method	Execution Time(sec)
Proposed	1.0031
[33]	5.5567
[32]	1.0124

6. CONCLUSION

The implementation of the novel algorithm in this paper uses the Elliptic curve (EC), shuffled Arnold cat map and hill cipher. Initially separate the R, G, B channels from the original color image (I_{RGB}) with 256*256 pixels. Then divide each channel into four equal sub-images. Perform the Arnold cap map function on each sub-image and reconstruct the sub-images into single planes. The obtained three planes are reconstructed into one image and perform shuffle operation the obtained image is stored in As_{RGB}. Later perform hill cipher operation with self-invertible matrix which is generated from ECC keys. Based on the key, the encryption image is obtained. Analysis of security and efficiency is computed by various testing methods shows that the proposed algorithm has large key space, more secure and highly resistant to several attacks. So, it can encrypt the color image efficiently.

- The extension of this work in future would be implementing to encrypt the high-resolution images in different fields like medical, military etc.

- To implement the proposed algorithm on the real-time video applications.

REFERENCES:

[1] Diffie W, Hellman ME. New directions in cryptography. InDemocratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman 2022 Aug 24 (pp. 365-390).

[2] Raja NT, Singh KM. Secure and Efficient Text Encryption Using Elliptic Curve Cryptography. InEvolution in Computational Intelligence: Proceedings of the 9th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA 2021) 2022 Apr 24 (pp. 521-529). Singapore: Springer Nature Singapore.

[3] Ataş MT, Güler H. Real-time encryption/decryption algorithm with a fractional chaotic system of various data: Image, speech, and text. International Journal of Applied and Computational Mathematics. 2022 Aug;8(4):161.

[4] Lee G, Kim M, Park JH, Hwang SW, Cheon JH. Privacy-Preserving Text Classification on BERT Embeddings with Homomorphic Encryption. arXiv preprint arXiv:2210.02574. 2022 Oct 5.

[5] Lai Q, Hu G, Erkan U, Toktas A. A novel pixel-split image encryption scheme based on 2D Salomon map. Expert Systems with Applications. 2023 Mar 1;213:118845.

[6] Gao X, Mou J, Xiong L, Sha Y, Yan H, Cao Y. A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. Nonlinear dynamics. 2022 Mar;108(1):613-36.

[7] Gao X, Mou J, Banerjee S, Cao Y, Xiong L, Chen X. An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map. Journal of King Saud University-Computer and Information Sciences. 2022 Apr 1;34(4):1535-51.

[8] Sethi J, Bhaumik J, Chowdhury AS. Chaos-based uncompressed frame level video encryption. InProceedings of the Seventh International Conference on Mathematics and Computing: ICMC 2021 2022 Mar 6 (pp. 201-217). Singapore: Springer Singapore.

[9] Alhayani BS, Hamid N, Almukhtar FH, Alkawak OA, Mahajan HB, Kwekha-Rashid AS, İlhan H, Marhoon HA, Mohammed HJ, Chaloob IZ, Alkhayyat A. Optimized video internet of things using elliptic curve cryptography-based encryption and decryption. Computers and Electrical Engineering. 2022 Jul 1;101:108022.

[10] Wu R, Gao S, Wang X, Liu S, Li Q, Erkan U, Tang X. AEA-NCS: An audio encryption algorithm based on a nested chaotic system. Chaos, Solitons & Fractals. 2022 Dec 1;165:112770.

[11] Dong Z, Wang X, Zhang X, Hu M, Dinh TN. Global exponential synchronization of discrete-time high-order switched neural networks and its application to multi-channel audio encryption. Nonlinear Analysis: Hybrid Systems. 2023 Feb 1;47:101291.

[12] Tsafack N, Sankar S, Abd-El-Atty B, Kengne J, Jithin KC, Belazi A, Mehmood I, Bashir AK, Song OY, Abd El-Latif AA. A new chaotic map with dynamic analysis and encryption application in internet of health things. IEEE Access. 2020 Jul 21;8:137731-44.

[13] Jithin KC, Sankar S. Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set. Journal of Information Security and Applications. 2020 Feb 1;50:102428.

[14] Ataş MT, Güler H. Real-time encryption/decryption algorithm with a fractional chaotic system of various data: Image, speech, and text. International Journal of Applied and Computational Mathematics. 2022 Aug;8(4):161.

[15] Alexan W, Elkandoz M, Mashaly M, Azab E, Aboshousha A. Color image encryption through chaos and kaa map. IEEE Access. 2023 Feb 3;11:11541-54.

[16] Erkan U, Toktas A, Lai Q. 2D hyperchaotic system based on Schaffer function for image encryption. Expert Systems with Applications. 2023 Mar 1;213:119076.

[17] Chen F, Wong KW, Liao X, Xiang T. Period distribution of generalized discrete Arnold cat map. Theoretical Computer Science. 2014 Oct 2;552:13-25.

[18] Caelli WJ, Dawson EP, Rea SA. PKI, elliptic curve cryptography, and digital signatures. Computers & Security. 1999 Jan 1;18(1):47-66.

[19] Maurer UM, Wolf S. The diffie–hellman protocol. Designs, Codes and Cryptography. 2000 Mar;19(2-3):147-71.

[20] Jao D. Elliptic curve cryptography. InHandbook of information and communication security 2010 (pp. 35-57). Berlin, Heidelberg: Springer Berlin Heidelberg.

[21] Hill LS. Cryptography in an algebraic alphabet. The American Mathematical Monthly. 1929 Jun 1;36(6):306-12.

[22] Magamba K, Kadaleka S, Kasambara A. Variable-length Hill cipher with MDS key matrix. arXiv preprint arXiv:1210.1940. 2012 Oct 6.

[23] Ching SL, Yunos F. Effect of self-invertible matrix on cipher hexagraphicpolyfunction. Cryptography. 2019 Jun 15;3(2):15.

[24] SIPI Image Databasehttps://sipi.usc.edu/database/database.php?volume=misc

[25] Belazi A, Talha M, Kharbech S, Xiang W. Novel medical image encryption scheme based on chaos and DNA encoding. IEEE access. 2019 Mar 20;7:36667-81.

[26] Batool SI, Waseem HM. A novel image encryption scheme based on Arnold scrambling and Lucas series. Multimedia tools and applications. 2019 Oct 15;78:27611-37.

[27] Wang X, Yang J. Spatiotemporal chaos in multiple coupled mapping lattices with multi-dynamic coupling coefficient and its application in color image encryption. Chaos, Solitons & Fractals. 2021 Jun 1;147:110970.

[28] Hosny KM, Kamal ST, Darwish MM. A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map. The Visual Computer. 2023 Mar;39(3):1027-44.

[29] Tsafack N, Kengne J, Abd-El-Atty B, Iliyasu AM, Hirota K, Abd EL-Latif AA. Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. Information Sciences. 2020 Apr 1;515:191-217.

[30] Nestor T, De Dieu NJ, Jacques K, Yves EJ, Iliyasu AM, Abd El-Latif AA. A multidimensional hyperjerk oscillator: Dynamics analysis, analogue and embedded systems implementation, and its application as a cryptosystem. Sensors. 2019 Dec 21;20(1):83.

[31] Wells PN. Handbook of image and video processing. Physiological Measurement. 2001 Feb 14;22(1):263-4.

[32] Vamsi D, CH PR. Hybrid Image Encryption Using Elliptic Curve Cryptography, Hadamard Transform and Hill Cipher. Webology. 2021 Jan;18(1):913-34.

[33] Chen J, Zhang Y, Qi L, Fu C, Xu L. Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression. Optics & Laser Technology. 2018 Feb 1;99:238-48.

[34] Desam V, CH PR. Hybrid partial differential elliptical Rubik's cube algorithm on image security analysis. Journal of Engineering, Design and Technology. 2023 Apr 20

[35] Vamsi D, Reddy P. Electronic health record security in cloud: Medical data protection using homomorphic encryption schemes. InResearch Anthology on Securing Medical Systems and Records 2022 (pp. 853-877). IGI Global.