Image Encryption Model based on Chaotic Maps and Group Learning Algorithm

[1]Dr. Gagandeep Kaur, [2]Dr. Sachin Kumar

[1]Post Doctoral Research Fellow, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India. gagankaur.0813@gmail.com

[2]Associate Professor, Dept. of Information Technology, Management Education & Research Institute, Affiliated to GGSIP University, New Delhi, India. sachinks.78@gmail.com

Abstract: Nowadays, digital images are used in several applications to communicate the information. Therefore, we employ image encryption methods to safeguard the information. Furthermore, chaotic maps have gained popularity in image encryption (IE) methods due to their improved security. Therefore, in this paper, we have proposed an optimized color IE model using the 3-D chaotic logistic map (CLM) and 1-D chaotic tent map (CTM). We employ the 3-D CLM for random key generation, while the 1-D CTM generates the shuffle indexes of the secret image. Furthermore, we incorporate a group learning (GL) algorithm to refine the initial set of parameters of the 3-D CLM. Moreover, in this research, a multi-objective is developed for the GL algorithm using various security parameters, namely, entropy, SSIM, and CC. In the encryption process, different planes of the secret color image are extracted, and performed operation with the random key is generated with 3-D CLM algorithm and shuffled the image based on the shuffling index is given by 1-D CTM. Next, the proposed IE model is evaluated for several images based on visual quality analysis and analysing the encrypted image (EI) characteristics with secret image (SI). Thus, the encrypted image histograms are completely distributed, as anticipated by the encryption model. In addition, the proposed IE model met the desired security benchmark parameters, namely, CC, SSIM, PSNR, and entropy in the range of $+0.006$ to -0.00231, $0\ to\ 0.011133$, $8.57 - 23.93dB$, and $7.9948 - 7.9971$, respectively. Finally, we used the entropy and CC parameters are used to evaluate the proposed IE model over others.

Keywords: Attack, Chaotic, Encryption, Entropy, GLA, Logistic, Metaheuristic, Multi-Objective, Security, Tent Map.

1. Introduction

Due to the exponential growth of internet technology in recent years, the amount of data communicated online has increased significantly [1]. The data is available in various forms but in the present scenario images are the most preferred form to communicate information in different applications, such as healthcare, defense, and social media [2]. However, data leakage occurs while transmitting the information through the internet, and it is prone to various attacks [3]. Attacks might be either passive or active, according to the literature [4-5]. In a passive attack, the attacker only monitors the data communication on the internet, such as in an eavesdropping attack. On the other side, in an active attack, the attacker tries to modify or temper the data. The most popular attacks in the image encryption models are statistical and differential attack. To overcome these attacks, security characteristics are taken into consideration by image encryption methods is given below [6–8].

- **Confidentiality:** Maintaining a level of secrecy is crucial to preventing sensitive information from falling into the wrong hands. Keeping information safe as it is stored, transmitted, and processed is essential. Encryption, access restrictions, and data masking are all methods often employed to protect sensitive information.
- **Integrity:** It is crucial to maintain data integrity to rule out the possibility of any unauthorized changes or manipulations. This involves keeping information safe from being altered, erased, or added to without permission. Digital signatures, authentication for message codes, and data hashing are all examples of popular methods for ensuring data security.
- **Availability** refers to the state of being available for usage by authorized users at any time. This involves doing things like guarding against DoS attacks and making sure your systems are highly accessible and fail-safe. Load balancing, redundant systems, and backup plans are just a few examples of the kinds of approaches used to guarantee availability.
- **Authenticity:** Information and communication should originate from a reliable source, therefore, verifying their authenticity is crucial. Among the forms of identity fraud that need to be guarded against are impersonation and spoofing. The terms "authentication," "digital certificates," and "biometric identification" all refer to methods used to verify a person's identity.

- **Non-repudiation:** It is crucial that a communication or transaction be non-repudiable so that neither side can deny sending or receiving it. This includes safeguarding against replay attacks as well as message manipulation. Digital signatures, message authentication codes, and timestamps are only a few examples of the tools often employed to guarantee the irrefutability of a transaction.

These security characteristics are achieved using various security methods, such as encryption, and steganography [9–10]. The encryption methods scramble the data, whereas steganography methods conceal the data in some cover media [11–12]. Out of these methods, encryption is preferred over steganography because data is scrambled, and descrambling is only possible for someone who knows the secret key. Thus, in this paper, research is carried out on encryption methods. In the IE method, random key and encryption method is incorporated to scramble the confidential image (CI). On the receiver end, same key incorporated with decryption method to recover the CI, as shown in Figure 1[11]. If the encryption and decryption methods use the same key it is known as symmetric encryption; otherwise, it is asymmetric.

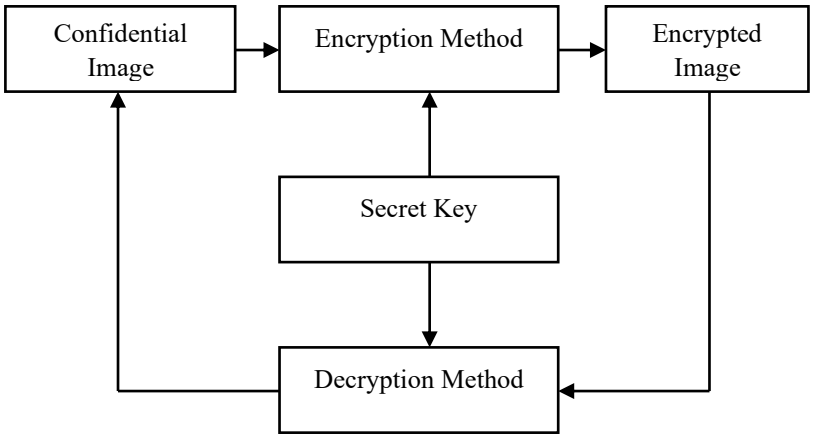


Figure 1. Schematic Representation of Encryption and Decryption Method

In the present era, the chaotic maps are gained popularity to encrypt the secret image due to high security and computational efficiency [13-16]. Further, the selection of the initial parameter is the cornerstone of the success of chaotic map in securing the secret image. Hence, metaheuristic algorithms are utilized to find the parameter values of the chaotic map. However, in the literature, several metaheuristic algorithms are available [17]. Therefore, the purpose of this investigation is to choose the best metaheuristic algorithm among the *n* number of metaheuristic algorithms are available in the literature which required the minimum parameter tuning, better exploration and exploitation rate, and provide global solution. After that, it is employed in the proposed IE model for search the best parameters of the CLM algorithm. The main contribution of this paper is summarized below.

- We have developed a random key generation method using 3-D CLM and GLA algorithm to encrypt the different planes of the color image.
- We have developed a multi-objective function using three security parameters, namely, E, CC, and SSIM to determine the best initial parameters of the CLM algorithm.
- We have developed a shuffling index matrix for shuffle the encrypted image using the 1-D CTM algorithm.
- The IE model provides the robustness against various attacks when it is evaluated based on different parameters and compared with the existing models.

Here are the sections that follow in this paper. Section 2 shows the related work is done in the IE. Section 3 defines the methodology part in which dataset, algorithms employed to design proposed IE model, and performance metrics are explained. Section 4 shows the proposed optimized IE model. Section 5 defines the results and discussion part for the proposed model. Section 6, eventually draw the conclusion.

2. Related Work

This section presents the image encryption models are proposed in the literature. Kumar et al. [18], used the BWO and 1-D CLM algorithm for encrypt the confidential grey-scale images. They have chosen the BWO algorithm over GA due to better convergence rate to find the parameters. Besides that, they have designed a single objective function (OF) based on entropy. Furthermore, N. Kumar and S. Saini [19-20], designed two encryption models by utilizing the CM and metaheuristic algorithms. In the first model, they have used 3-D CLM and JAYA algorithm

for encrypt the different planes of the color image by generating the different keys whereas in the second model, used the 2-D chaotic Henon map and TAO algorithm for encrypt the grey-scale images. In both models, entropy is used as OF. Next, Kaur et al. [21], used the 3-D CLM and OOA algorithm for encrypt the color images by considering the two parameters, CC and SSIM as the objective function. Further, recently, Sameh et al. [22], used the eight chaotic maps and several metaheuristic algorithms for encrypt the images to overcome the differential attack. Xu et al. [23] developed a reversible data hiding method in which data is encrypted by performing the permutation of the secret data blocks. Next, Almasoud et al. [24], presented an IE model, by utilizing the hash function for key generation, metaheuristic bonobo optimizer for block substitution, and DNA encoding for permutation purposes. Khalaf et al. [25], developed an IE model by optimizing the CLM algorihm using the grasshopper optimization by considering the correlation coefficient as the objective function. Elkahil et al. [26], utilized the 2-D beta chaotic map for generate the different stages, namely, permutation and substitution for image encryption. Wang et al. [27], considered the metaheuristic PSO algorithm to find tune the chaotic map for key generation purposes in the IE method.

From the above studies, we have found the following key points.

- In the literature, several metaheuristic algorithms are used to adjust the parameters of the CM algorithm for key generation. However, the selection of the metaheuristic algorithm is a challenging task because number of parameters are involvement in it based on it, it searches the solution space for optimal solution. For example, in the GA, mutation rate and crossover, in BWO algorithm, procreate, cannibalism, and mutation rate, in TAO algorithm, elimination alate and adaption factor need to define. Further, based on the searching process which is define the exploration rate of the algorithm, these algorithms are differentiated from each other.
- Next, in the metaheuristic algorithms, objective function plays an important role because based on its fine tuning of the parameters is done. In the literature, entropy, CC, and SSIM are the used to design the single or dual objective function.

Based on the above key points, in this research, we have proposed an optimized image encryption model in which best metaheuristic algorithm is chosen which required the minimum parameter tuning and provides better exploration rate to search the solution space. Further, we have proposed a multi-objective function by considering the multiple parameters.

3. Methodology

In this section gives an overview of the dataset, followed by chaotic maps (3-D CLP and CTM), GLA, and performance measure metrics are utilized for evaluate the image encryption model.

- **Dataset:** In the IE models, the USC SIPI Image database is the most chosen database in the literature. Further, different standard sizes (256×256,512×512 and 1024×1024) are available. In this research, several color images are considered to evaluate the proposed model [28].
- **3-D CLM Algorithm**: The basic equation of 1-D and 3-D CLM is determined using Eq. (1-4) [29].

$$x_n = \mu x_n(1 - x_n) \tag{1}$$

$$x_{n+1} = \alpha x_n(1 - x_n) + \beta y_n^2 x_n + \gamma z_n^3 \tag{2}$$

$$y_{n+1} = \alpha y_n(1 - y_n) + \beta z_n^2 y_n + \gamma x_n^3 \tag{3}$$

$$z_{n+1} = \alpha z_n(1 - z_n) + \beta x_n^2 z_n + \gamma y_n^3 \tag{4}$$

In Eq. (1), $0< x <1$ and μ = {3.57-3.99}. In contrast, Eq. (2-4), α={3.68-3.99}, β= {0-0.022}, γ= {0-0.015}. In this research, metaheuristic algorithm is used to fine tune the 3-D CLM algorithm by determining the parameter values of αβγ.

- **GLA**: The GLA mimics how managers and group leaders influence the skills of their members [30]. In contrast to previous algorithms, this one separates the population into many equal groups, chooses a few people to lead each group according to their fitness. This also determines the manager who is the person with the highest fitness level among all the people. The following are the proposed algorithm's key features:

  Initially, the population is generated at random.

- The best person, or the most fit person in the whole population, takes over as manager of all the other people.
- Several groups are represented by the whole population (four groups were considered in this study).
- The leader of each group is the superior member, or the one who is the most suited inside the group.
- Each group leader has an impact on the other members of the group.
- The manager influences other people as well as the group leaders.
- The process of mutation is used to randomly alter an individual's structure.

The GL algorithm's pseudocode is finally provided here.

Table 1. Pseudocode of the GL Algorithm [22]

1. Initialize the GLA algorithm Parameters, Population, iteration, and mutation rate 2. Create a random population according to the population size 3. Determine the manager based on which population is better among others. 4. Split the population into groups and each group leader is determined. 5. The GLA algorithm is iterated for fixed number of iterations according the iteration parameter. Calculate the impact of managers on group leader (using Eq. (5)). Calculate the impact of group leader on the group members (using Eq. (6)). Calculate the impact of managers on the group members (using Eq. (7)). 6. Mutate the population according to the mutation rate. 7. The optimal solution is the manager population.

$$LA = (x - y) \times r \tag{5}$$

In above Eq. (5), xy denotes the group leader and manager. Further, r denotes the random number between 0 and 1, and LA is the new group leader after the manager's influence.

$$newpop(i) = (LA - pop(i)) \times r \tag{6}$$

In above Eq. (6), LA determined from Eq. (5) and new population generated is with the help of it. Further, pop(i) is an individual inside the group, i ∈n, n is the group size.

$$new\_Individual(i) = (pop(i) - y) \times r \tag{7}$$

In above Eq. (7), new individual in the group are determined by utilizing the previous two equations.

- **1-D Chaotic Tent Map**: In this research, 1-D CTM is used for generate shuffling index in the proposed IE model. The CTM is determined using Eq. (8-9) [31].

$$x_{i+1} = f(x_i, \mu) \tag{8}$$

$$f(x_i, \mu) = \begin{cases} f(x_i, \mu) = \mu x_i & if\ (x_i < 0.5) \\ f(x_i, \mu) = \mu(1 - x_i) & Otherwise \end{cases} \tag{9}$$

In Eq. (8-9), x_i, x_{i+1}represents the present and next state. On the other hand, μ denotes the control parameter.

- **Performance Metrics**: In this paper, the proposed model is evaluated by various parameters to show its robustness against statistical attack. The parameters are evaluated in the statistical attack are MSE, RMSE, PSNR, SSIM, CC, MD, and execution time. The detailed description of these parameters is given below [32-35].

Table 2. Performance Metrics

Parameter	Equation
E	$E_s = \sum_{i=0}^{2^k-1} p(s_i) \times \log_2 \frac{1}{p(s_i)}$ (9)
CC	$r_{\gamma\beta} = \frac{cov(\gamma\beta)}{\sqrt{D(\gamma)}\sqrt{D(\beta)}}$ (10) $EE(\gamma) = \frac{1}{N}\sum_{i=1}^{N} \gamma_i$ (11) $D(\gamma) = \frac{1}{N}\sum_{i=1}^{N} (\gamma_i - EE(\gamma))^2$ (12) $cov(\gamma\beta) = \frac{1}{N}\sum_{i=1}^{N} (\gamma_i - EE(\gamma)(\beta_i - EE(\beta)))$ (13)

	In above Eq. covariance, variance, and mean is represented by $\gamma\beta, D(\gamma), EE(\gamma)$, respectively.
MSE	$MSE = \frac{1}{WH}\sum_{i=1}^{W}\sum_{j=1}^{H}[I_{ij} - K_{ij}]^2$ (14)
RMSE	RMSE=$\sqrt{MSE}$ (15)
PSNR	$PSNR = 20 \times \log_{10}(\frac{255}{\sqrt{MSE}})$ (16)
MD	$MD = \frac{H_0 - H_{L-1}}{2} + \sum_{i=1}^{L-2} H_i$ (17) In Eq. (17), H_i denotes the histogram difference between images whereas $L \in \{0 - 255\}$ denotes the total intensity level presents in the image. In the ideal case, high value of maximum deviation required for better security.
Time Complexity	In this parameter, the total amount of time that encryption takes to execute is determined.

4. Proposed Image Encryption Model

The main motive of this research is to optimized the image encryption model to enhance the security. To accomplish this goal, 3D CLM, 1-D CTM, and metaheuristic GL algorithm is taken into consideration. Next, the flowchart of the proposed IE model is shown in Figure 2.

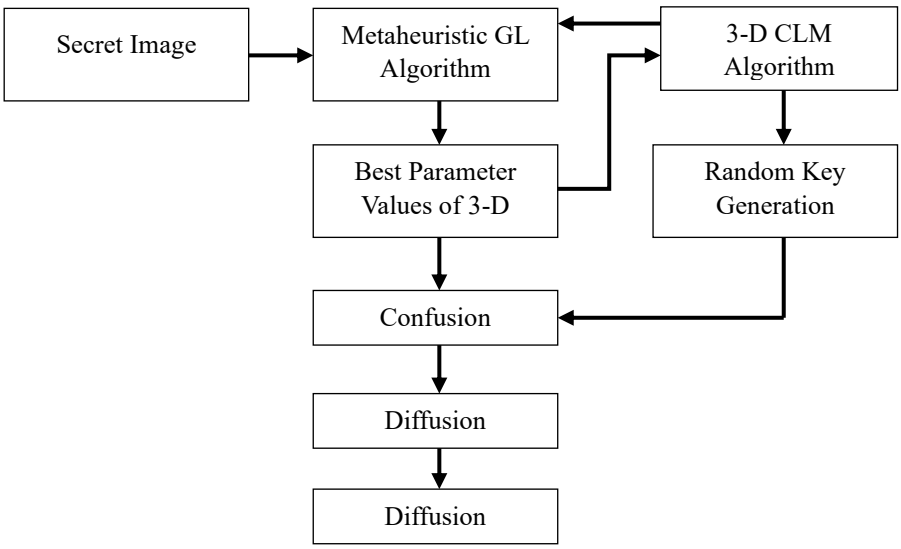


Figure 2. Flowchart of the Proposed Image Encryption Model

Initially, the secret image is read. Further, it is given to the GL algorithm along with 3-D CLM algorithm. The next step is for the GL algorithm to find the optimal values by exploring the solution space based on lower and upper bound and then evaluated using the objective function. In this research, we have developed a multi-objective function using the three security parameters, namely, E, SSIM, and CC. The equation of the proposed multi-objective function is shown below.

$$OF = \frac{\frac{E}{8} + (|1 - CC|) + (1 - SSIM)}{3} \quad (18)$$

In the IE model, the entropy of an image is varied between 1-8 whereas a high value near to 8 is required for good encryption. On the other hand, CC and SSIM value of an image is varied between -1 to 1 and 0-1, respectively. In the ideal case, CC and SSIM value near to 0 is required for encryption models. Therefore, in this research, these parameters are normalized in the 0-1 range by dividing the entropy value by 8 and taking the absolute difference of CC. Further, in this research work, the OF function is maximized. After determining the best parameter values, it is given to the 3D CLM algorithm. The 3D CLM algorithm generates the three random keys based on these parameter values. The random keys along with secret image is given to the confusion matrix in which exclusive-OR operation is performed between them. In the next step, the diffusion is performed by shuffling the image matrix in the horizontal and vertical direction based on the shuffling index value. The shuffling index value for

the image matrix is determined using the CTM algorithm. In this algorithm, a random sequence is generated. After that the random sequence is sorted and shuffling index is determined. On the receiver side, to decrypt the secret image, the initial parameters value of the 3-D CLM, 1-D CTM needs to communicate to the receiver along with the encrypted image. After that, reverse steps need to carry out which is performed on the encryption model in the reverse order. Table 3-4 shows the pseudocodes for the GLM and CTM algorithm for determine best parameter value and shuffling index value.

Table 3. Pseudocode for GLA Algorithm for the Proposed IE Model

Input: CLM Parameters, xyz={0-1}, α={3.68-3.99}, β= {0-0.022}, γ= {0-0.015}, Population, Dimension of the Population, Iteration size (IS), mutation rate, groups, and OF
Output: Best Parameter values of CLM
1. Create a random population according to the population size and its dimension.
2. Fitness evaluation of the population using OF.
3. Determine the manager which population gives maximum value of the OF
4. Split the population into groups.
5. Determine the group leader based on which population outperforms over other
6. The GLA algorithm is iterated according to the IS. Determine the impact of manager on group leaders, group leader and manager impact on the members
7. Determine the best parameter values which is basically manager population

Table 4. Pseudocode for CTM Algorithm for the Proposed IE Model

Input: Tent Map Parameters: $x: [0-1], r: [1.4-2]$
Output: Shuffling Index for row and column of the Image
1. Initially, generate the random $x\ and\ r$.
2. Generate the random sequence using Eq. (9).
3. After sorting the random sequence, find its index values.
4. According to the sequence, the image matrix is row-wise and column-wise is shuffled.

5. Results and Discussion

This part of the research work shows the examining of the proposed IE model for various color images. In this work, MATLAB 2018a software is employed for simulation purposes due to huge inbuilt library and functions of image processing. The hardware configuration to simulate the proposed model is i7 processor, 64-bit window operating system, 8GB RAM. Further, in this section, ten color images are considered to show the evaluation of the proposed IE model.

5.1 Simulation Setup Configuration

In this research, the security of the IE model is enhanced by finding the best parameters of the CLM algorithm for image encryption. To carry out this goal, the GL algorithm need to setup according to the CLM algorithm, as shown in Table 5.

Table 5 Preliminary GL Algorithm Parameter Value

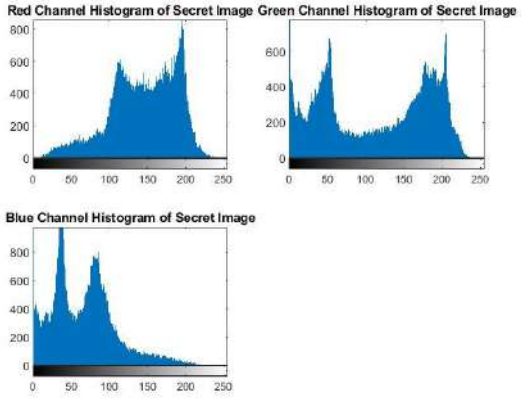
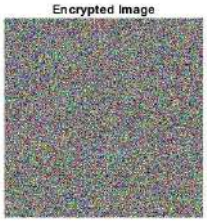
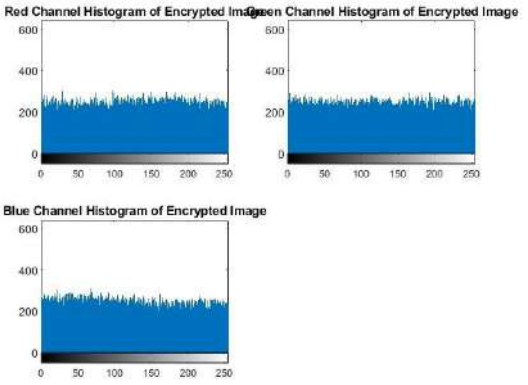
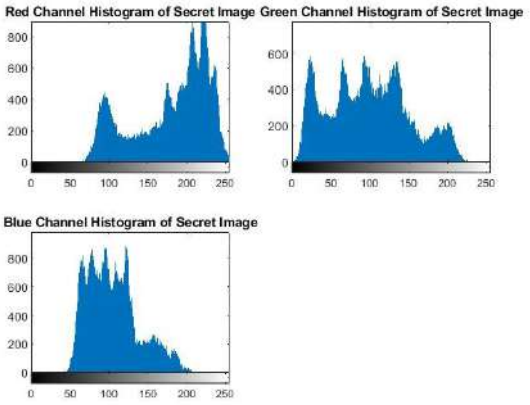
Parameter	Value
P	[10]
P_{dim}	[3]
I	[30]
Total no. of Groups	[4]
OF	E, CC, and SSIM
MR	0.1

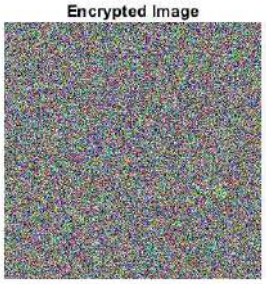
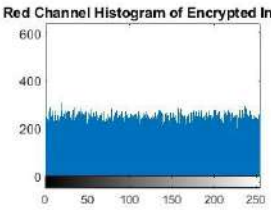
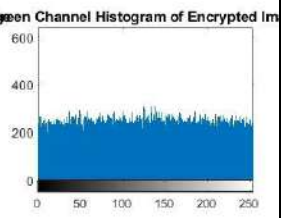
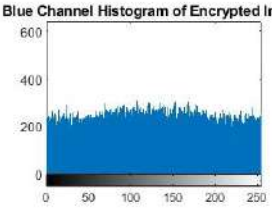
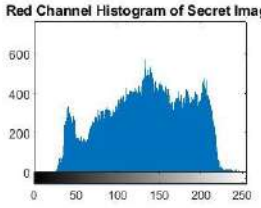
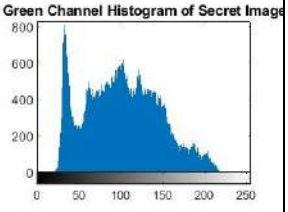
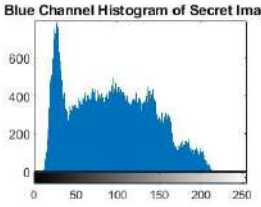
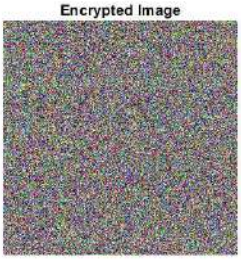
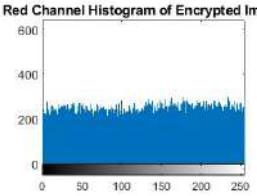
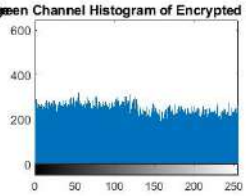
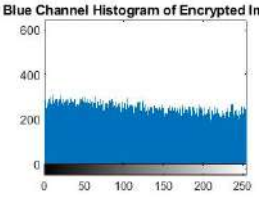
5.2 Visual Quality Analysis of the Proposed IE Model

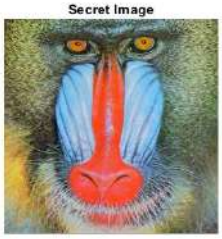
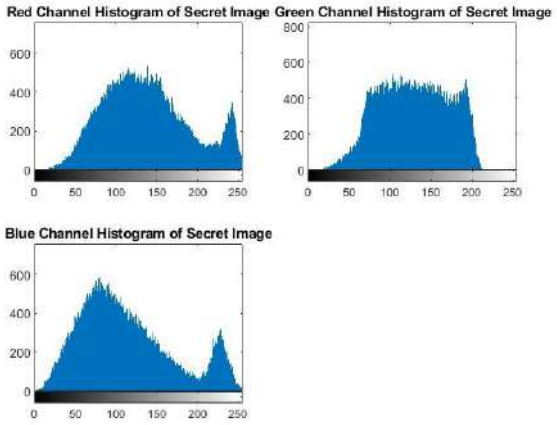
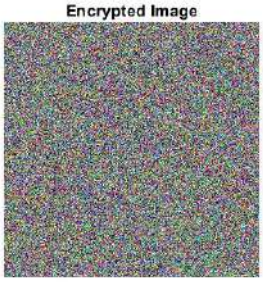
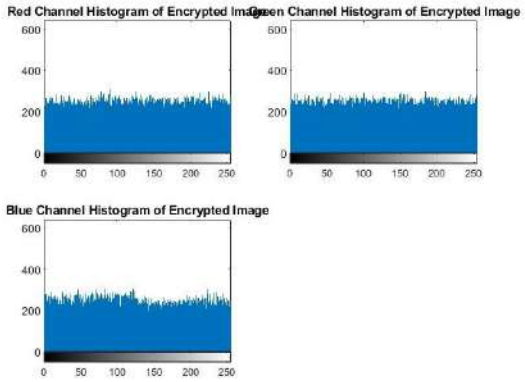
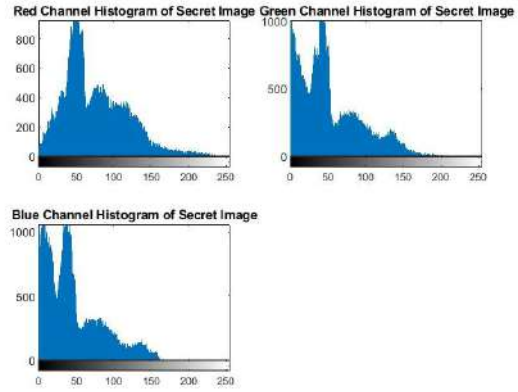
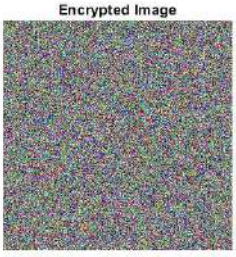
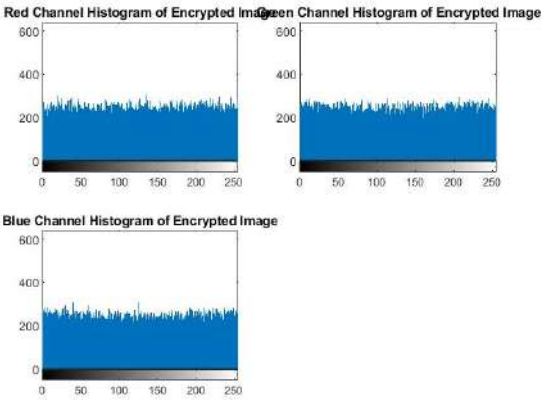
Here, the EI and its histogram are compared to the SI in terms of visual quality. If the EI is noisy and has evenly distributed histogram, then the encryption is good according to the IE Model. Table 6 shows the visual quality analysis of the different secret images for the proposed IE Model. The results indicate that the encrypted images

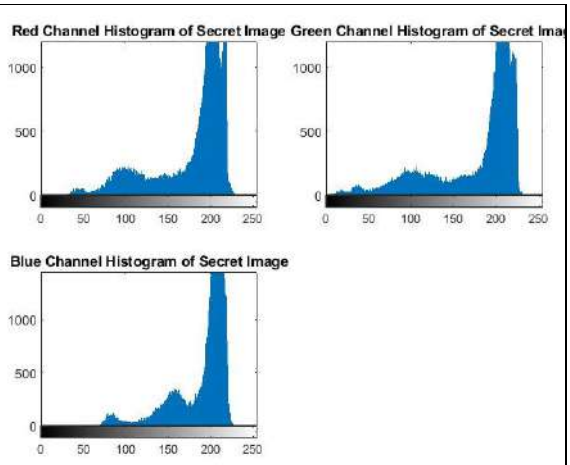
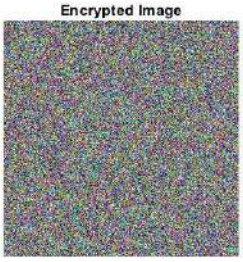
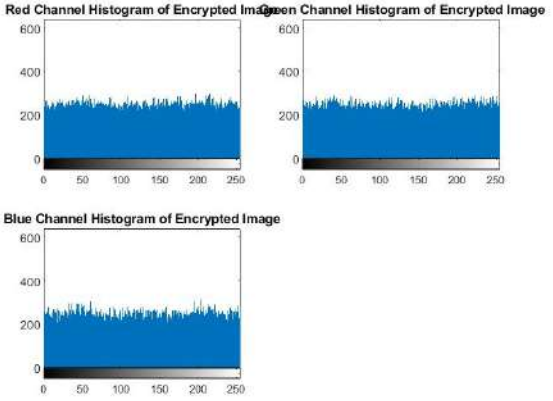
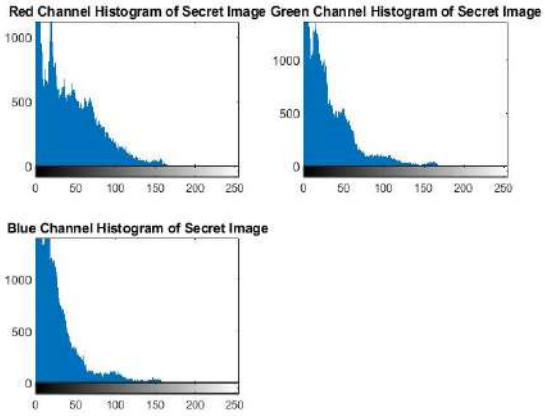
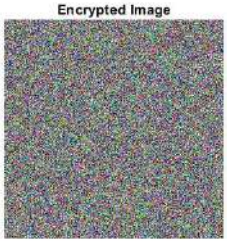
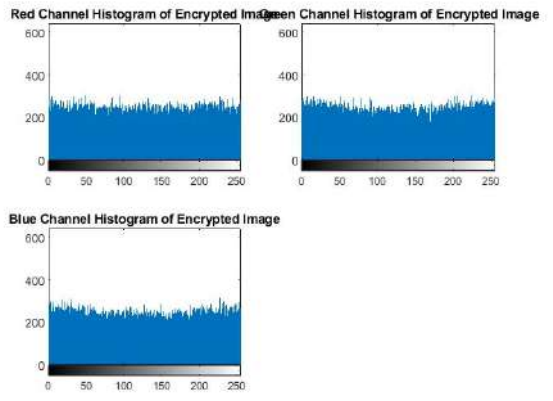
look noisy when it is compared with secret image. On the other hand, the histogram of the encrypted image is equally distributed when it is compared with the histogram of the secret image.

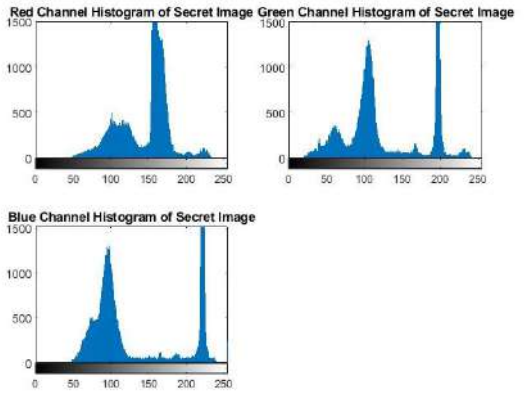
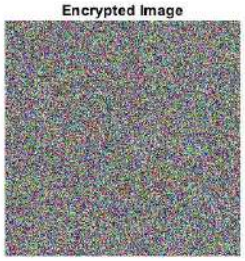
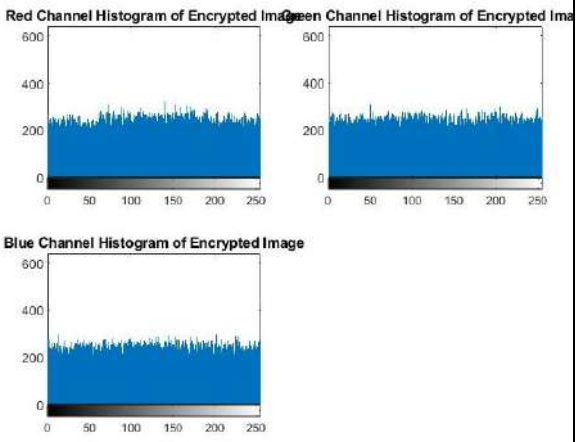
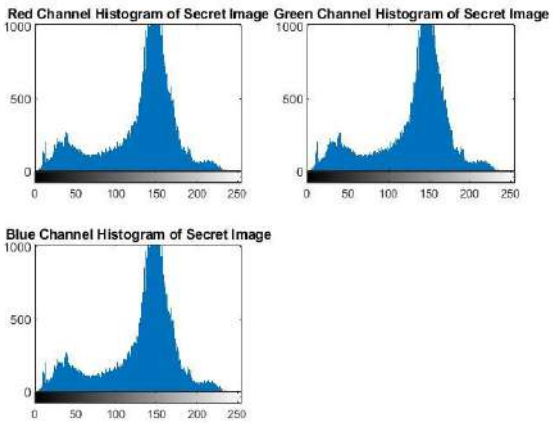
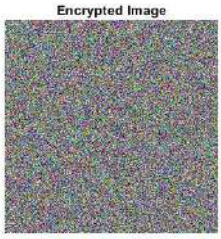
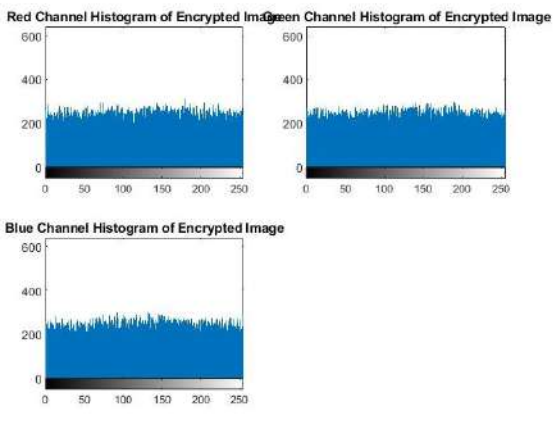
Table 6. Visual Quality Analysis of the Proposed IE Model

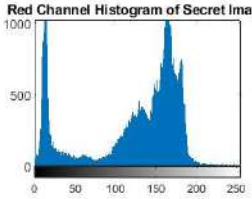
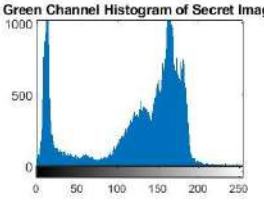
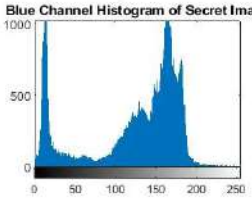
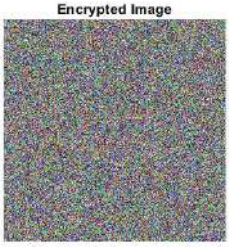
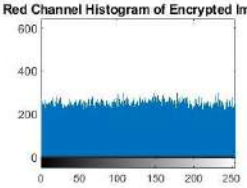
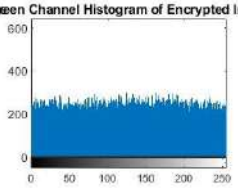
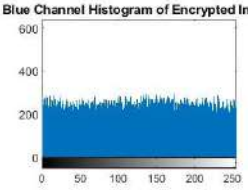
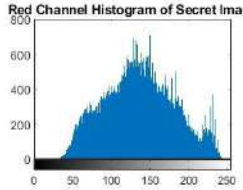
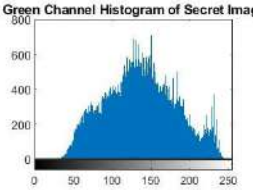
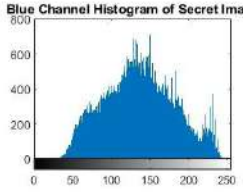
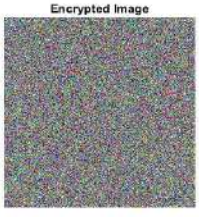
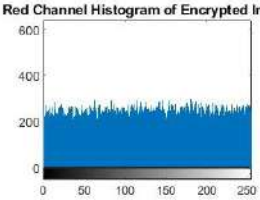
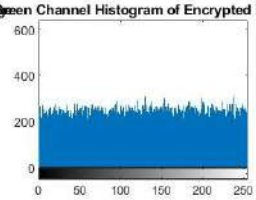
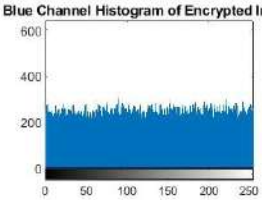
Images	Image Quality	Histogram Analysis
Pepper		
		
Lena		

	Encrypted Image 	Red Channel Histogram of Encrypted Image  Green Channel Histogram of Encrypted Im  Blue Channel Histogram of Encrypted Image 
Barbara	Secret Image 	Red Channel Histogram of Secret Image  Green Channel Histogram of Secret Image  Blue Channel Histogram of Secret Image 
	Encrypted Image 	Red Channel Histogram of Encrypted Image  Green Channel Histogram of Encrypted Image  Blue Channel Histogram of Encrypted Image 

Baboon	Secret Image 	
	Encrypted Image 	
Female	Secret Image 	
	Encrypted Image 	

Aeroplane	Secret Image 	
	Encrypted Image 	
Couple	Secret Image 	
	Encrypted Image 	

House	 Secret Image	 Red Channel Histogram of Secret Image Green Channel Histogram of Secret Image Blue Channel Histogram of Secret Image
	 Encrypted Image	 Red Channel Histogram of Encrypted Image Green Channel Histogram of Encrypted Ima Blue Channel Histogram of Encrypted Image
Boat	 Secret Image	 Red Channel Histogram of Secret Image Green Channel Histogram of Secret Image Blue Channel Histogram of Secret Image
	 Encrypted Image	 Red Channel Histogram of Encrypted Image Green Channel Histogram of Encrypted Image Blue Channel Histogram of Encrypted Image

Cameraman	Secret Image 	Red Channel Histogram of Secret Image  Green Channel Histogram of Secret Image  Blue Channel Histogram of Secret Image 
	Encrypted Image 	Red Channel Histogram of Encrypted Image  Green Channel Histogram of Encrypted Image  Blue Channel Histogram of Encrypted Image 
Elaine	Secret Image 	Red Channel Histogram of Secret Image  Green Channel Histogram of Secret Image  Blue Channel Histogram of Secret Image 
	Encrypted Image 	Red Channel Histogram of Encrypted Image  Green Channel Histogram of Encrypted Image  Blue Channel Histogram of Encrypted Image 

5.3 Performance Evaluation

This section shows the security parameters are evaluated for the proposed IE model by analysing the confidential and encrypted image characteristics. The security parameters are considered in this work is CC, SSIM, entropy, MD, MSE, RMSE, PSNR, and execution time. Table 7(a-b) displays the results of evaluating the proposed IE model for various images. In this table, each plane of the color image is evaluated using the different parameters and their average value is also shown. Further, analysis of these parameters is shown in Figures 3-7. Figure 3-4 shows the average CC ($+0.006$ to -0.00231) and SSIM ($0\ to\ 0.011133$) analysis for various images. This shows that the suggested IE model produces results close to the optimal value between the encrypted and secret images, with low CC and SSIM values. Further, comparison of secret and encrypted image entropy is illustrated in Figure 5. It appears that the suggested IE model gets a high value close to 8 for a variety of images, according to the results. Further, we have analysed the $female$ and $aeroplane$ images the highest entropy over other images. Figure 6 shows the average MD analysis for various images are used for evaluation purposes. The results indicates that the $couple$ image achieves the highest maximum deviation whereas $baboon$ image achieves the lowest. Further, Figure 7 illustrates the average PSNR for the different images. The $aeroplane$ image achieves the lowest PSNR over other, according to the results. This reflects that the $aeroplane$ image has maximum noise addition due to encryption process.

Table 7(a). Performance Evaluation of the Proposed IE Model

Images	Planes	CC	SSIM	Input Entropy	Output Entropy	MD	MSE	RMSE	PSNR (in dB)	Execution Time (in msec)
Pepper	R	0.0046	0.0088	7.3789	7.9967	5.12E+04	4.92E+03	70.1362	11.212	5.871038
	G	0.0017	0.0081	7.6462	7.9976	3.46E+04	4.14E+03	64.3698	11.9572	
	B	0.0038	0.0076	7.162	7.9962	5.42E+04	976.6323	31.2511	18.2335	
	Avg.	**0.003367**	**0.008167**	**7.3957**	**7.996833**	**4.67E+04**	**3.35E+03**	**55.25237**	**13.8009**	
Lena	R	-0.0032	0.0093	7.2469	7.997	51586	9.32E+03	96.517	8.4387	6.537958
	G	-2.50E-05	0.01	7.5733	7.9968	3.77E+04	2.35E+03	48.4466	14.4255	
	B	0.002	0.0114	6.9403	7.9951	6.39E+04	1.96E+03	44.2535	15.2119	
	Avg.	**-0.00041**	**0.010233**	**7.2535**	**7.9963**	**51071**	**4.54E+03**	**63.07237**	**12.69203**	
Barbara	R	8.45E-04	0.0097	7.5518	7.9967	37892	4.37E+03	66.1353	11.7221	5.914771
	G	-0.0022	0.0089	7.3756	7.9937	46985	2.38E+03	48.75	14.3713	
	B	-0.0014	0.0079	7.4773	7.994	4.04E+04	2.21E+03	47.0617	14.6774	
	Avg.	**-9.18E-04**	**0.008833**	**7.468233**	**7.9948**	**41764**	**2.99E+03**	**53.98233**	**13.59027**	
Baboon	R	-0.0117	0.0088	7.6439	7.9971	35692	5.02E+03	70.8633	11.1224	7.495777
	G	0.0025	0.0105	7.3529	7.9975	5.07E+04	3.68E+03	60.6893	12.4686	
	B	0.0023	0.0113	7.6786	7.9953	34263	3.66E+03	60.4959	12.4963	
	Avg.	**-0.0023**	**0.0102**	**7.558467**	**7.996633**	**40222.33**	**4.12E+03**	**64.01617**	**12.0291**	
Female	R	0.0047	0.0088	7.2761	7.997	52501	1.21E+03	34.7767	17.305	6.414011
	G	0.0021	0.0066	7.0377	7.9971	5.96E+04	664.9365	25.7864	19.903	
	B	0.0028	0.0054	6.8786	7.9971	64248	487.6806	22.0835	21.2494	
	Avg.	**0.0032**	**0.006933**	**7.064133**	**7.997067**	**58795.33**	**7.87E+02**	**27.54887**	**19.4858**	
Aeroplane	R	0.0029	0.0095	6.7421	7.9976	6.74E+04	8.52E+03	92.2841	8.8283	7.571679
	G	0.0045	0.0115	6.8249	7.9973	6.63E+04	8.89E+03	94.3107	8.6396	
	B	0.0107	0.0115	6.2475	7.9963	78636	9.75E+03	98.7341	8.2415	
	Avg.	0.006033	**0.010833**	**6.604833**	**7.997067**	**7.08E+04**	**9.05E+03**	**95.10963**	**8.5698**	

Table 7 (b). Performance Evaluation of the Proposed IE Model

Images	Planes	CC	SSIM	Input Entropy	Output Entropy	MD	MSE	RMSE	PSNR (in dB)	Execution Time (in Seconds)
Couple	R	0.002	0.0067	6.7693	7.9963	69669	384.8022	19.6164	22.2784	8.43384
	G	0.0025	0.0033	6.3381	7.9954	8.04E+04	240.364	15.5037	24.3221	
	B	-0.0019	0.0041	6.2083	7.9956	83275	197.0258	14.0366	25.1856	
	Avg.	**0.000867**	**0.0047**	**6.438567**	**7.995767**	**77790.67**	**274.064**	**16.38557**	**23.9287**	
House	R	8.70E-04	0.0108	6.4005	7.9959	7.21E+04	4.57E+03	67.6191	11.5294	7.720833
	G	6.14E-04	0.0105	6.5603	7.9969	68709	4.68E+03	68.3787	11.4324	
	B	-0.0048	0.0102	6.4042	7.9971	7.66E+04	6.03E+03	77.6317	10.33	
	Avg.	**-1.11E-03**	**0.0105**	**6.455**	**7.996633**	**7.25E+04**	**5.09E+03**	**71.20983**	**11.09727**	
Boat	R	-0.0048	0.01	7.1766	7.9966	55148	3.76E+03	61.3253	12.378	7.03142
	G	-1.23E-04	0.0098	7.1766	7.9968	55178	3.76E+03	61.3086	12.3804	
	B	-0.002	0.0114	7.1766	7.9964	5.48E+04	3.74E+03	61.1264	12.4062	
	Avg.	**-0.00231**	**0.0104**	**7.1766**	**7.9966**	**55047.33**	**3.75E+03**	**61.25343**	**12.3882**	
Cameraman	R	-0.0017	0.0082	7.0911	7.997	60725	3.73E+03	61.0861	12.412	8.005287
	G	7.81E-04	0.0083	7.0911	7.9969	6.13E+04	3.77E+03	61.429	12.3633	
	B	-0.0041	0.0077	7.0911	7.9965	60996	3.78E+03	61.5054	12.3525	
	Avg.	**-0.00167**	**0.008067**	**7.0911**	**7.9968**	**61017**	**3.76E+03**	**61.34017**	**12.37593**	
Elaine	R	-0.003	0.0102	7.4825	7.9967	4.13E+04	4.38E+03	66.172	11.7173	6.921456
	G	-0.0012	0.0108	7.4825	7.9966	41786	4.41E+03	66.3899	11.6888	
	B	0.0041	0.0124	7.4825	7.997	41751	4.37E+03	66.1257	11.7234	
	Avg.	**-3.3E-05**	**0.011133**	**7.4825**	**7.996767**	**4.16E+04**	**4.39E+03**	**66.2292**	**11.70983**	

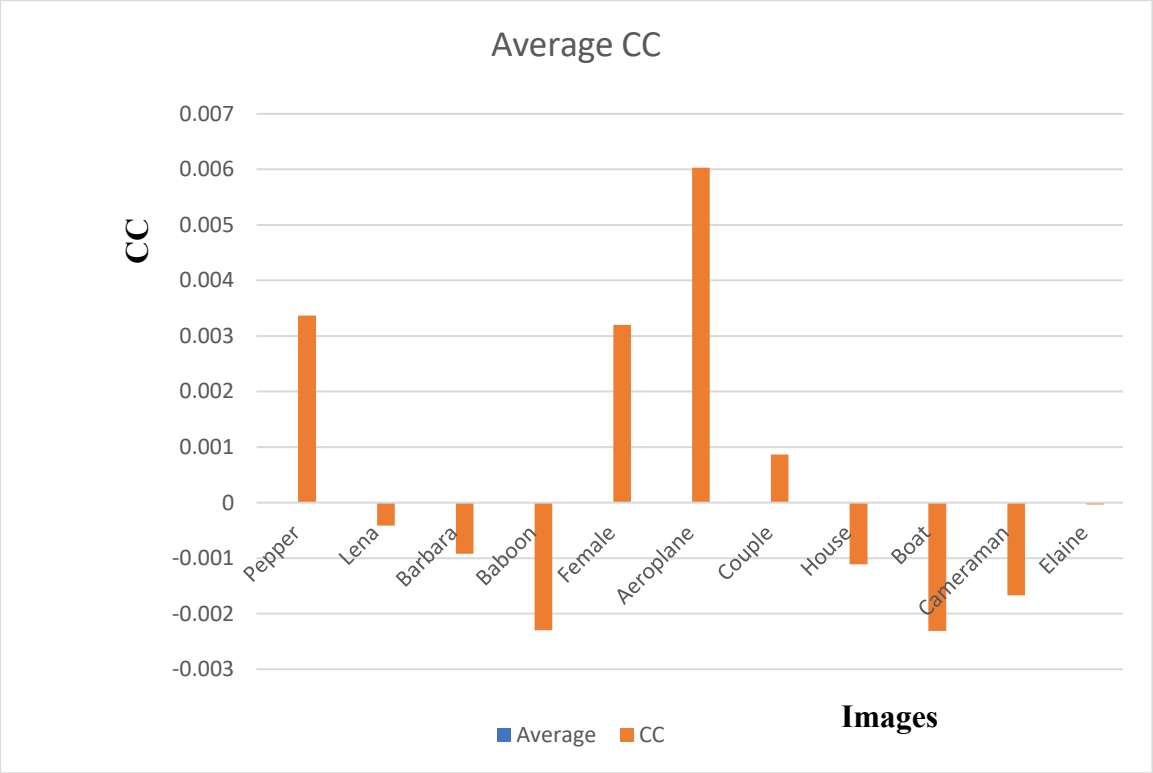


Figure 3. Average Correlation Analysis for the Proposed IE Model

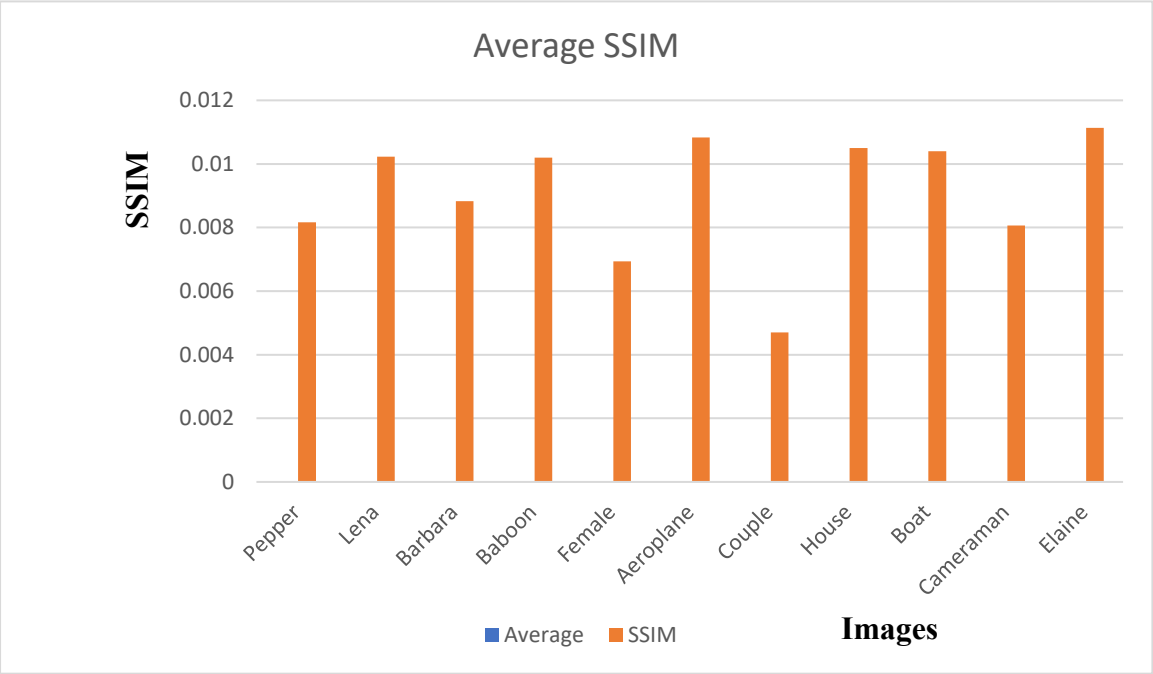


Figure 4. Average SSIM Analysis for the Proposed IE Model

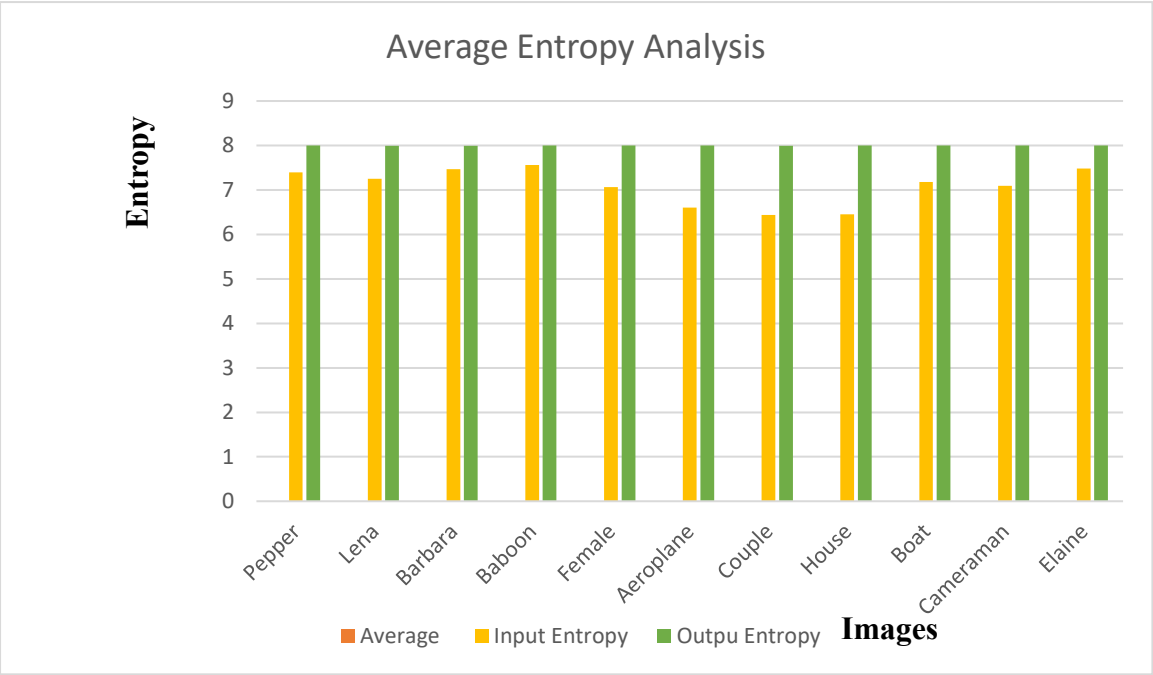


Figure 5. Average Entropy Analysis for the Proposed IE Model

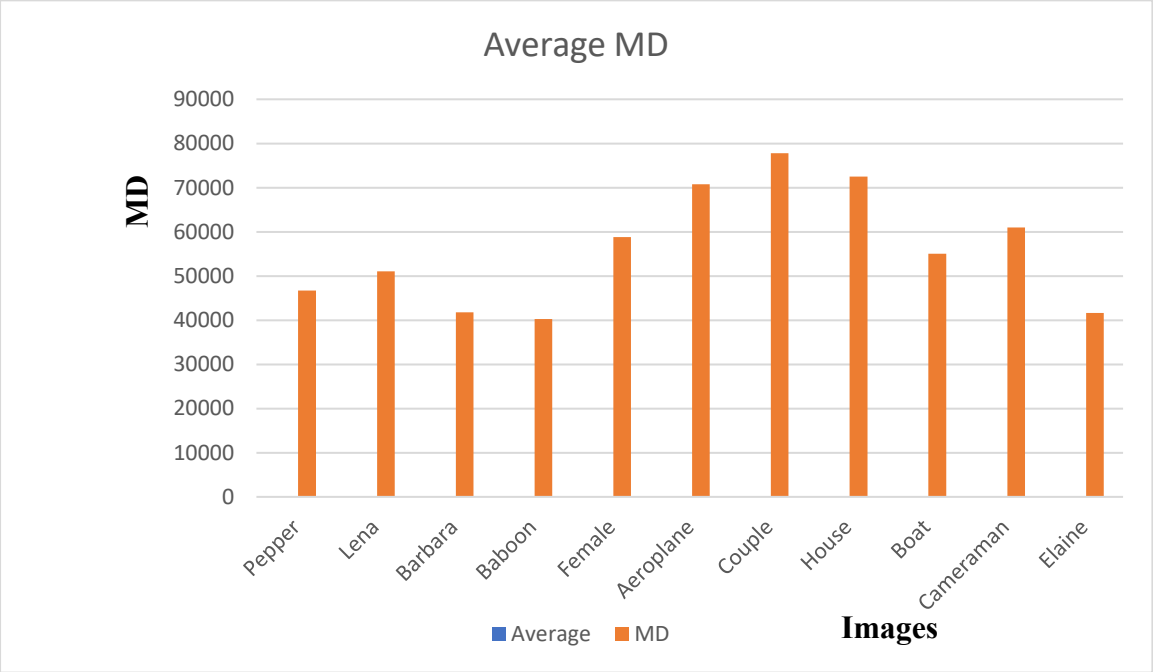


Figure 6. Average MD Analysis for the Proposed IE Model

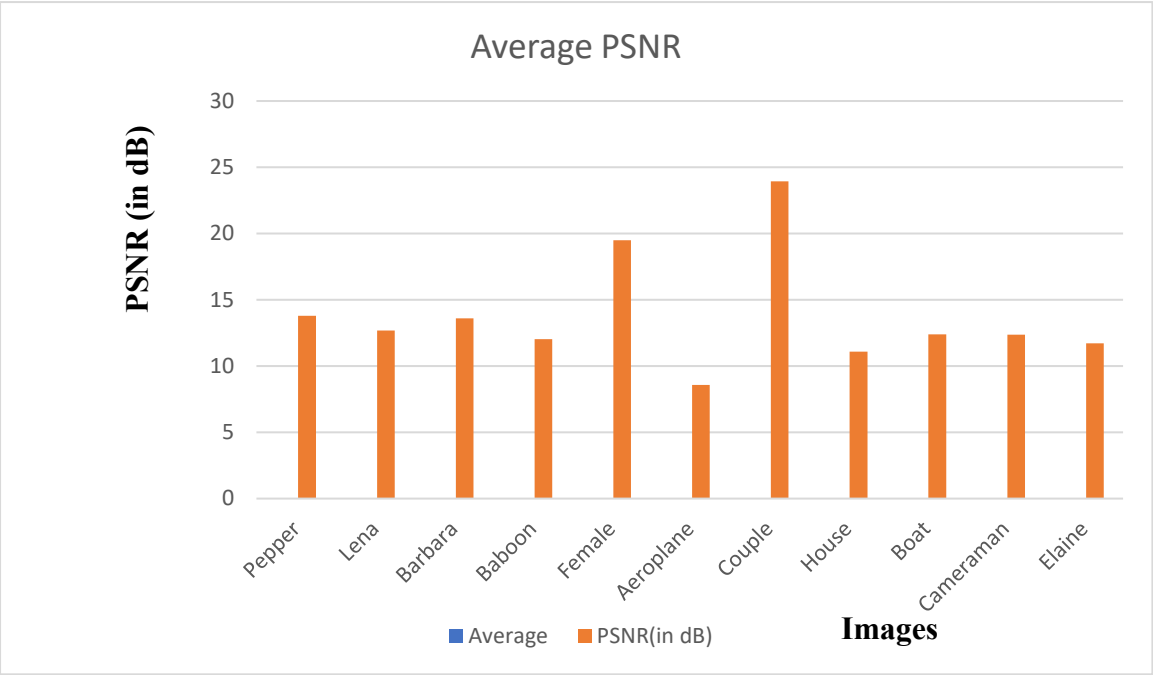


Figure 7. Average PSNR Analysis for the Proposed IE Model

5.3 Comparative Analysis

The entropy and CC parameter is considered for compared the proposed IE model with the existing IE models. In order to accomplish this goal, the proposed IE model is evaluated for same images are considered by existing authors in Table 8-9. The proposed IE model achieves better entropy for *cameraman, Elaine, and pepper* images when compared to IE model proposed by Sameh et al. [22] and Xu et al. [23] whereas a little bit-lower entropy for *lena* image when compared to Sameh et al. [23], as shown in Figure 8. Further, lower value of CC is accomplished by proposed IE model over IE model is proposed by Sameh et al. [22].

Table 8. Comparative Analysis

Images	Sameh et al. [22]	Xu et al. [23]	Proposed IE Model
Cameraman	7.9956	7.9862	7.9968
Elaine	7.9951	7.9895	7.9968
Lena	7.9978	7.9948	7.9963
Pepper	7.9961	7.9827	7.9968

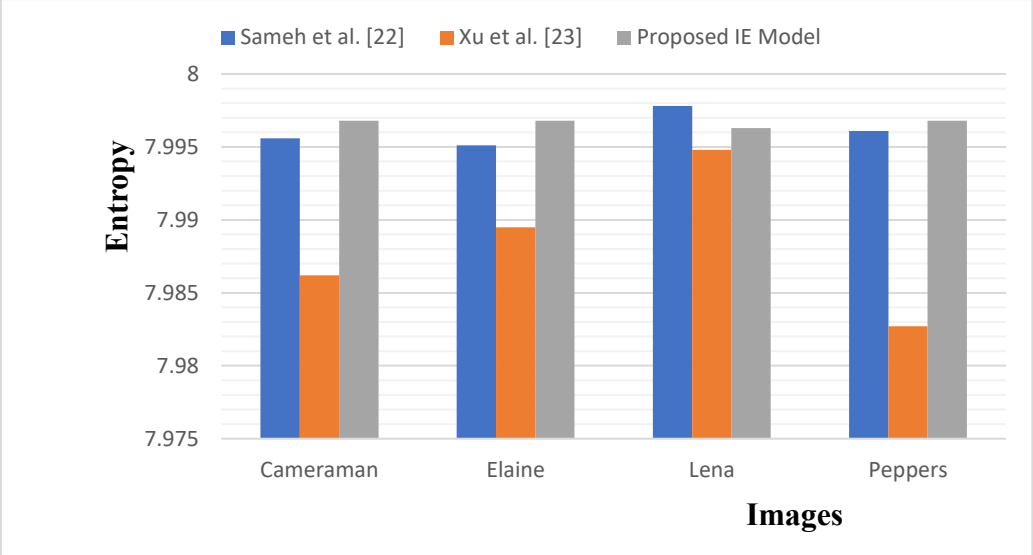


Figure 8. Entropy Analysis of the Proposed IE Model with the Existing IE Model

Table 9. CC Analysis between Proposed IE and Sameh et al. [22] Model

Images	**Sameh et al. [22]**	**Proposed Model**
Cameraman	−0.0039	-0.00167
Elaine	−0.0010	-0.00003
Lena	−0.0032	-0.00041
Pepper	−0.0022	0.003367

6. Conclusion

In this paper, we have developed an optimized IE model using the chaotic maps and GL algorithm to secure the color images on the internet. Initially, 3-D CLM is employed for generate random key by fine tuning the initial parameters of it using the metaheuristic GL algorithm. The GL algorithm is to search the best parameter values of 3-D CLM algorithm. Further, in this research, three security parameters, namely, entropy, CC, and SSIM are used to design objective function. We generate random keys using the 3-D CLM algorithm after we have determined the parameter values. Then, we use the secret image in an exclusive-OR operation. Then, in order to get the final encrypted image, the diffusion operation is applied to it. In order to accomplish this goal, CTM algorithm is considered which gives the shuffling index values. Based on this index values, shuffling of the pixels is done. The proposed IE model is evaluated on several standard images by considering the various security parameters. A high entropy value near to 8, low value of CC, SSIM, and PSNR is achieved. Besides that, other security parameters, namely, MSE, RMSE, and MD achieves the high value which is required in the IE Models. Finally, entropy and CC parameters are compared with the existing IE Model. Finally, compared to the previous models, the suggested IE model has high entropy and low CC.

References

[1] Kaur, M., Singh, S. and Kaur, M., 2021. Computational image encryption techniques: a comprehensive review. *Mathematical Problems in Engineering*, *2021*, pp.1-17.

[2] Kaur, M. and Kumar, V., 2020. A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, *27*, pp.15-43.

[3] Kaur, M. and Kumar, V., 2020. A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, *27*, pp.15-43.

[4] Dahiya, S. and Garg, M., 2020. Unmanned aerial vehicles: Vulnerability to cyber attacks. In *Proceedings of UASG 2019: Unmanned Aerial System in Geomatics 1* (pp. 201-211). Springer International Publishing.

[5] Foster, I.D., Larson, J., Masich, M., Snoeren, A.C., Savage, S. and Levchenko, K., 2015, October. Security by any other name: On the effectiveness of provider based email security. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security* (pp. 450-464).

[6] "Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation" n.d., *Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation*, viewed <https://www.linkedin.com/pulse/confidentiality-integrity-availability-authenticity-albert-kolbach>.

[7] Brindha, M., 2018, January. Confidentiality, integrity and authentication of DICOM medical images. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 71-75). IEEE.

[8] Biswas, C., Gupta, U.D. and Haque, M.M., 2019, February. An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography. In *2019 international conference on electrical, computer and communication engineering (ECCE)* (pp. 1-5). IEEE.

[9] Al-Yousuf, F.Q.A. and Din, R., 2020. Review on secured data capabilities of cryptography, steganography, and watermarking domain. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, *17*(2), pp.1053-1059.

[10] Varghese, F. and Sasikala, P., 2023. A Detailed Review Based on Secure Data Transmission Using Cryptography and Steganography. *Wireless Personal Communications*, pp.1-28.

[11] Mandal, P.C., Mukherjee, I., Paul, G. and Chatterji, B.N., 2022. Digital image steganography: A literature survey. *Information Sciences*.

[12] Bhavani, Y., Kamakshi, P., Kavya Sri, E. and Sindhu Sai, Y., 2022. A survey on image steganography techniques using least significant bit. In *Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2021* (pp. 281-290). Singapore: Springer Nature Singapore.

[13] Zhang, B. and Liu, L., 2023. Chaos-based image encryption: Review, application, and challenges. *Mathematics*, *11*(11), p.2585.

[14] Sameh, S.M., Moustafa, H.E.D., AbdelHay, E.H. and Ata, M.M., 2024. An effective chaotic maps image encryption based on metaheuristic optimizers. *The Journal of Supercomputing*, *80*(1), pp.141-201.

[15] Zhang, B. and Liu, L., 2023. Chaos-based image encryption: Review, application, and challenges. *Mathematics*, *11*(11), p.2585.

[16] Pankaj, S. and Dua, M., 2024. Chaos based Medical Image Encryption Techniques: A Comprehensive Review and Analysis. *Information Security Journal: A Global Perspective*, *33*(3), pp.332-358.

[17] Rajwar, K., Deep, K. and Das, S., 2023. An exhaustive review of the metaheuristic algorithms for search and optimization: taxonomy, applications, and open challenges. *Artificial Intelligence Review*, *56*(11), pp.13187-13257.

[18] Kumar, A., 2022. Improved Chaotic Logistic Map Algorithm based on Bio-Inspired Algorithm for Image Encryption. *Tobacco Regulatory Science (TRS)*, pp.1915-1928.

[19] Kumar, N. . and Saini, S. . 2024, Image Encryption Model based on Chaotic Henon Map and Termite Alate Optimization Algorithm. *International Journal of Intelligent Systems and Applications in Engineering*, 12(18s), pp. 428–436. Available at: https://ijisae.org/index.php/IJISAE/article/view/4987 (Accessed: 12 November 2024)

[20] Kumar, N., Saini, S. and Garg, D., 2024. Color Image Encryption Model Based on 3-D Chaotic Logistic Map and JAYA Algorithm. *IETE Journal of Research*, pp.1-11.

[21] Kaur, G., Singh, Y., Bhadauria, P., Kumar, A. and Singh, J.P., 2024. Color Image Encryption Method based on Three-Dimensional Chaotic Map and Nature-Inspired Osprey Optimization Algorithm. *Power System Technology*, *48*(1), pp.306-321.

[22] Sameh, S.M., Moustafa, H.E.D., AbdelHay, E.H. and Ata, M.M., 2024. An effective chaotic maps image encryption based on metaheuristic optimizers. *The Journal of Supercomputing*, *80*(1), pp.141-201

[23] Xu, S., Chang, C.C. and Liu, Y., 2021. A high-capacity reversible data hiding scheme for encrypted images employing vector quantization prediction. *Multimedia Tools and Applications*, *80*(13), pp.20307-20325.

[24] Almasoud, A.S., Alabduallah, B., Alqahtani, H., Aljameel, S.S., Alotaibi, S.S. and Mohamed, A., 2024. Chaotic image encryption algorithm with improved bonobo optimizer and DNA coding for enhanced security. *Heliyon*, *10*(3).

[25] Khalaf, K.S., Sharif, M.A. and Wahhab, M.S., 2022. Digital Communication Based on Image Security using Grasshopper Optimization and Chaotic Map. *International Journal of Engineering*, *35*(10), pp.1981-1988.

[26] Elkhalil, N., Weddy, Y.C. and Ejbali, R., 2023. Image encryption using the new two-dimensional Beta chaotic map. *Multimedia Tools and Applications*, *82*(20), pp.31575-31589.

[27] Wang, J., Song, X. and El-Latif, A.A.A., 2022. Single-objective particle swarm optimization-based chaotic image encryption scheme. *Electronics*, *11*(16), p.2628.

[28] sipi.usc.edu. (n.d.). *SIPI Image Database*. [online] Available at: https://sipi.usc.edu/database/.

[29] Patel, S., Bharath, K.P. and Kumar, R., 2020. Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique. *Multimedia Tools and Applications*, *79*(43), pp.31739-31757.

[30] Rahman, C.M., 2023. Group learning algorithm: a new metaheuristic algorithm. *Neural Computing and Applications*, *35*(19), pp.14013-14028.

[31] Li, C., Luo, G., Qin, K. and Li, C., 2017. An image encryption scheme based on chaotic tent map. *Nonlinear Dynamics*, *87*, pp.127-133.

[32] Elkandoz, M.T. and Alexan, W., 2022. Image encryption based on a combination of multiple chaotic maps. *Multimedia Tools and Applications*, *81*(18), pp.25497-25518.

[33] Alexan, W., Elkandoz, M., Mashaly, M., Azab, E. and Aboshousha, A., 2023. Color image encryption through chaos and kaa map. *Ieee Access*, *11*, pp.11541-11554.

[34] Patro, K.A.K. and Acharya, B., 2021. An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system. *Nonlinear Dynamics*, *104*(3), pp.2759-2805.

[35] Alexan, W., Elkandoz, M., Mashaly, M., Azab, E. and Aboshousha, A., 2023. Color image encryption through chaos and kaa map. *Ieee Access*, *11*, pp.11541-1155