Palestine Journal of Mathematics

Vol 15(1)(2026) , 998–1017

CHAOS-BASED ENCRYPTION ALGORITHM USING CHEN'S HYPER-CHAOTIC MAP AND ELGAMAL CRYPTOSYSTEM

D. Singh, M. K. Patel and N. Khaitan*

Communicated by Manoj Patel

MSC 2020 Classifications: Primary 94A08; Secondary 68P25.

Keywords and phrases: Image processing, ElGamal cryptosystem, Chen's hyper-chaotic system, 2D Hénon map, Image security.

Acknowledgement: The first author is thankful to DST, India, for support through grant no.: SR/FST/MS- 1/2021/104(C) under DST-FIST project. The corresponding author is thankful for the financial assistance from the CSIR, New Delhi, in the form of a Junior Research Fellowship (JRF). The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions which improved the quality of our paper.

Abstract Technology has seen remarkable growth over the past few decades, accompanied by a significant rise in the use of multimedia devices. This widespread adoption of digital devices has led to an explosion in the circulation of multimedia data. Since, the volume of digital content continuously increasing, so there is a need for robust security measures to protect this valuable data from unauthorized access and malicious threats. A lot of data is communicated in the form of images over open networks. Effective encryption algorithms are essential for safeguarding image data and ensuring its confidentiality and integrity. In response to this growing demand for enhanced image security, this paper presents an efficient image encryption algorithm based on the ElGamal cryptosystem combined with Chen's hyper-chaotic system and 2D Hénon map. The Chen's hyper-chaotic map is used for diffusion of image pixels, whereas 2D Hénon map is utilized to introduce confusion. The Chen's hyper-chaotic system provides high level of unpredictability and complexity to the image data. It provides an added layer of security when combined with 2D Hénon map. Our approach has been rigorously tested through simulations and the results demonstrate the efficiency and effectiveness of the proposed scheme. Further, a comprehensive security analysis along with comparison with some existing encryption techniques supports the robustness of the algorithm. These analyses confirm that our approach not only meets the current security requirements, but also provides a reliable solution for protecting digital media data in today's technologically advanced landscape.

1 Introduction

In past few decades, the technology has grown rapidly and usage of multimedia channels has been increased widely. A lot of multimedia data is being circulated in the form of images and videos. Since, this digital data is communicated through some open network channels, therefore, the security of communicated digital data has been a great concern in various domains such as social media, medical imaging, satellite imaging, digital transactions, etc. In order to protect secrecy in this fast pace changing technological era, several image security algorithms have been introduced. But due to rapid technological advancement in hardware and software, algorithms gets outdated and are not capable of protecting data, which may attract several threats to the secret data. Thus, there is strong demand to construct some novice data encryption algorithms.

Research advancements in image security have been received using DNA coding [11, 27, 36, 45, 46], RSA cryptosystem [25, 32], wavelet transform [7, 16, 23], cosine transform [21, 39], fractional Fourier transform [19, 20] and many more. Several researchers have used spatial domain encryption which comprises of scrambling and sequence encryption. In [47], a novel scheme

for encryption and decryption of multiple colour images is proposed by combining bit-level extension with discrete wavelet transform (DWT). Additionally, chosen-plaintext and differential attacks are mitigated by generating secret keys with SHA-512 hash function. Authors in [44] proposed an image encryption algorithm using DNA coding and a compound-coupled chaotic system (CCCS) to enhance level of security in image encryption. In [37], Vaish have introduced an error free and key sensitive color image encryption scheme using Sine powered map and Arnold transform in Stockwell domain. In [12], authors introduced an adaptive sparse basis compressive sensing (ASB-CS) model using singular value decomposition (SVD) and a new fractional-order Hopfield neural network with parametric deformed exponential rectified linear unit (PDE-ReLU) memristor. In [15], an image encryption scheme combining Arnold's cat map for pixel shuffling, elliptic curve cryptography for encryption, and a genetic algorithm to optimize key generation and enhancing security, is provided. In [33], Song et al. presented a parallel image encryption algorithm using intra bitplane scrambling. In [42], Xu et al. introduced dynamical analysis of an improved FitzHugh-Nagumo neuron model with multiplier-free implementation. In [35], Sun et al. provided dynamic analysis of HR-FN-HR neural network coupled by locally active hyperbolic memristors and encryption application based on Knuth-Durstenfeld algorithm.

Several public key cryptosystems such as RSA, ElGamal, RC4, Paillier are popular in this domain. The authors in [9] have applied ElGamal cryptosystem for image security. The authors in [17] proposed a medical image encryption scheme utilizing improved ElGamal cryptosystem. In [28], researchers have used ElGamal crytosystem and Arnold map to encrypt an Electronic Patient Record (EPR) and then further embedded it for additional security. The ElGamal method generates distinct ciphertexts for the same plaintext message with each encryption operation. This feature improves security by ensuring that even if a hacker intercepts different ciphertexts, they cannot readily interpret the original message. It has scalablility, high computational complexity, higher security, low space consumption. It also performs better than some other public key cryptosystems [30] as it is not based on factorizing substantial prime numbers.

Due to the unpredictable nature of chaos-based schemes, it becomes a good candidate for several cryptographic schemes. The chaotic systems ensure higher security, creating resistance to brute-force attacks. Chaotic systems are popular in image encryption techniques because they possess ergodicity, robustness, pseudo-randomness, complexity, high sensitivity to initial values, and adjustable parameters. There are mainly two types of chaotic maps [1], one or 2-dimensional and multidimensional chaotic maps. The multidimensional chaotic system entails more time for execution due to its complicated structure and the methodology of finding solutions. In disparity, one- or two-dimensional chaotic maps have a more straightforward design and are executed efficiently in recent MATLAB versions and require less computational time. In view of this result, we employed a combination of lower-dimensional chaotic maps instead of a single multidimensional chaotic system. Niu et al. presented an image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators [29]. Kocak et al. introduced an image encryption algorithm based on key optimization by using the particle swarm optimization (PSO) algorithm and a novel modular integrated logistic exponential (MILE) map, which provides enhanced chaotic performance, faster processing, and strong resistance to cryptanalysis [14]. Çelik et al. [5] introduced an encryption scheme by applying affine and substitution techniques along with an extended one-dimensional chaotic map to enhance encryption strength. The authors in [24] have developed a public key image encryption technique based on modified approach of Vigener cipher combined with the Arnold and Baker maps. Zhou et al. [48] proposed a novel image encryption scheme based on chaotic signals with finite-precision error. In [4], Bahaddad et al. presented an image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption. In [34], Su et al. provided a three-dimensional (3D) space permutation and diffusion technique for chaotic image encryption using Merkel tree and DNA code. In [6], authors introduced a symmetric cryptosystem for RGB image encryption combining a 3D hybrid chaotic system, a novel pixel shuffle operator, and cellular automata. Vijayakumar et al. [38] proposed an encryption technique by combining S-boxes, cellular automata (CA) along with using a 4D memristive hyperchaos to enhance randomness, uncertainty, and ergodicity. Li et al. [18] proposed an image encryption algorithm using a 6D chaotic system and DNA encoding. The image is diffused and shuffled by chaotic sequences at both pixel and DNA encoding levels, producing a highly secure encrypted image. Two chaotic maps, namely

logistic and Hénon maps are used in [13] to generate encryption keys. The 2D Hénon map in [22,31] exhibits high sensitivity of its parameter values, non-linearity and unpredictable nature.

In recent years, researchers have investigated hyper-chaotic system because it has more than one positive Lyapunov exponent, larger key space, better sensitivity, high security and more complex dynamical characteristics. An image cryptosystem based on hyper-chaotic map has been proposed in [10]. Chen's hyper-chaotic system is recently utilised in [2,8,40] as it's computation time is shorter than that of other chaotic systems. In [43], Yu et al. presented dynamics analysis, FPGA realization and image encryption application of a 5D memristive exponential hyperchaotic system.

By reminiscing the ideas above and considering the urge of the image security in defence sector, medical and smart devices, we are disseminating a novel image encryption algorithm which is highly secure and robust over open networks. In the proposed algorithm, the ElGamal cryptosystem is combined with multi-dimensional Chen's hyper-chaotic system for diffusion and 2-dimensional Hénon map for confusion. A comprehensive analysis of our algorithm is provided, addressing key challenges such as key sensitivity, computational efficiency, and resistance to cryptographic attacks. Through experimental validation, we demonstrated that our algorithm offer a viable and potent alternative to remaining image encryption methods, paving the way for more secure and efficient image data protection strategies.

The structure of the paper is as follows: Section 2 provides preliminaries required for this paper, whereas Section 3 introduces structure of proposed scheme for encryption and decryption of images. Section 4 presents the simulation results for the given scheme. Section 5, Section 6 and Section 7 are devoted to the statistical results, security analysis and quality measures respectively. Section 8 compares the proposed scheme's results with some of the existing techniques. At last, Section 9 presents the conclusion of the paper.

2 Preliminaries

In order to construct the proposed algorithm, it is required to ponder over the following preliminaries:

2.1 ElGamal cryptosystem

The ElGamal cryptosystem introduced by T. Elgamal in 1985, is an asymmetric key cryptosystem based on discrete logarithm problem which requires to find the exponent $0 < x < \phi(p)$ of the equation $r^x \equiv y \ (mod\ p)$ for the given positive integers r, y and p [3]. The Elgamal cryptosystem is described below:

- First, select a large prime p and a positive integer r such that r is a primitive root of p.
- Select a random positive integer k such that $2 \leq k \leq p-2$.
- Compute $s \equiv r^k \ (mod\ p)$.
- (r, s, p) are public keys and k is private key.
- For encryption, select a positive integer l such that $2 \leq l \leq p-2$.
- Compute $e \equiv s^l \ (mod\ p)$ and $f \equiv r^l \ (mod\ p)$.
- Next, compute $c \equiv m * e \ (mod\ p)$ where m is the plain message.
- For decryption, compute $m \equiv c * f^{-k} \ (mod\ p)$.

For instance, let us take the prime number $p = 269$ and the primitive root $r = 3$. Now, choose the integer $k = 9$ which lies between 2 and 267. Next, compute $s \equiv 3^9 \ (mod\ 269) \equiv 46 \ (mod\ 269)$. So, public keys are $(r, s, p) = (3, 46, 269)$ and private keys is $k = 9$. Next, choose the random integer $l = 37$ which lies between 2 and 267. Next, compute $e \equiv 46^{37} \ (mod\ 269) \equiv 230 \ (mod\ 269)$. For encryption of message $m = 131$, multiply m with e to obtain $c \equiv 131 * 230 \ (mod\ 269) \equiv 2 \ (mod\ 269)$. For decryption of ciphered message c, calculate $f \equiv 3^{37} \ (mod\ 269) \equiv 122$ and our message $m \equiv 2 * 122^{-9} \ (mod\ 269) \equiv 2 * 200 \ (mod\ 269) \equiv 131 \ (mod\ 269)$.

2.2 Chen's hyper-chaotic system

The Chen's hyper-chaotic system is extensively used in image encryption algorithms as it takes less time to generate sequences due to the presence of two positive Lyapunov exponents [8]. This system is represented as follows:

$$\begin{cases} \dot{x} = \alpha(y - x), \\ \dot{y} = \delta x - xz + \gamma y - h, \\ \dot{z} = xy - \beta z, \\ \dot{h} = x + \kappa, \end{cases} \tag{2.1}$$

where $\alpha,\ \beta,\ \gamma,\ \delta$, and κ are secret key parameters. The system (2.1) becomes a hyperchaotic for $-0.7 < \kappa < 0.7$, $\alpha = 36$, $\beta = 3$, $\gamma = 28$, and $\delta = -16$. It is utilized to create four hyper-chaotic sequences using famous Runge-Kutta method of order four. It provides better security compare to other chaotic systems [8, 40].

2.3 2D Hénon map

The Hénon map is proposed by M. Hénon as a simplified version of the Poincaré section of the Lorenz model [41]. The two dimensional invertible discrete Hénon map is given by:

$$\begin{cases} x_{i+1} = 1 - ax_i^2 + y_j \ (mod\ n), \\ y_{j+1} = x_i + b \ (mod\ n), \end{cases} \tag{2.2}$$

where n is the order of the image matrix, and a, c are the key parameters which lies in the finite cyclic group of order n. Also, (x_i, y_j) and (x_{i+1}, y_{j+1}) are the respective pixel positions of the old and new images. The inverse of the above map is given by:

$$\begin{cases} x_i = y_{j+1} - b \ (mod\ n), \\ y_j = ax_i^2 + x_{i+1} - 1 \ (mod\ n). \end{cases} \tag{2.3}$$

3 Proposed scheme

3.1 Image encryption algorithm

In the proposed scheme first we apply ElGamal encryption scheme to diffuse the image pixels and then Chen's hyper-chaotic map is applied to diffuse the pixels of partially encrypted image. In the next round, we implement 2D Hénon Map to confuse pixels of the image data obtained from previous step. Three color component images red component (N_R), green component (N_G), and blue component (N_B) are segregated from an RGB image (N_{RGB}). We apply the ElGamal cryptosystem on these component images for the first stage of partial encryption to get images (N_{R_1}), (N_{G_1}) and (N_{B_1}). As discussed in Section 2.1, for the above partial encrypted images, use keys k_R for (N_{R_1}), k_G for (N_{G_1}) and k_B for (N_{B_1}). To improve the encryption quality, different key parameters are used for all three color plates. Next, with the help of Chen's hyper-chaotic system, we construct an image matrix of sizes $n \times n$ with random entries using parameter κ_R. Similarly, using the parameters κ_G and κ_B we constructed image matrices for (N_{G_1}) and (N_{B_1}), respectively. These random image matrices are XORed with (N_{R_1}), (N_{G_1}) and (N_{B_1}) to get new encrypted image matrices (N_{R_2}), (N_{G_2}) and (N_{B_2}). For the third stage encryption and to decrease correlation among the pixels, exploit Hénon map with parameters a_R, b_R for (N_{R_2}), a_G, b_G for (N_{G_2}) and a_B, b_B for (N_{B_2}) to get final encrypted image matrices (N_{R_3}), (N_{G_3}), and (N_{B_3}). Concatenating these component images to produces the final ciphered image C. The block diagram for the proposed encryption algorithm is summarize in Figure 1.

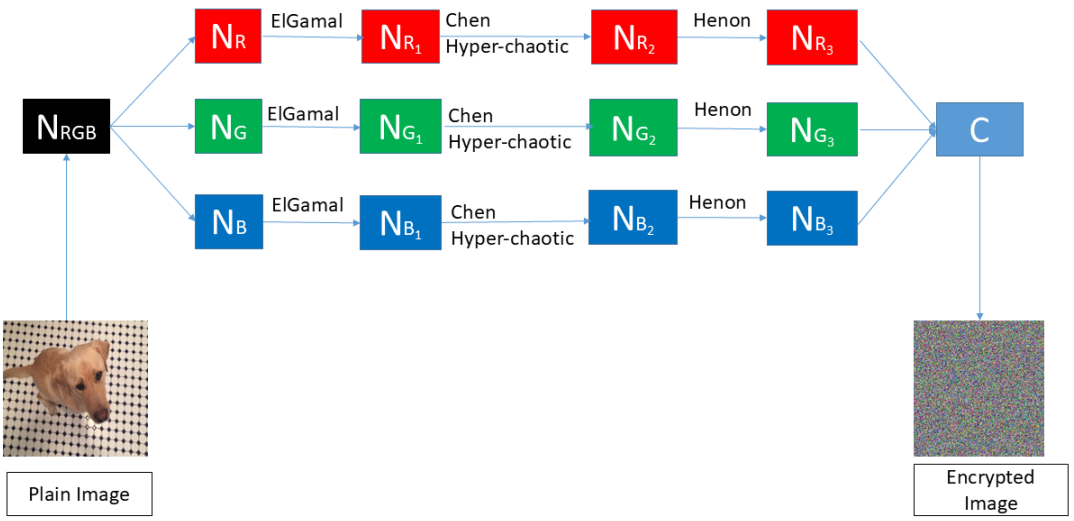

Figure 1: Block diagram for proposed technique

Generation of Random matrix using Chen's hyper-chaotic system

To increase the performance and to resist statistical attacks in image cryptography; the hyper-chaotic maps play crucial role in image ciphering schemes. The Chen's hyper-chaotic system will be used in the proposed algorithm to generate random matrix of entries from 0 to 255.

With the help of the Runga-Kutta method of order four, hyperchaotic sequences $< u_j >, < v_j >, < z_j >$, and $< w_j >$ are generated. These sequences are further used to generate a random matrix. The prediction time for Chen's setup is low than that of other chaotic systems. Also, due to higher security of Chen's system compared to other chaotic systems, it is implemented in the proposed algorithm.

The following steps are followed to generate the random matrix:

- Transform the above hyper-chaotic sequences $< u_j >, < v_j >, < z_j >$, and $< w_j >$ into sequences $< u_j^* >, < v_j^* >, < z_j^* >$, and $< w_j^* >$ of integers from 0 to 255 as follow:

$$\begin{aligned} u_j^* &= |fix((u_j - fix(u_j)) \times 10^{14})| \ (mod\ 256), \\ v_j^* &= |fix((v_j - fix(v_j)) \times 10^{14})| \ (mod\ 256), \\ z_j^* &= |fix((z_j - fix(z_j)) \times 10^{14})| \ (mod\ 256), \\ w_j^* &= |fix((w_j - fix(w_j)) \times 10^{14})| \ (mod\ 256), \end{aligned} \tag{3.1}$$

  where $fix(k)$ gives integer nearest to k towards zero.

- With the help of sequences defined in system (3.1), a hyper-chaotic sequence $P = \{I_1, I_2, I_3, ..., I_{n^2}\}$ is created as follows

$$I_j = \begin{cases} u_j^* & if \quad 0 \equiv w_j^* (mod\ 3), \\ v_j^* & if \quad 1 \equiv w_j^* (mod\ 3), \\ z_j^* & if \quad 2 \equiv w_j^* (mod\ 3), \end{cases} \tag{3.2}$$

  for $j = 1, 2, 3, ..., n^2$.

- Rearrange the elements of sequence $\{I_j\}$ to form a matrix I of size $(n \times n)$.

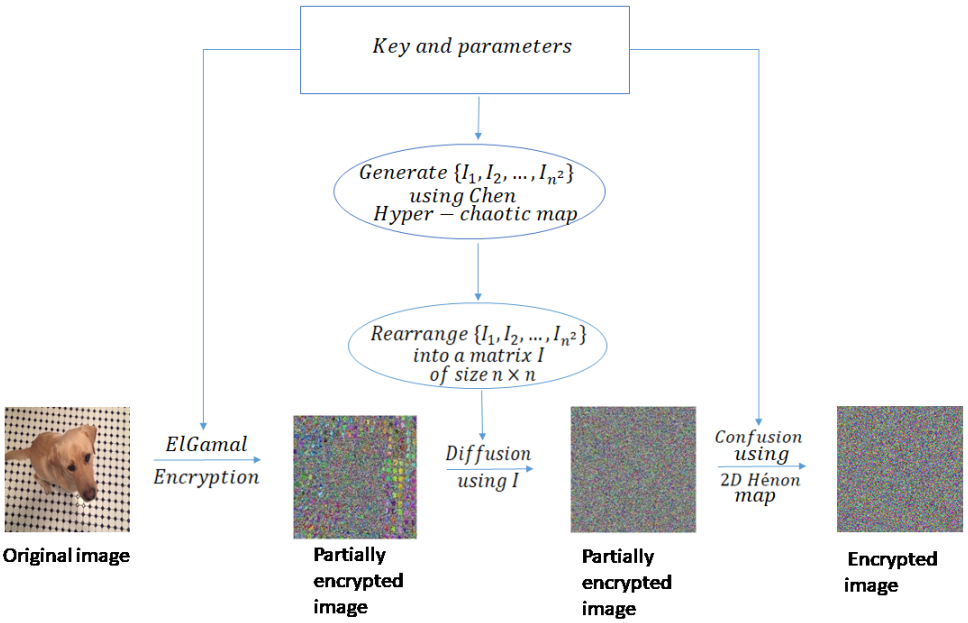

Figure 2: Flow chart of the proposed encryption algorithm

The step by step execution of the proposed algorithm is described as follows:

Step 1: Take the secret keys (k_R, k_G, k_B) for the ElGamal cryptosystem.

Step 2: Consider the 2-D Hénon map's secret parameters (a_R, a_G, a_B) and (b_R, b_G, b_B).

Step 3: Apply Chen's hyper-chaotic map to obtain the matrix I of size $n \times n$ whose entries are ranging from 0 to 255 (Please refer to Figure 2).

Step 4: Extract the component color images (viz, red (N_R), green (N_G) and blue (N_B)) from the plain image (N_{RGB}).

Step 5: Consider the color component N_R.

Step 6: Employ the ElGamal cryptosystem to the component image N_R, which produces first stage partial ciphered image N_{R_1}

$$N_{R_1} = mod(N_R \times s^l,\ 256).$$

Step 7: Take bitXOR of image N_{R_1} and the square matrix I obtained in Step 3 to obtain second stage partial encrypted image N_{R_2} as

$$N_{R_2} = N_{R_1} \bigoplus I.$$

Step 8: Apply 2-D Hénon map to image N_{R_2} to produce final encrypted component image N_{R_3}.

Step 9: Repeat Step 7 to Step 9 for other two color component images N_G and N_B to produce their respective encrypted components N_{G_3} and N_{B_3}.

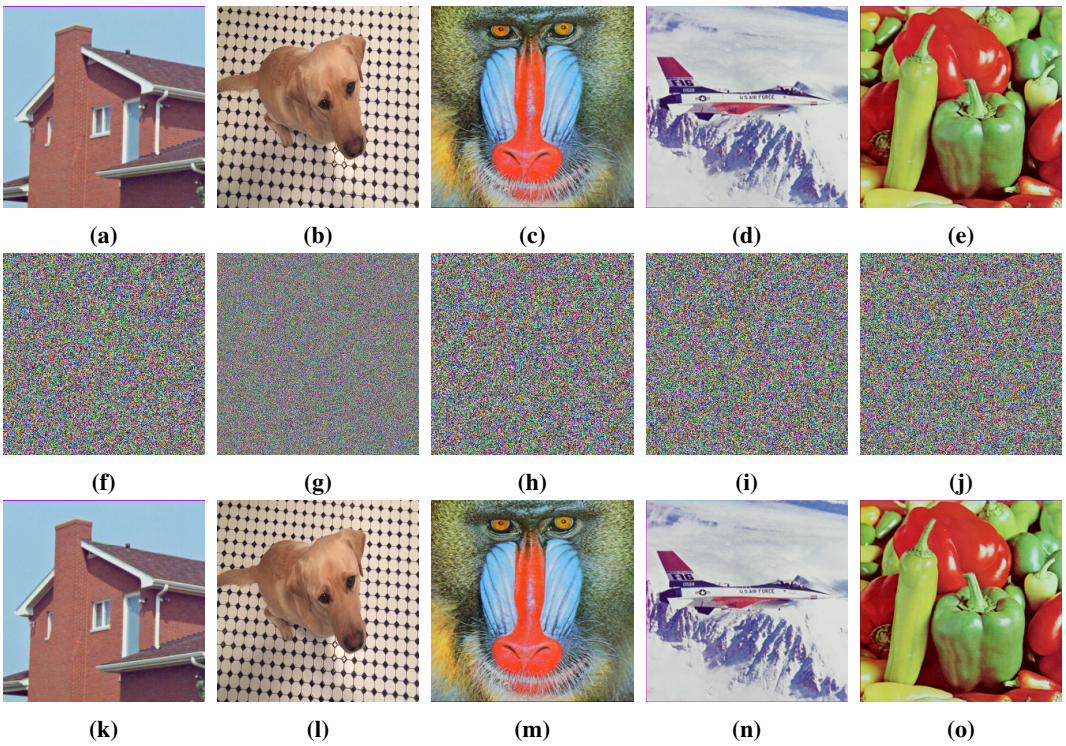

Figure 3: (a-e) show the experimental images for proposed algorithm. (f-j) show the encrypted images corresponding to the experimental images. (k-o) show the decrypted images corresponding to the encrypted images.

Step 10: Concatenate the obtained images in Step 9 and Step 10 to produce final colored cipher image (C)

$$C = cat(3, N_{R_3}, N_{G_3}, N_{B_3}).$$

3.2 Proposed scheme for image decryption

The process of decryption is reverse to that of encryption. We perform the all the above steps in reverse order starting from Step 11 to all the way to Step 4 to recover the original image (N_{RGB}) back from the ciphered image (C).

4 Simulation results

For the simulation of results of proposed image encryption algorithm, the different RGB images of size 256×256 are chosen randomly from the USC-SIPI database (https://sipi.usc.edu/database/). The algorithm is executed in MATLAB R2023b software using an Apple M1 chip with 8GB RAM system. The visual encryption results of different experimental images are given in Figure 3.

5 Statistical Analysis

5.1 Histogram analysis

A histogram of an image is a visual representation that shows the distribution of different brightness values in the image. It plots the frequencies of pixels for each possible brightness value, which typically ranges from 0 to 255 for an 8-bit grayscale image. Here, Figure 4 :(a-e) represent original image, (f-j) represent histogram of original image, (k-o) represent histogram of

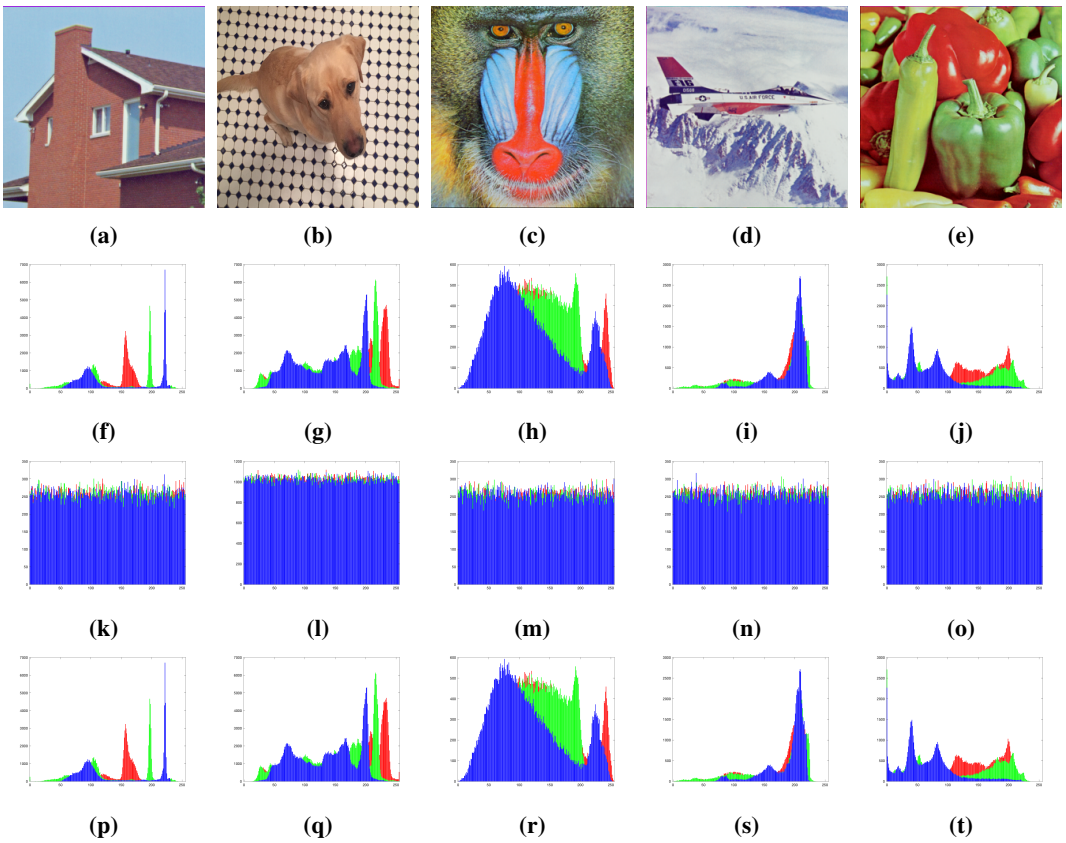

Figure 4: (a-e) show the experimental images for proposed algorithm; show the histogram of (f-j) original images. (k-o) encrypted images corresponding to that of the original images. (p-t) decrypted images corresponding to that of the encrypted images.

encrypted image, (p-t) represent histogram of decrypted image which is exactly same as histogram of original image which shows that our method is efficient.

5.2 Chi-square test

The image of the histogram provides a visual representation of the distribution of pixel intensity values. However, the chi-square test can be employed to interpret the histogram statistically. Mathematically, χ^2 is defined as:

$$\chi^2 = \frac{\sum_{i=1}^{256}(O_i - E)^2}{E}, \tag{5.1}$$

where O_i is the observed pixel intensity value, and $E = \frac{p \times q}{256}$ is the expected pixel intensity value of encrypted image of size $p \times q$.

It is demonstrated seen in the Table 1 that the values of chi-square test are less than the theoretical values 293.2478 with 255 degrees of freedom, at significance level of 5% and hence the proposed algorithm satisfy the null hypothesis which means that the pixels are uniformly distributed in encrypted images.

Table 1: Analysis of different encrypted images for Chi-square test

Images	χ^2_{test}			
	R	G	B	Average
House	253.6328	249.2891	229.5312	244.1510
Kobi	233.4375	248.1562	262.8594	248.1510
Baboon	286.9453	261.1641	240.5234	262.8776
Airplane (F-16)	257.3438	283.8281	282.0156	274.3958
Peppers	274.9453	283.7891	229.6875	262.8073

5.3 Correlation analysis

Correlation analysis of an image involves examining the relationship between different neighbouring pixel values of an image. It is generally observed that the neighbouring pixels of the plain image are highly correlated, i.e., there correlation coefficient is very near to 1 [24]. An encryption algorithm is good if the neighbouring pixels of the encrypted image are not correlated, in other words, the correlation coefficient is very near to zero. The correlation for two neighbouring pixels sequences $\{o_i\}_{i=1}^{M}$ and $\{p_i\}_{i=1}^{M}$ of an image is given by:

$$C_{op} = \frac{\sum_{i=1}^{M}(o_i - \overline{o})(p_i - \overline{p})}{\sqrt{(\sum_{i=1}^{M}(o_i - \overline{o})^2) \times (\sum_{i=1}^{M}(p_i - \overline{p})^2)}}, \tag{5.2}$$

where $\overline{o}$ and $\overline{p}$ are respective mean of the data $\{o_i\}_{i=1}^{M}$ and $\{p_i\}_{i=1}^{M}$.

It is clear from the results, presented in Table 2 that the correlation in plain images (in all three directions viz, diagonal, vertical and horizontal) is very near to 1 whereas for encrypted images (in all three directions) the value of correlation is very near to 0. Also, the graphical interpretation of correlation of the image House in Figure 5 and 6 shows that pixel values of encrypted image are evenly distributed throughout the image and hence, it verifies the proposed algorithm's robustness and efficiency.

Table 2: Analysis of different encrypted images for correlation analysis

Images		Correlation in plain images			Correlation in ciphered images		
		DC	VC	HC	DC	VC	HC
House	R	0.9126	0.9353	0.9671	-0.0044	-0.0020	0.0023
	G	0.9320	0.9474	0.9805	-0.0059	-0.0032	0.0001
	B	0.9625	0.9749	0.9820	-0.0017	0.0002	-0.0011
Kobi	R	0.8156	0.9166	0.8750	-0.0031	0.0012	0.0006
	G	0.8372	0.9261	0.8899	0.0034	-0.0002	-0.0007
	B	0.8685	0.9389	0.9122	0.0009	-0.0011	0.0078
Baboon	R	0.9034	0.9208	0.9474	-0.0013	-0.0003	0.0021
	G	0.7925	0.8380	0.8728	-0.0026	0.0068	0.0007
	B	0.8763	0.9139	0.9216	-0.0010	-0.0023	0.0061
Airplane (F-16)	R	0.8738	0.9239	0.9389	0.0018	-0.0026	-0.0056
	G	0.8814	0.9343	0.9309	0.0047	0.0058	-0.0017
	B	0.8800	0.9089	0.9503	0.0085	-0.0022	0.0049
Peppers	R	0.9369	0.9680	0.9646	-0.0056	0.0003	-0.0021
	G	0.9466	0.9750	0.9698	-0.0031	0.0042	-0.0004
	B	0.9263	0.9636	0.9570	0.0056	0.0031	0.0065

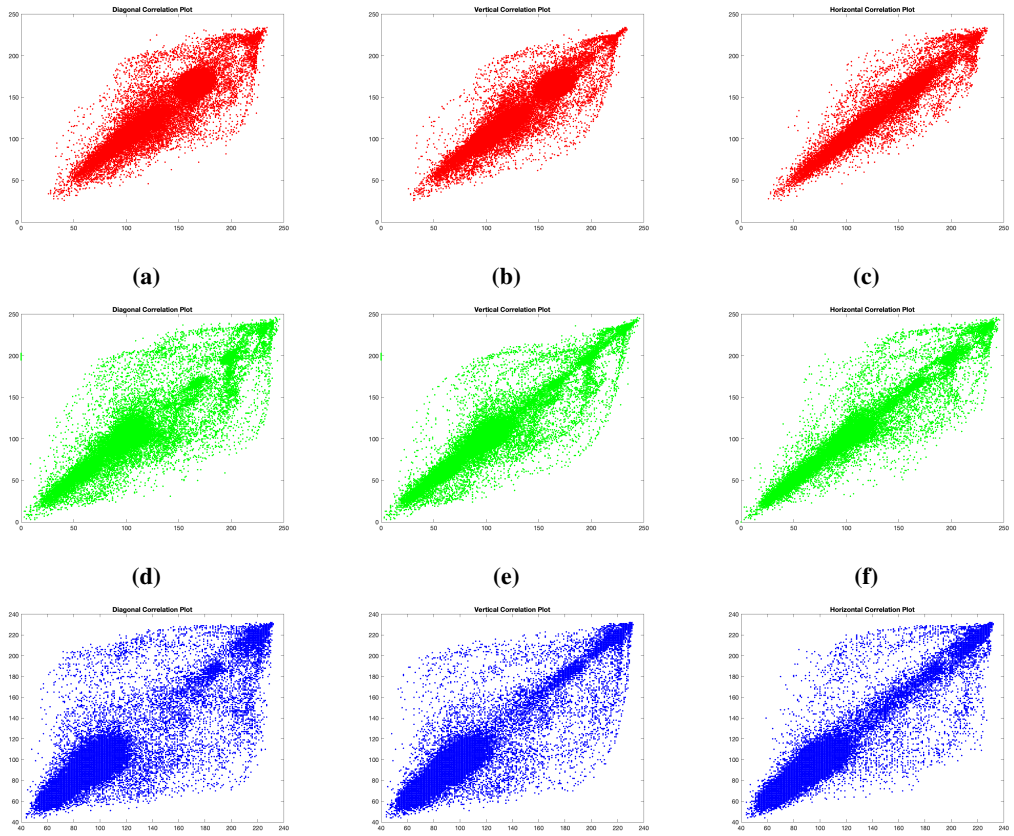

Figure 5: show the horizontal, vertical and diagonal correlation of (a-c) red component of House image. (d-f) green component of House image. (g-i) blue component of House image.

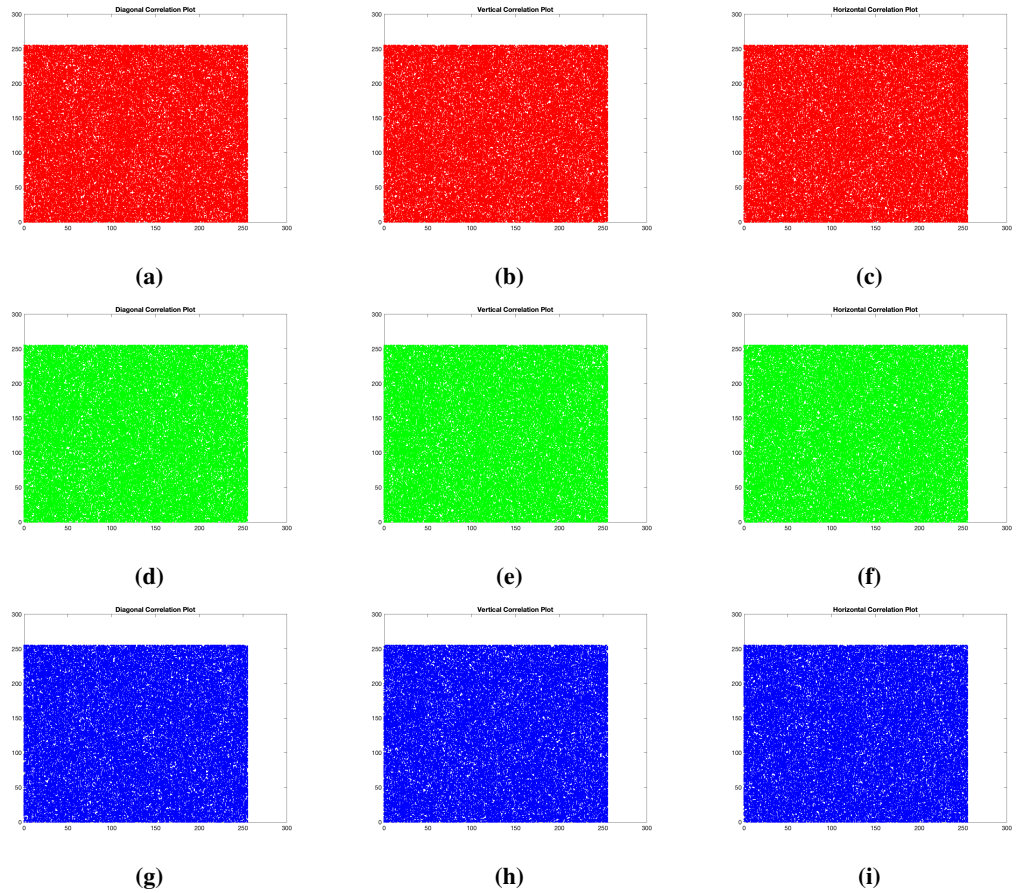

Figure 6: (a-c) show the horizontal, vertical and diagonal correlation of red component of encrypted House image. (d-f) show the horizontal, vertical and diagonal correlation of green component of encrypted House image. (g-i) show the horizontal, vertical and diagonal correlation of blue component of encrypted House image.

6 Security analysis

6.1 Key space analysis

The key space refers to the complete collection of all valid and different keys which are used in a specific cryptographic algorithm.

A substantial key space is crucial for a robust cryptographic algorithm to resist brute force attacks, as it hinders hackers from accurately determining the specific key parameters. The ElGamal private key parameters k_R, k_G, k_B play a critical role in determining the key space of the proposed algorithm. In addition to this, the Hénon parameters $a_R, a_G, a_B, b_R, b_G, b_B \in \mathbb{Z}_n$ contribute a substantial impact on the size of the key space. Further, the numbers of iterations τ_R, τ_G, τ_B also enhances the keyspaces. The total key space for the proposed algorithm is 2^{250} (approx.) which is more than the minimum required value 2^{100}. Therefore, the proposed algorithm is able to provide resistance against different cryptanalytic assaults.

6.2 Key sensitivity

The key sensitivity analysis validates the crucial role of secret keys, parameters, and their configuration in any image encryption algorithm. This analysis ensures the algorithm's robustness, offering protection against potential breaches. For an efficient encryption algorithm, high key sensitivity is critical, ensuring that even a slight change in the value (or a random arrangement) of key parameters denies the retrieval of the original image. Furthermore, even with all keys and parameters are correct, but fails to adhere to the correct decryption order cannot return the origi-

nal image. Our results show that the proposed algorithm exhibits exceptional sensitivity to keys, parameters, and their arrangement. The key sensitivity analysis is performed on the encrypted House image and the results are shown in Figure 7. The Hénon parameters $a_R, a_G, a_B, b_R, b_G, b_B$ with their proper arrangement, along with the iteration numbers τ_R, τ_G, τ_B, are the sensitive keys in the proposed scheme.

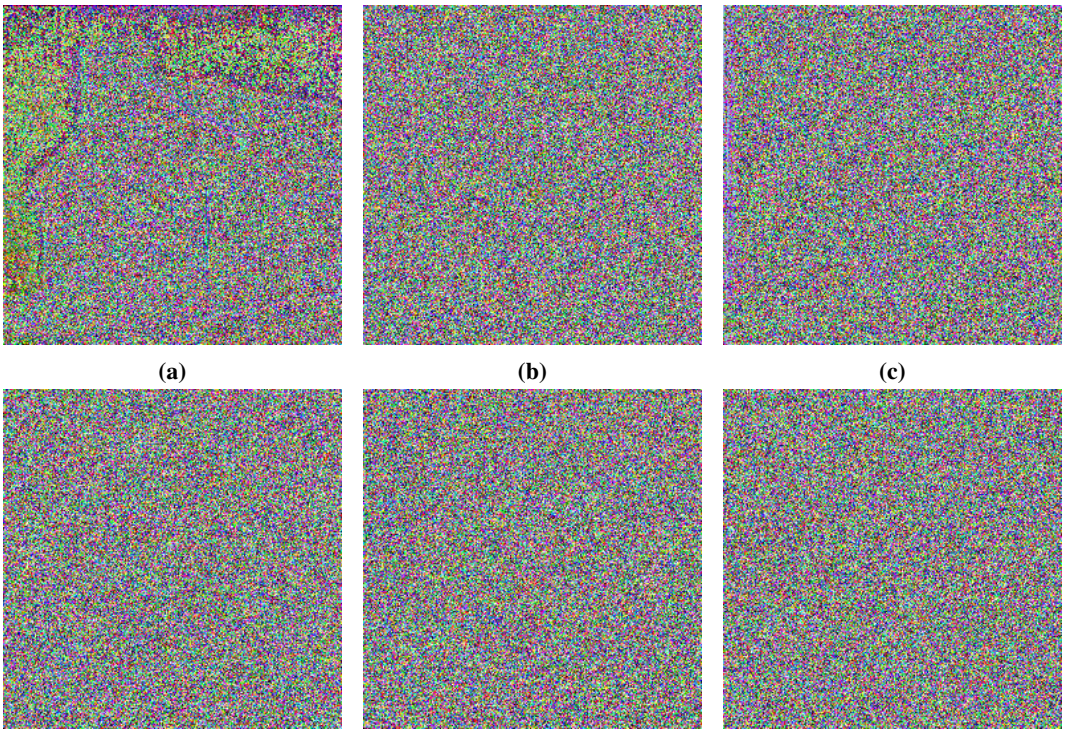

Figure 7: shows decrypted image of House by slightly changing (a) key parameters k of ElGamal cryptosystem. (b) key parameters κ of Chen's hyper-chaotic map. (c) initial conditions of Chen's hyper-chaotic map. (d) key parameters a and b of 2D Hénon map; (e-f) shows decrypted image of House by changing the order of decryption.

7 Quality measures

7.1 Mean square error

The mean square error represents the mean of the squares of the difference of two respective image pixels. It is calculated with the help of the expression:

$$MSE = \frac{1}{mn} \sum_{x=1}^{m} \sum_{y=1}^{n} \left[I_1(x,y) - I_2(x,y) \right]^2, \tag{7.1}$$

where I_1 and I_2 are the original and encrypted image matrices of size $m \times n$. The higher values of MSE show high robustness of the algorithm. Table 3 and 4 provides the proposed scheme's MSE values and clearly indicates that the algorithm is highly efficient and robust.

Table 3: Analysis of different encrypted images for mean square error

Images	MSE			
	R	G	B	Average
House	6904.6298	8642.5626	9596.5877	8381.2600
Kobi	10747.2634	9190.0162	8025.8169	9321.0322
Baboon	8400.2585	7388.0189	9062.5517	8283.6097
Airplane (F-16)	9820.8879	10481.4407	10360.8077	10221.0454
Peppers	7917.4194	11120.9976	11060.1131	10032.8434

Table 4: Analysis of different decrypted images for mean square error

Images	MSE		
	R	G	B
House	0	0	0
Kobi	0	0	0
Baboon	0	0	0
Airplane (F-16)	0	0	0
Peppers	0	0	0

7.2 Peak signal to noise ratio

The peak signal to noise ratio is a quality metric that quantifies the difference between a plain image and corrosponding encrypted image. It can be obtained by:

$$PSNR = log_{10}\left[\frac{(P_v)^2}{MSE}\right]^{10}, \tag{7.2}$$

where P_v is the peak pixel value in the image matrix, i.e., 255 and MSE is calculated using Equation (7.1). If the values of $PSNR$ is less than 10 decibels, then the algorithm is considered as good scheme [24]. Table 5 and 6 displays the experimental findings of peak signal-to-noise ratio ($PSNR$) for the proposed technique using various test images. It is evident from Table 5 and 6 that the proposed technique is robust and efficient.

Table 5: Analysis of different encrypted images for peak signal to noise ratio

Images	PSNR			
	R	G	B	Average
House	9.7394	8.7644	8.3096	8.9378
Kobi	7.8178	8.4976	9.0859	8.4671
Baboon	8.8879	9.4455	8.5583	8.9639
Airplane (F-16)	8.2093	7.9266	7.9769	8.0376
Peppers	9.1450	7.6694	7.6932	8.1692

Table 6: Analysis of different decrypted images for peak signal to noise ratio

Images	PSNR		
	R	G	B
House	∞	∞	∞
Kobi	∞	∞	∞
Baboon	∞	∞	∞
Airplane (F-16)	∞	∞	∞
Peppers	∞	∞	∞

7.3 Structural similarity index measure

The structural similarity index measure is again a quality metric that quantifies the similarities between a plain image and corrosponding encrypted image. It can be computed as:

$$SSIM(I_1, I_2) = \frac{(2\mu_1\mu_2 + C_1)(2\sigma_{12} + C_2)}{(\mu_1^2 + \mu_2^2 + C_1) + (\sigma_1^2 + \sigma_2^2 + C_2)}, \tag{7.3}$$

where μ_1 and μ_2 represent the average of pixel values of I_1 and I_2 respectively, σ_1 and σ_2 represent the variance of pixel values of I_1 and I_2 respectively, σ_{12} represents the covariance of pixel intensity values of I_1 and I_2, $C_1 = (t_1P_v)^2$ and $C_2 = (t_2P_v)^2$ are stabilizing parameters with $t_1 = 0.01$ and $t_2 = 0.03$ and P_v is the peak pixel value of I_1 and I_2, i.e., 255 [24]. The $SSIM$ values for the proposed encryption scheme are provided in the Table 7. It can be observed that all the SSIM values are very near to zero, which shows that the original and encrypted images are structurally totally different. Hence, the proposed algorithm is very secure and robust scheme.

Table 7: Analysis of different encrypted images for structural similarity index measure

Images	SSIM		
	R	G	B
House	0.0083	0.0101	0.0111
Kobi	0.0092	0.0108	0.0118
Baboon	0.0084	0.0075	0.0110
Airplane (F-16)	0.0097	0.0106	0.0093
Peppers	0.0105	0.0072	0.0070

7.4 Entropy analysis

Shannon's global entropy reflects the level of randomness or uncertainty in the source information. The entropy E of an 8-bit image is determined by using:

$$E = \sum_{\substack{k=0 \\ p(l_k)\neq 0}}^{255} p(l_k) log_2 \left(\frac{1}{p(l_k)} \right), \tag{7.4}$$

where $p(l_k)$ represents the probability of occurrence of pixel value k in the image matrix [24] and these summation runs over all the pixel values for which $p(l_k) \neq 0$.

The more uniform distribution of pixel values within the image data will result in a higher global Shannon's entropy. The higher entropy value for the encrypted image indicates a more secure image encryption algorithm. An ideally encrypted image should have an ideal entropy value of 8. Table 8 provides the global Shannon's entropy values for the five original images and their corresponding encrypted images across the R, G, and B colour planes for the proposed algorithm. The global Shannon entropy values for the encrypted images are nearly 8, indicating

a random distribution of pixels within the encrypted images. Therefore, the proposed algorithm is sufficiently robust to counter the statistical attacks.

Table 8: Analysis of different encrypted images for entropy analysis

Images	Entropy of the original images			Entropy of the encrypted images			
	R	G	B	R	G	B	Average
House	6.4311	6.5389	6.2320	7.9972	7.9971	7.9974	7.9972
Kobi	7.3951	7.4470	7.3182	7.9971	7.9969	7.9972	7.9971
Baboon	7.6058	7.3581	7.6665	7.9971	7.9972	7.9971	7.9971
Airplane (F-16)	6.7255	6.8253	6.2078	7.9971	7.9973	7.9970	7.9971
Peppers	7.3009	7.5570	7.0929	7.9970	7.9965	7.9972	7.9969

7.5 NPCR and UACI analysis

A differential attack is a technique that assists attackers in decrypting images. The attacker uses two images differing by a single bit and applies the same encryption scheme with the same keys to both images. The attacker then attempts to establish a relationship between the two images to deduce the secret keys. An algorithm resists differential attacks well when every bit in the encrypted image is affected by a one-bit change in the original image. The evaluation of differential attacks involves employing two widely used metrics: the number of changing pixel rates (NPCR) and unified averaged changed intensity (UACI). The equations for calculating NPCR and UACI between two cipher images of the same size $m \times n$ are calculated as follows:

$$NPCR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} S(i,j)}{mn} \times 100, \tag{7.5}$$

where

$$S(i,j) = \begin{cases} 0, & \text{if } R_1(i,j) = R_2(i,j) \\ 1, & \text{if } R_1(i,j) \neq R_2(i,j) \end{cases},$$

and

$$UACI = \frac{1}{mn}\left[\frac{\sum_{i=1}^{m}\sum_{j=1}^{n} |R_1(i,j) - R_2(i,j)|}{255}\right] \times 100, \tag{7.6}$$

where R_1 and R_2 are two encrypted images: one obtained by directly encrypting the plain image and the other obtained after making a minute change to the image. Table 9 below lists the NPCR and UACI values for five test images for each R, G and B colour plane.

Table 9: Analysis of different encrypted images for NPCR and UACI

Images	NPCR(%)				UACI (%)			
	R	G	B	Average	R	G	B	Average
House	100	100	100	100	44.6744	13.6673	44.8687	34.4035
Kobi	100	100	100	100	48.8663	49.7822	48.3450	48.9978
Baboon	100	100	100	100	19.4286	46.8392	19.4654	28.5777
Airplane (F-16)	100	100	100	100	22.6998	24.9245	41.6796	29.7680
Peppers	100	100	100	100	12.8082	15.1527	23.6194	17.1934

7.6 Occlusion attack

Network congestion, malicious interference, or intruders may cause data loss or alter pixels in specific areas when transmitting an encrypted image over a channel. Occlusion attack analysis evaluates the encryption algorithm's ability to recover data when losses occur during transmission. An encryption algorithm is effective if it can recover critical information from an encrypted image even if some data is lost. In this analysis, different portions of the encrypted house image are occluded, and the corresponding decrypted images are obtained. Figure 8: (a-d) shows the encrypted house image with occlusions in various portions, whereas Figure 8: (e-h) shows the corresponding decrypted image. It may be observed from Figure 8 that the decrypted images remain recognizable and preserve most of the valuable information of the original image. The occlusion attack analysis confirms that the proposed algorithm successfully decrypts occluded encrypted images while preserving most of the valuable information. Therefore, the algorithm effectively counters various occlusion attacks.

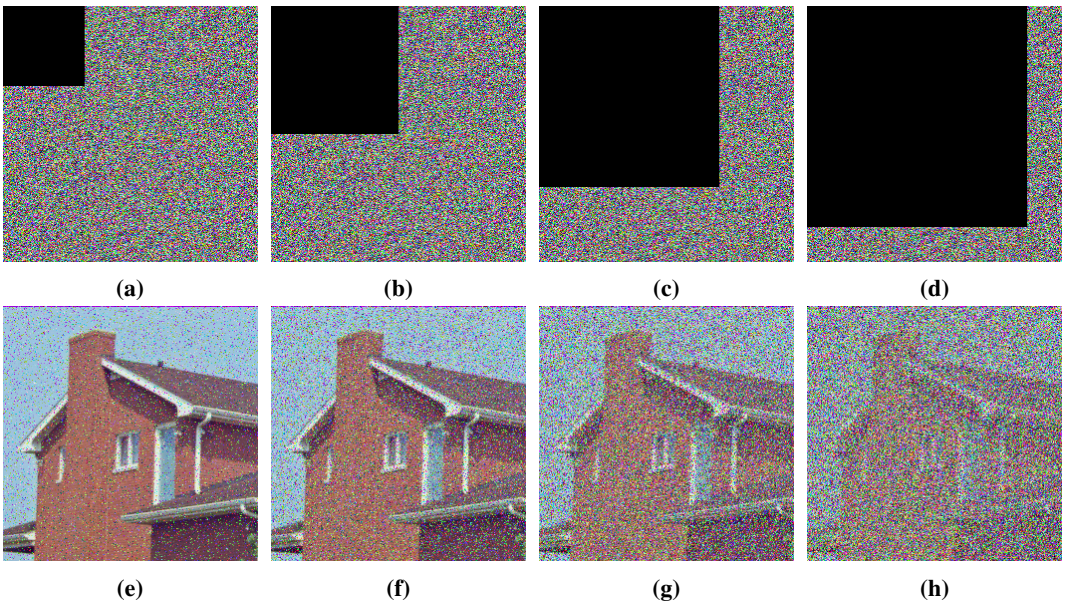

Figure 8: (a-d) shows the encrypted image of House with 10%, 25%, 50%, 75% cropped.
(e-h) shows the corresponding decrypted image of House with 10%, 25%, 50%, 75% cropped.

7.7 Run's test for randomness

Run's test is a non-parametric statistical method that assesses the likelihood of randomness in an event. The run's test applied to the cipher image yields a value of 0 if the pixel values are randomly distributed; otherwise, the test results in a value of 1. The proposed algorithm's run's test is analyzed using Matlab software, and the results are presented in Table 10, indicate that the encrypted images exhibit strong statistical randomness in image data. The Run's test results confirm that proposed algorithm efficiently resists the brute force attacks.

Table 10: Analysis of randomness using runs test

Images	Results for runs test	Randomness
House	0	pass
Kobi	0	pass
Baboon	0	pass
Airplane (F-16)	0	pass
Peppers	0	pass

7.8 Encryption time analysis

The computational time of an algorithm is crucial as it dictates its practical relevance in real-world situations. Table 11 below, presents the encryption time calculated for different test images for the proposed image encryption algorithm. It is clear that the proposed algorithm consumes lesser time for encryption of various test images, which verifies the faster encryption through the proposed algorithm.

Table 11: Analysis of different images for encryption time

Images	Size	Encryption time (in seconds)
House	$256 \times 256 \times 3$	1.126473
Kobi	$256 \times 256 \times 3$	1.158652
Baboon	$256 \times 256 \times 3$	1.327679
Airplane (F-16)	$256 \times 256 \times 3$	1.429406
Peppers	$256 \times 256 \times 3$	1.234877

8 Performance comparison with some existing techniques

This section shows a performance comparison of the proposed encryption algorithm with several recently established algorithms [1], [43], [26] for images of size 256×256. Table 12 and Figure 9 shows that the proposed algorithm requires significantly less encryption time than others. The encryption time can also be further reduced by employing suitable hardware and software on high-end computers. The lesser time for executions highlights the efficiency of the proposed algorithm. These improved speed attributes enhance security and minimise computational power.

Table 12: Comparative analysis of different methods for encryption time

Techniques	Encryption time (in seconds)
Proposed Scheme	1.2
[43]	1.38
[1]	15
[26]	47.367

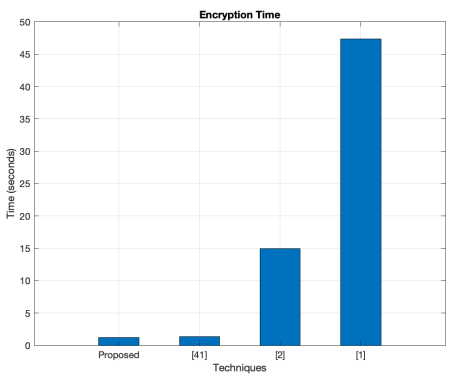

Figure 9: Bar graph encyption time

9 Conclusion

In this paper, an efficient multilayer image ciphering algorithm is presented with the help of the ElGamal public key cryptosystem, Chen's hyper-chaotic system, and 2D Hénon map. The infrangiblity of solving discrete logarithm problem provides high security in the ElGamal encryption algorithm. The random matrix generated through Chen's hyperchaotic system is XORed with the partially encrypted image. The final tinct of confusion is achieved by exploiting the 2D Hénon map which provides randomness in pixel values and produces highly unbreakable algorithm. The simulation results demonstrate the encryption versatility of the proposed algorithm across various images. From the statistical analysis presented in Section 5, it is clear that the values of entropy highly resemble with the corresponding ideal values. The security analysis in Section 6 declare the that security of the proposed scheme depends not only on keys and parameters, but also on their order at every stage of encryption and decryption. The results (average values) obtained in terms of $SSIM = 0.0095$, $MSE = 9247.9581$, $PSNR = 8.5151$, and Entropy, $E = 7.9971$ declare the efficiency and security of the proposed algorithm. Hence, the proposed technique for image encryption provides extra layers of image security and is capable of preventing the hackers against brute-force attacks and encounters differential attacks.

10 Future Research Scope

In the current times, tremendous amount of digital data is transmitted over the internet. Researchers have proposed numerous image encryption schemes in the literature. A key concern is ensuring the secure and rapid transmission of digital data. In future, we aim to reduce the overall computational cost by employing more effective tools and mathematical methods. Additionally, we will investigate other chaotic maps to develop efficient and secure image encryption algorithms. We will concentrate on the small devices to identify secure encryption methods tailored for these devices. Further, our aim is to investigate more efficient and reliable methods for managing security of 3-D images.

References

[1] Muhammad Akraam, Tabasam Rashid, and Sohail Zafar, *A chaos-based image encryption scheme is proposed using multiple chaotic maps*, Mathematical Problems in Engineering **2023** (2023), no. 1, 2003724.

[2] Wassim Alexan, Dina El-Damak, and Mohamed Gabr, *Image encryption based on fourier-dna coding for hyperchaotic chen system, chen-based binary quantization s-box, and variable-base modulo operation*, IEEE Access (2024).

[3] Dana Sairangazhykyzy Amirkhanova, Maksim Iavich, and Orken Mamyrbayev, *Lattice-based post-quantum public key encryption scheme using elgamal's principles*, Cryptography **8** (2024), no. 3, 31.

[4] Adel A Bahaddad, Khalid Ali Almarhabi, and Sayed Abdel-Khalek, *Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption*, Alexandria Engineering Journal **75** (2023), 41–54.

[5] Hidayet Çelik and Nurettin Doğan, *A hybrid color image encryption method based on extended logistic map*, Multimedia Tools and Applications **83** (2024), no. 5, 12627–12650.

[6] A Yousefian Darani, Y Khedmati Yengejeh, H Pakmanesh, and G Navarro, *Image encryption algorithm based on a new 3d chaotic system using cellular automata*, Chaos, Solitons & Fractals **179** (2024), 114396.

[7] Kaushik Deb, Md. Sajib Al-Seraj, Md. Moshiul Hoque, and Md. Iqbal Hasan Sarkar, *Combined dwt-dct based digital image watermarking technique for copyright protection*, 2012 7th international conference on electrical and computer engineering, 2012, pp. 458–461.

[8] Li-Hua Gong, Xiang-Tao He, Shan Cheng, Tian-Xiang Hua, and Nan-Run Zhou, *Quantum image encryption algorithm based on quantum image xor operations*, International Journal of Theoretical Physics **55** (2016), 3234–3250.

[9] Hayder Raheem Hashim and Irtifaa Abdalkadum Neamaa, *Image encryption and decryption in a modification of elgamal cryptosystem in matlab*, arXiv preprint arXiv:1412.8490 (2014).

[10] Houcemeddine Hermassi, Rhouma Rhouma, and Safya Belghith, *A modified hyperchaos based image cryptosystem*, 2009 6th international multi-conference on systems, signals and devices, 2009, pp. 1–6.

[11] Bhat Jasra and Ayaz Hassan Moon, *Color image encryption and authentication using dynamic dna encoding and hyper chaotic system*, Expert Systems with Applications **206** (2022), 117861.

[12] Donghua Jiang, Nestor Tsafack, Wadii Boulila, Jawad Ahmad, and JJ Barba-Franco, *Asb-cs: Adaptive sparse basis compressive sensing model and its application to medical image encryption*, Expert Systems with Applications **236** (2024), 121378.

[13] Manjit Kaur and Vijay Kumar, *Adaptive differential evolution-based lorenz chaotic system for image encryption*, Arabian Journal for Science and Engineering **43** (2018), no. 12, 8127–8144.

[14] Omer Kocak, Uğur Erkan, Abdurrahim Toktas, and Suo Gao, *Pso-based image encryption scheme using modular integrated logistic exponential map*, Expert Systems with Applications **237** (2024), 121452.

[15] Sanjay Kumar and Deepmala Sharma, *A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm*, Artificial Intelligence Review **57** (2024), no. 4, 87.

[16] Chih-Chin Lai and Cheng-Chih Tsai, *Digital image watermarking using discrete wavelet transform and singular value decomposition*, IEEE Transactions on instrumentation and measurement **59** (2010), no. 11, 3060–3063.

[17] Dolendro Singh Laiphrakpam and Manglem Singh Khumanthem, *Medical image encryption based on improved elgamal encryption technique*, Optik **147** (2017), 88–102.

[18] Qingfeng Li and Lei Chen, *An image encryption algorithm based on 6-dimensional hyper chaotic system and dna encoding*, Multimedia Tools and Applications **83** (2024), no. 2, 5351–5368.

[19] Xiao-Wei Li and In-Kwon Lee, *Modified computational integral imaging-based double image encryption using fractional fourier transform*, Optics and Lasers in Engineering **66** (2015), 112–121.

[20] Yanbin Li, Feng Zhang, Yuanchao Li, and Ran Tao, *Asymmetric multiple-image encryption based on the cascaded fractional fourier transform*, Optics and Lasers in Engineering **72** (2015), 18–25.

[21] Zhengjun Liu, Lie Xu, Ting Liu, Hang Chen, Pengfei Li, Chuang Lin, and Shutian Liu, *Color image encryption by using arnold transform and color-blend operation in discrete cosine transform domains*, Optics Communications **284** (2011), no. 1, 123–128.

[22] Parveiz Nazir Lone, Deep Singh, and Umar Hussain Mir, *A novel image encryption using random matrix affine cipher and the chaotic maps*, Journal of Modern Optics **68** (2021), no. 10, 507–521.

[23] Yuling Luo, Minghui Du, and Junxiu Liu, *A symmetrical image encryption scheme in wavelet and time domain*, Communications in Nonlinear Science and Numerical Simulation **20** (2015), no. 2, 447–460.

[24] Umar Hussain Mir, Parveiz Nazir Lone, Deep Singh, and DC Mishra, *A public and private key image encryption by modified approach of vigener cipher and the chaotic maps*, The Imaging Science Journal (2023), 1–15.

[25] Umar Hussain Mir, Deep Singh, and Parveiz Nazir Lone, *Color image encryption using rsa cryptosystem with a chaotic map in hartley domain*, Information Security Journal: A Global Perspective **31** (2022), no. 1, 49–63.

[26] Rose Mohammed and L Mohammed Jawad, *Secure image encryption scheme using chaotic maps and rc4 algorithm*, Solid State Technology **63** (2020), no. 3, 3465–3449.

[27] Bhaskar Mondal and Tarni Mandal, *A light weight secure image encryption scheme based on chaos & dna computing*, Journal of King Saud University - Computer and Information Sciences **29** (2017), no. 4, 499–504.

[28] Nouioua Nadhir, Seddiki Ali, and Ghaz Abdelkrim, *Medical image watermarking scheme in transform domain based on asymmetric crypto-system and arnold chaotic map*, 2021 44th international conference on telecommunications and signal processing (tsp), 2021, pp. 267–272.

[29] Ying Niu, Hangyu Zhou, and Xuncai Zhang, *Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators*, Scientific Reports **14** (2024), no. 1, 7033.

[30] Ying Qin and Bob Zhang, *Privacy-preserving biometrics image encryption and digital signature technique using arnold and elgamal*, Applied Sciences **13** (2023), no. 14, 8117.

[31] Morteza SaberiKamarposhti, Mahdi Sahlabadi, Chia-Chen Lin, and Ravie Chandren Muniyand, *Using 2d hénon map, cycling chaos and dna sequence for new secure color image encryption algorithm*, Arabian Journal for Science and Engineering **49** (2024), no. 3, 4125–4137.

[32] Deep Singh and Sandeep Kumar, *A multiphase encryption scheme using rsa, modified rmac and chen's hyperchaotic map*, Multimedia Tools and Applications **83** (2024), no. 19, 57059–57088.

[33] Wei Song, Chong Fu, Yu Zheng, Ming Tie, Jun Liu, and Junxin Chen, *A parallel image encryption algorithm using intra bitplane scrambling*, Mathematics and Computers in Simulation **204** (2023), 71–88.

[34] Yining Su, Xingyuan Wang, Mingxiao Xu, Chengye Zou, and Hongjun Liu, *A three-dimensional (3d) space permutation and diffusion technique for chaotic image encryption using merkel tree and dna code*, Sensing and Imaging **24** (2023), no. 1, 5.

[35] Junwei Sun, Chuangchuang Li, Zicheng Wang, and Yanfeng Wang, *Dynamic analysis of hr-fn-hr neural network coupled by locally active hyperbolic memristors and encryption application based on knuth-durstenfeld algorithm*, Applied Mathematical Modelling **121** (2023), 463–483.

[36] Shuliang Sun, *Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules*, Optical Engineering **56** (2017), no. 11, 116117–116117.

[37] Ankita Vaish, *An error free and key sensitive color image encryption using sine powered map and arnold transform in stockwell domain*, Multimedia Tools and Applications (2023), 1–19.

[38] M Vijayakumar and A Ahilan, *An optimized chaotic s-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map*, Ain Shams Engineering Journal **15** (2024), no. 4, 102620.

[39] Chao Wang and Ling Song, *An image encryption scheme based on chaotic system and compressed sensing for multiple application scenarios*, Information Sciences **642** (2023), 119166.

[40] Xiaopeng Wei, Ling Guo, Qiang Zhang, Jianxin Zhang, and Shiguo Lian, *A novel color image encryption algorithm based on dna sequence operation and hyper-chaotic system*, Journal of Systems and Software **85** (2012), no. 2, 290–299.

[41] Kuan-Wai Wong, Wun-She Yap, Bok-Min Goi, Denis C-K Wong, and Guodong Ye, *Cryptanalysis of an image encryption scheme based on two-point diffusion strategy and henon map*, Journal of Information Security and Applications **81** (2024), 103692.

[42] Quan Xu, Xiongjian Chen, Bei Chen, Huagan Wu, Ze Li, and Han Bao, *Dynamical analysis of an improved fitzhugh-nagumo neuron model with multiplier-free implementation*, Nonlinear Dynamics **111** (2023), no. 9, 8737–8749.

[43] Fei Yu, Si Xu, Xiaoli Xiao, Wei Yao, Yuanyuan Huang, Shuo Cai, Bo Yin, and Yi Li, *Dynamics analysis, fpga realization and image encryption application of a 5d memristive exponential hyperchaotic system*, Integration **90** (2023), 58–70.

[44] Hangming Zhang and Hanping Hu, *An image encryption algorithm based on a compound-coupled chaotic system*, Digital Signal Processing **146** (2024), 104367.

[45] Qiang Zhang, Ling Guo, and Xiaopeng Wei, *Image encryption using dna addition combining with chaotic maps*, Mathematical and Computer Modelling **52** (2010), no. 11-12, 2028–2035.

[46] Qiang Zhang, Lili Liu, and Xiaopeng Wei, *Improved algorithm for image encryption based on dna encoding and multi-chaotic maps*, AEU-International Journal of Electronics and Communications **68** (2014), no. 3, 186–192.

[47] Nan-Run Zhou, Long-Long Hu, Zhi-Wen Huang, Meng-Meng Wang, and Guang-Sheng Luo, *Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm*, Expert Systems with Applications **238** (2024), 122052.

[48] Shuang Zhou, Xingyuan Wang, and Yingqian Zhang, *Novel image encryption scheme based on chaotic signals with finite-precision error*, Information Sciences **621** (2023), 782–798.

Author information

D. Singh, School of Undergraduate Studies, Dr. B.R. Ambedkar University Delhi, Delhi-6
Department of Mathematics and Statistics, Central University of Punjab, Bathinda, Punjab, India.
E-mail: deepsinghspn@gmail.com

M. K. Patel, Department of Mathematics, National Institute of Technology, Nagaland, India.
E-mail: mkpitb@gmail.com

N. Khaitan*, School of Engineering, P P Savani University, Kosamba, Surat, Gujarat
Department of Mathematics and Statistics, Central University of Punjab, Bathinda, India.
E-mail: khaitan2709@gmail.com

Received: 2024-04-01.
Accepted: 2025-02-28