ChaDRaL: RGB Image Encryption based on 3D Chaotic Map, DNA, RSA and LSB

Nirali Parekh
Department of Computer Engineering
Dwarkadas J. Sanghvi College of Engineering
Mumbai, India
nirali25parekh@gmail.com
Lynette D'Mello
Department of Computer Engineering
Dwarkadas J. Sanghvi College of Engineering
Mumbai, India
Lynette.DMello@djsce.ac.in

***Abstract*—In this paper, an RGB image encryption algorithm based on DNA, chaos, RSA and LSB is introduced. The proposed algorithm leverages the advantages of symmetric and asymmetric cryptography as well as steganography. On one hand, the image is encrypted using a symmetric algorithm that combines DNA sequence operations and Lorenz chaotic system. On the other hand, the secret key which is used to encrypt the image is now itself encrypted with an asymmetric algorithm i.e. RSA. Lastly, this encrypted key is hidden in the cipher image using LSB steganographic scheme. As a result, the problem of key transfer is also eliminated. The proposed encryption approach is tested over different well-known images that are taken from USC-SIPI image database. The security analysis of the proposed method showed that histogram of a cipher image produced a uniform distribution, a higher entropy and a low correlation among image pixels. Also, it has great performance in terms of established metrics such as UACI, NPCR, PSNR and SSIM. The simulation results show that our scheme can achieve good encryption and resist attacks like statistical attack and differential attack. This combination of both steganography and cryptography results in increased authority and security.**

***Index Terms*—Image Encryption, Lorenz Map, DNA, cryptography, steganography**

I. Introduction

Reliance on digital media for convenient data transfer leads to serious security concerns in the web. The exponential growth of computational power has led to stronger and more frequent brute force attacks than ever before [1]. Image Data is used in communication for applications such as military communication, medical imaging systems, etc that deal with confidential images which poses the need for the data to be encrypted before it is transmitted. Various conventional encryption schemes have been studied, such as Data Encryption Standard (DES) [2], Advanced Encryption Standard (AES) [3]. However, these schemes have been invented for text or bit encryption and appear not to be ideal for image applications due to special characteristics like redundancy and high correlation among pixels [4], [5]. The major challenge in designing effective image encryption algorithms is that it is rather difficult to shuffle and diffuse image data efficiently by traditional cryptographic means. These limitations are solved by Chaos systems which possess has the properties of randomness, and sensitivity to initial conditions [6].

DNA computing, an emerging field is also permeating into cryptography as various hybrid encryption algorithms with chaos and DNA are proposed. These algorithms based on DNA encoding and chaos maps are symmetric algorithms. i.e. the sender and receiver require a common secret key for encryption and decryption respectively which hence leaves the problem of secure key transmission. Asymmetric algorithms such as RSA were designed specifically to address this issue. removes the problem of transfer of the key. But it can not grab the place of a symmetric algorithm for images because its computation time goes as high as 1500 times than the symmetric DES algorithm [7].

In order to overcome the defects of symmetric and asymmetric encryption algorithms, a hybrid approach is proposed. This method is based on DNA, chaos, RSA, and LSB. First, the image is encrypted using DNA and chaos maps using a secret key, then, this key is encrypted using RSA and it is hidden in the ciphered image using the LSB technique. The major advantage of our approach is that it eliminates the problem of key transmission while at the same time maintaining the efficiency in computation cost and security. Table II tabulates the advantages and objectives of the algorithms used in ChaDRaL.

This paper is organized as follows. section II describes the previous works and advancements in this field. in short. In section III, the proposed digital image encryption algorithm based on the Lorenz chaos system, DNA, RSA, and LSB is described, and in section IV, the experimental results of the proposed digital image encryption algorithm are discussed. Next, analysis in terms of time and security metrics is presented in section V. Finally, the paper is concluded in section VI.

II. Literature Review

Many researchers have turned their attention to these research areas and have been proposing new image encryption algorithms based on chaos theory. Various image encryption algorithms [8]–[13] . In particular, the one-dimensional chaotic map like Logistic map is one of the popular chaotic systems because of its speed and simplicity [14]. However, these chaotic encryption algorithms utilize 1D or multidimensional chaos maps all of which include transforming the image pixel position and pixel values. Some works [15]–[17] point out the critical security vulnerabilities of using encryption algorithms constituted by a single and pure chaos map. Consequently, some works merged chaotic systems with other algorithms like Hill Cipher [18]. Now, in recent years, hybrid algorithms based on DNA encoding and chaos maps have been explored by researchers [19]–[21]

A brief overview of previous works in the image encryption field have been presented in Table I

ref	Encryption method	Chaotic map used
[10]	Chaos	Tent map, standard map, logistic map
[11]	Chaos	logistic map
[9]	Chaos	logistic map and piecewise linear chaotic map (PWLCM)
[8]	Chaos	Modified 2D cat map
[13]	Chaos	1D logistic map
[12]	Chaos	NCA map
[19]	Chaos + DNA	2D logistic map
[20]	Chaos + DNA	1D and 2D logistic maps
[18]	Chaos	1D logistic map, sine map, and Chebyshev map
[6]	Chaos + DNA	Logistic map
[21]	Chaos + DNA	1D logistic map
[22]	chaos	Chebyshev map
[23]	Chaos + DNA	Lorenz and Rossler map
[24]	Chaos + DNA	Lorenz map
[25]	RC6 + LSB	-
[26]	ECC + Hill Cipher + LSB	-
[27]	AES + RSA + LSB	-
[28]	Chaos + AES	Arnold map

TABLE I: Summary Table of studies included in the Literature Review

III. Proposed Algorithm

The overall architecture of the proposed image encryption system is depicted in Figure 1.

algorithm	domain	Which issue does it solve?	Security objectives it achieves
Chaos and DNA	Symmetric cryptography	Solves the slow encryption speed of asymmetric algorithms	Authentication, Confidentiality, Data Integrity and identification
RSA	Asymmetric cryptography	Solves the issue of key exchange of image encryption	Authentication, Identification, Confidentiality, Data Integrity and Non-repudiation
LSB	Keyless steganography	It eliminates the problem of key exchange	Confidentiality

TABLE II: Summary of Advantage and Objectives of algorithms used in proposed Image Encryption Scheme

A. Concepts in the Proposed Methodology

1) DNA: With evolution in DNA computing, the researchers presented many biological operations and algebraic and xor operations based on DNA sequence [29]. The eight kinds of coding combinations that satisfy the principle of complementary base pairing [30] are given in Table III, where two bits represent one DNA base. In the proposed algorithm, we select the rule number of DNA encoding by performing computing on the user input key K. Example: If the binary pixel value of an image is `01101110`, so the corresponding DNA sequence according to the first encoding rule is `ATGT`

DNA sequences	Rules							
	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

TABLE III: Eight kinds of DNA map rules

2) Lorenz Chaos system: In the proposed algorithm, we have chosen the Lorenz chaos system which is perhaps one of the best-known chaotic system diagrams. They are highly sensitive to small differences in their initial conditions. The

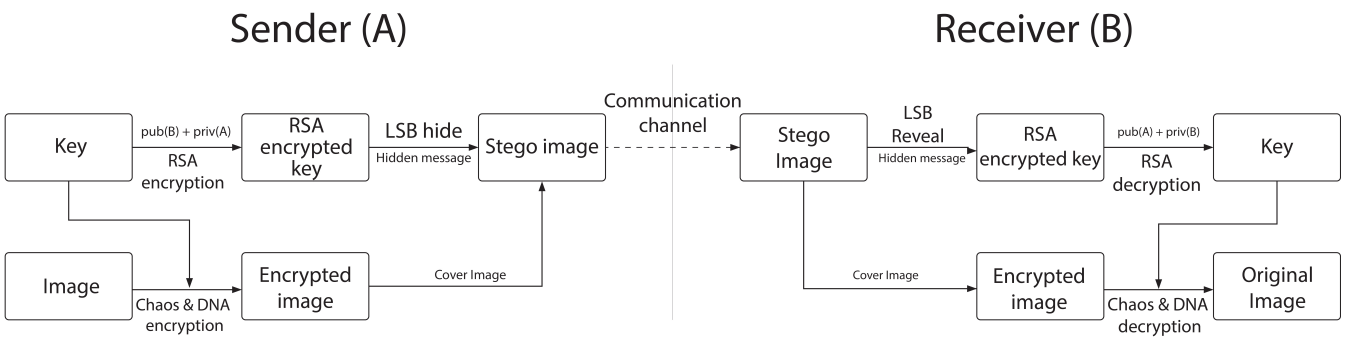


Fig. 1: Architecture of the proposed image cryptosystem - ChaDRaL

Lorenz system is described by the following system of differential equations:

$$\frac{\mathrm{d}x}{\mathrm{d}t} = \sigma y - \sigma x \tag{1a}$$

$$\frac{\mathrm{d}y}{\mathrm{d}t} = \rho x - xz - y \tag{1b}$$

$$\frac{\mathrm{d}z}{\mathrm{d}t} = xy - \beta z \tag{1c}$$

The real numbers σ, β, and ρ are called the control parameters, whereas x, y, z are the state variables. For the given control parameters and initial values x0, y0, z0 of the state variables, the Lorenz chaotic attractor is graphed using the above equations (1) using methods like RK45. The graph obtained resembles a butterfly of the dynamical system as shown in Figure 2 It is observed that for σ= 10, β = 8/3 σ, β, and ρ ¿ 24.7 most Lorenz orbits exhibit chaotic wandering [31].

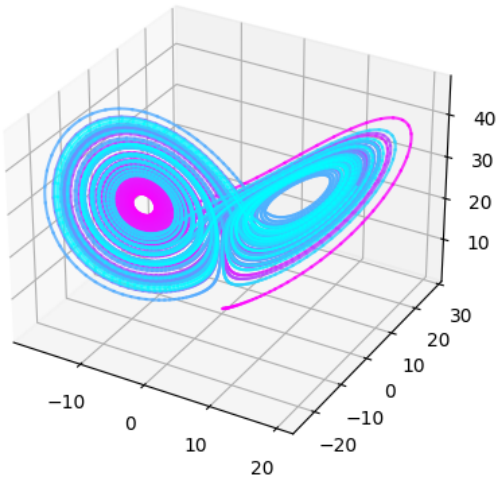


Fig. 2: Chaotic behavior of Lorenz attractor, σ = 10, β = 8/3 and ρ = 28

For the proposed image encryption algorithm, we shall fix the system parameters σ = 10, β = 8/3 and ρ = 28 for the Lorenz system. And the initial values x0, y0, z0 are to be determined based on the key input by the user. This is a large enough keyspace to resist brute-force attacks. Moreover, any slight change in initial conditions will cause trajectories to produce enormous differences in output as proved by the experiments of [32].

3) RSA: RSA algorithm [33] is an asymmetric cryptography algorithm. RSA is a relatively slow algorithm which is why it is not practically used to directly encrypt images. Since RSA is preferred only for quick encryption of small pieces of data, in our proposed algorithm, we encrypt our key input by the user using the RSA algorithm.

4) LSB: LSB is one of the most versatile and efficient known method of steganography for hiding information in digital data [34].The three channels of a color image- red, blue, and green, each pixel byte indicates the intensity of the corresponding color, and the range is from 0 to 255. In the proposed method, the LSB technique replaces the Least Significant bit of the pixel value to accommodate one of the bits of the secret RSA encrypted key.

5) SHA256: The cryptographic hash SHA-256 [35] generates an almost-unique 32-byte signature for a text. The strength of encryption lies not only in the complexity of the encryption algorithm but also in the strength, randomness, and complexity of the key. Hence, in the proposed algorithm, SHA256 hashing algorithm is utilized to randomize the key and convert the user input key to a fixed size output.

B. Encryption

Input: Image I , a secret key K.
Other Requirements: To encrypt the image, the sender must know the receiver's public key and his own private key. The proposed encryption process is shown in the flowchart in Figure 3, with a detailed description given:

C. Decryption

Input: $I_{crypto+stego}$
Other Requirements: To decrypt the image, the receiver needs to know the sender's public key and his private key. The algorithm decryption process is the inverse of the encryption process.

Algorithm 1: Encryption Algorithm

1 Input 8-bit color image $\mathrm{I}(\mathrm{m}, \mathrm{n}, 3)$, where m, n are the image dimensions of rows and columns, respectively.
2 Input the key K from the sender.
3 Calculate DNA rule number r by: $r = (\Sigma$ ascii values of characters of $\mathrm{key}K) \bmod 8$
4 Splitting the RGB image I into $\mathrm{R}(\mathrm{m}, \mathrm{n})$, $\mathrm{G}(\mathrm{m}, \mathrm{n})$, $\mathrm{B}(\mathrm{m}, \mathrm{n})$ components, and transform the pixel values of decomposed matrices R, G, B to binary to form $\mathrm{R}(\mathrm{m}, \mathrm{n} \times 8)$, $\mathrm{G}(\mathrm{m}, \mathrm{n} \times 8)$ and $\mathrm{B}(\mathrm{m}, \mathrm{n} \times 8)$.
5 Encode the three binary matrices respectively as per the DNA encoding rules selected by rule number r where $\mathrm{r} \in [1, 8]$ and get three DNA sequence matrices $\mathrm{R_{DNA}}(\mathrm{m}, \mathrm{n} \times 4)$, $\mathrm{G_{DNA}}(\mathrm{m}, \mathrm{n} \times 4)$, and $\mathrm{B_{DNA}}(\mathrm{m}, \mathrm{n} \times 4)$
6 Compute $\mathrm{Hash}(\mathrm{K})$ of 256 bits using the SHA256 algorithm. $\mathrm{K_{SHA}}(256 \times 1)$
7 Convert $\mathrm{K_{SHA}}$ to $(\mathrm{m} \times 2, \mathrm{n} \times 4)$ key matrix by repeating $\mathrm{K_{SHA}}$ as many times as necessary. Encode this key matrix in accordance with the DNA encoding rule r where $\mathrm{r} \in [1, 8]$ and obtain $\mathrm{K_{DNA}}(\mathrm{m}, \mathrm{n} \times 4)$.
8 Exclusive OR the $\mathrm{R_{DNA}}$, $\mathrm{G_{DNA}}$ and $\mathrm{B_{DNA}}$ with $\mathrm{K_{DNA}}$ using DNA XOR rules. Eg $\mathrm{R_{DNA}[i, j]} = \mathrm{R_{DNA}[i, j]} \hat{} \mathrm{K_{DNA}[i, j]}$
9 Compute Lorenz initial parameters x_0, y_0, z_0 by chain-XOR of $\mathrm{K_{SHA}}$.
10 Generate the chaotic sequence x_n, y_n and z_n whose length $l = \mathrm{m} \times \mathrm{n} \times 8/2$ by using Lorenz chaos where the initial conditions are x_0, y_0, z_0, and system parameters are σ, β, and ρ.
11 Generate f_x, f_y, f_z by sequence indexing x_n, y_n, and z_n sequences where $\mathrm{f_x[i]}$ holds the index of where $\mathrm{x[i]}$ belongs in the sorted order of x_n
12 Scramble $\mathrm{R_{DNA}}$, $\mathrm{G_{DNA}}$, and $\mathrm{B_{DNA}}$ matrices using f_x, f_y and f_z to obtain $\mathrm{R_{scram}}$, $\mathrm{G_{scram}}$, and $\mathrm{B_{scram}}$
13 Decode the three matrices $\mathrm{R_{scram}}$, $\mathrm{G_{scram}}$, and $\mathrm{B_{scram}}$ respectively in accordance with the DNA decoding rule r where $\mathrm{r} \in [1, 8]$ and get $\mathrm{R_{enc}}\ (\mathrm{m}, \mathrm{n})$, $\mathrm{G_{enc}}\ (\mathrm{m}, \mathrm{n})$, and $\mathrm{B_{enc}}\ (\mathrm{m}, \mathrm{n})$
14 Recover the RGB image by combining $\mathrm{R_{enc}}\ (\mathrm{m}, \mathrm{n})$, $\mathrm{G_{enc}}\ (\mathrm{m}, \mathrm{n})$, and $\mathrm{B_{enc}}\ (\mathrm{m}, \mathrm{n})$ to obtain I_{crypto} which is the encrypted image.
15 Encrypt key K by RSA algorithm using the private key of sender A $\mathrm{priv(A)}$ and public key of receiver B - $\mathrm{pub(B)}$. We obtain K_{RSA}.
16 Using LSB steganography, hide K_{RSA} using I_{crypto} as the cover image. Hence, we finally get the $\mathrm{I}_{crypto+stego}$

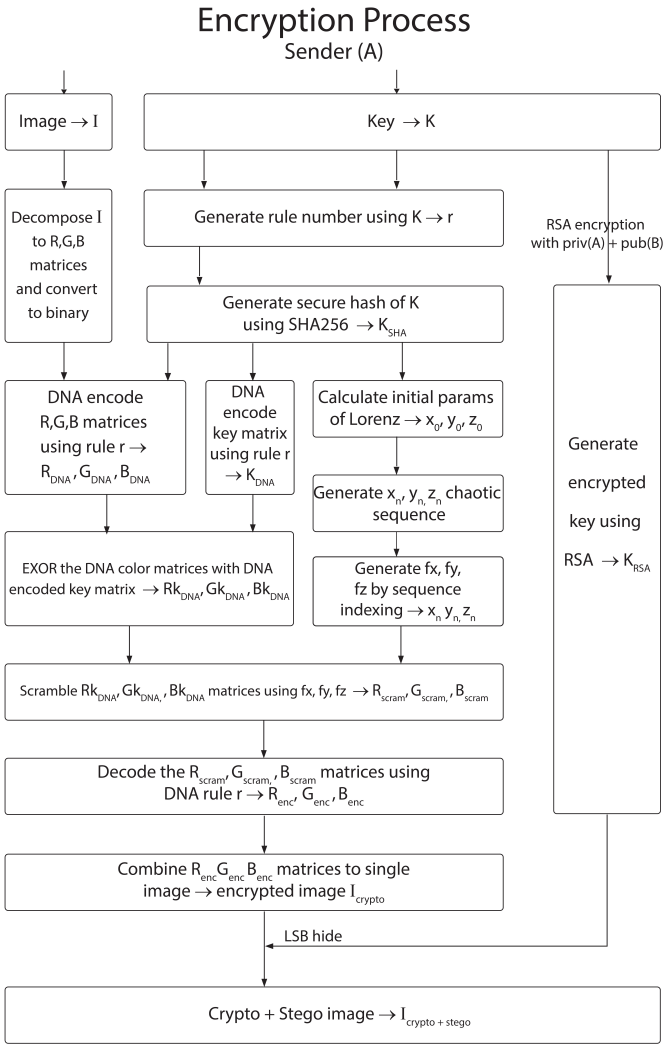


Fig. 3: Flow Diagram of the Encryption Process

IV. Experimental results

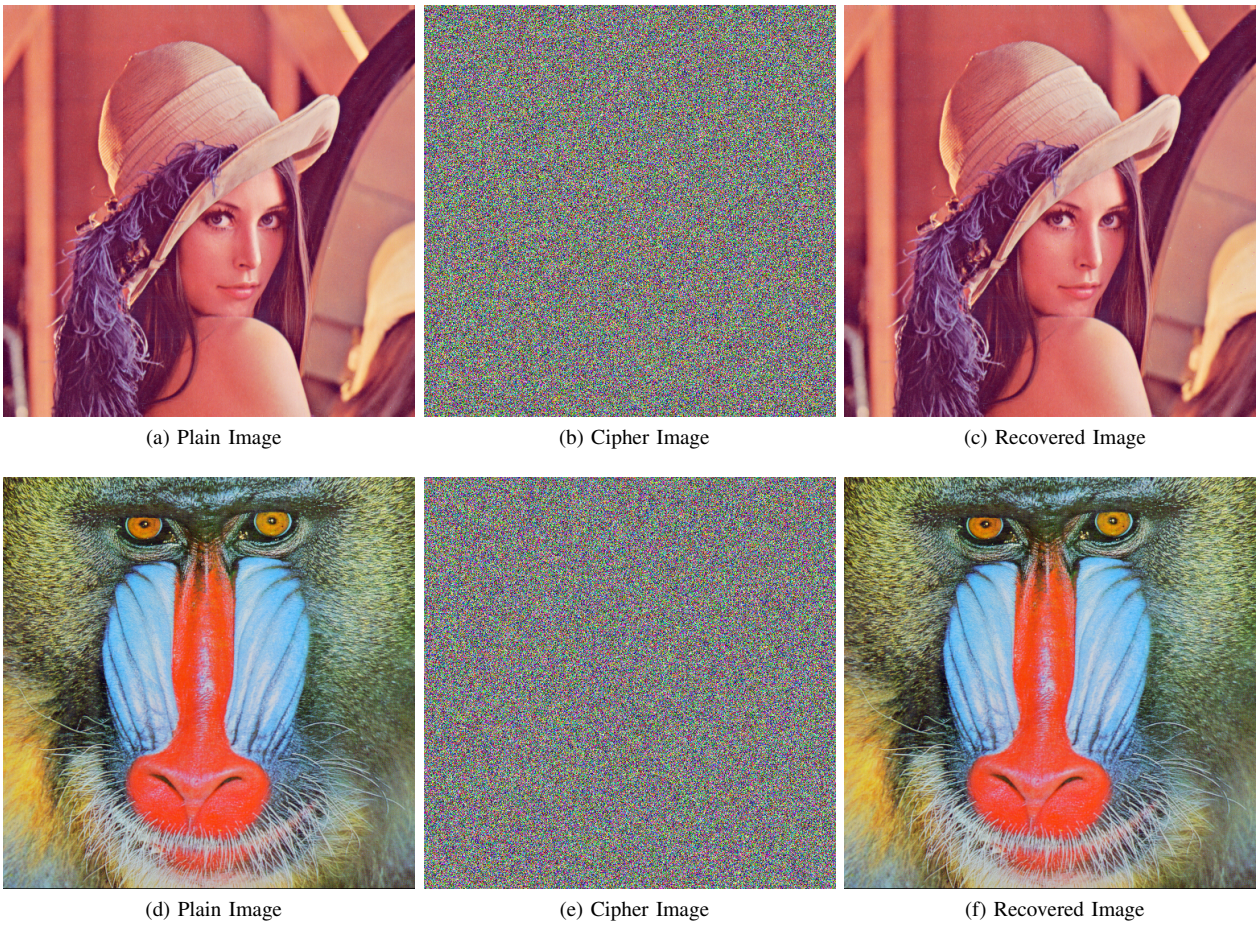
The proposed algorithm is tested using a PC with a 3.1GHz processor Intel(R) Core i5-8250U, 8 GB RAM, and Windows 10, 64-Bit Operating System. The proposed algorithm was tested over different color images that are taken from USC-SIPI image dataset [36].

The proposed color image encryption scheme is tested by using visual review. Any visible analogy between plain images and their corresponding encrypted images cannot be detected using plain inspection. Figure 4 shows the experimental results of test images Lena and Baboon respectively. The encrypted image doesn't show any segmented color clusters or any resemblance to the source figures.

V. Performance in terms of time consumption and security analysis

A. Time consumption

The average time is calculated as follows: the proposed algorithm was executed 25 times each time using a new random secret key, and the average timings were calculated



(a) Plain Image (b) Cipher Image (c) Recovered Image

(d) Plain Image (e) Cipher Image (f) Recovered Image

Fig. 4: Plain images (a, d) Cipher images (b,e) Recovered images (c,f) of Lena and Baboon respectively

respectively. Table IV shows the comparison of the proposed algorithm with some other cited algorithms. As we can see, it works faster than some encryption algorithms, some exceptions being [8] and [9], which shows better computational performance.

ref	image	image size	Encryption time	Decryption time
ChaDRaL	Lena	512 color	80.05	85.97
[10]	Lena	512 color	93.8	102.6
[11]	Lena	512 color	95.6	104.31
[9]	Lena	512 color	30	30
[28]	Lena	256 gray	2900	-
[8]	Lena	512 color	31.72	32.17
AES	Lena	256 gray	454100	465700

TABLE IV: Comparison of average encryption and decryption time of ChaDRaL, with some known algorithms (in millisecond)

B. Imperceptibility - MSE, PSNR, SSIM

The mean-square error (MSE) and the peak signal-to-noise ratio (PSNR) between two images is used to compare image encryption quality. The mean-squared error is calculated using:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N} \tag{2}$$

where M and N are the numbers of rows and columns in the input images. Then MSE is used to compute PSNR using the following:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right) \tag{3}$$

Here, R is the maximum fluctuation in the input image data type.

Our proposed algorithm achieves a high value of PSNR, which demonstrates the superiority of the signal to that of the noise, which indicates better quality of the reconstructed image. The lower the value of MSE, the lower the error.

The structural similarity index (SSIM) [37] is a metric used for measuring the similarity between two images. The SSIM index is a decimal value between -1 and 1, where two identical images have an SSIM value of 1. Let $x = \{xi \mid i = 1, 2, \ldots N\}$ and y = {yi | i = 1, 2, . . . N} be the original and the test image signals, respectively. The measure between two windows x and y of common size N is [38]:,

Images	test image	MSE	PSNR	SSIM
Original image and Cipher image	lena	8828.6	8.6719	0.0200
	baboon	8597.6	8.7870—	0.0201
	tulips	11032	7.7043	0.0179
	peppers	10318	7.9950	0.0195
Original image and Recovered image	lena	0.7372	49.455	0.9987
	baboon	0.7975	49.113	0.9995
	tulips	0.3182	53.104	0.9991
	peppers	0.5684	50.585	0.9985

TABLE V: Quantitative results of the Imperceptibility analysis

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{4}$$

$$where,\ \mu_x = average\ of\ x$$

$$\mu_y = average\ of\ y$$

Table V tabulates the MSE, PSNR, and SSIM values that are performed between original and cipher images and then between original and recovered images. In the first case, between plain and cipher images, the obtained values of SSIM are very close to zero, those of PSNR low, and MSE very high all of which indicate substantial difference amid the original image and encrypted image. In the second case, for plain and recovered images, the obtained values of SSIM are very close to 1, those of PSNR high, and MSE values close to 0. These values demonstrate the effectiveness of the proposed encryption algorithm applied to secure image transmission.

C. Differential Attack - NPCR, UACI

In the chosen plaintext attack, an attacker can arbitrarily select a certain number of plaintext, let the algorithm encrypt it, and get the corresponding ciphertext. We analyze a chosen-plaintext attack named differential attack. The differential analysis measures how sensitive the plain image is to minor modifications. This is done via two metrics, namely, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) [39]. Let us assume encrypted images before and after one-pixel modification in a plain image are C1 and C2. The NPCR and UACI are defined as follows:

$$NPCR = \frac{\sum_{i=0}^{W-1}\sum_{j=0}^{H-1} D(i,j)}{W \times H} \times 100\% \tag{5}$$

$$UACI = \frac{1}{W \times H}\left(\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100\% \tag{6}$$

where D is a two-dimensional set, having the same size as image $C1$ or $C1$, and W and H are respectively the width and height of the image. The set $D(i,j)$ is defined such as the similarity boolean matrix for $C1$ and $C2$ i.e, if $C1(i,j) = C2(i,j)$ then $D(i,j) = 1$; otherwise,$D(i,j) = 0$

The NPCR and UACI differential analysis test results from the proposed encryption algorithm are shown in Table VI. The optimal NPCR value is almost 99.61%, and the optimal UACI value is almost 33.46%. [39], [40]

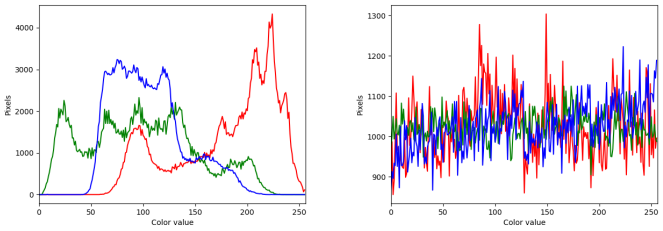
image	NPCR	UACI
Lena	0.99618	0.30447
baboon	0.99596	0.29838
peppers	0.99629	0.3262
tulips	0.99603	0.33653

TABLE VI: Quantitative results of the Differential Analysis

D. Statistical analysis: Histogram, Correlation, Entropy

The following measures show that the confusion and diffusion properties are preserved in the proposed image encryption scheme [5].

1) Histograms: In image encryption, the distribution of the pixel values is displayed using a histogram. The histogram of the encrypted image should change into a flat pattern. Figure 5 shows histogram analysis of three channels (red, green, and blue) of the plain and encrypted images. As they vividly show, in the original image, the pixels show visible patterns or trends in some values. In contrast, the pattern of the encrypted image histogram is very flat, and almost every pixel is divided into each value. This shows that the proposed encryption method can resist statistical attacks effectively.



(a) Original Image (b) Cipher Image

Fig. 5: The RGB histogram analysis of the 'Lena'

2) Correlation Analysis : Adjacent pixels in the plain images are very redundant and correlated. As a general requirement for all image encryption schemes, the encrypted image should be greatly different from its original form. The correlation analysis is one of the usual and reliable ways to measure this property.

The correlation coefficient is calculated using the formula [41], [42]:

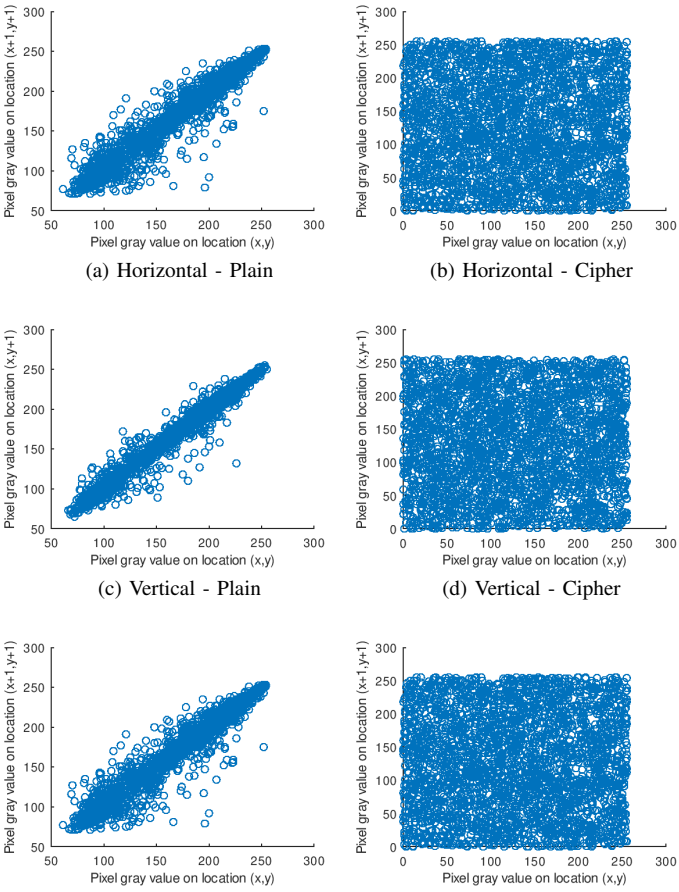
$$CC = \frac{\mathrm{cov}(x,y)}{\sigma_x\sigma_y} = \frac{\sum_{n=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{n=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{n=1}^{N}(y_i - E(y))^2}} \tag{7}$$

$$where,\ x\ and\ y\ are\ pixel\ values\ of\ the\ same\ indices\ of$$

the original image and ciphered image respectively

If the correlation coefficient is near 1, this means that the original image and the encrypted image are very dependent on each other, i.e. the original image can be reproduced easily from the encrypted image [42].

Table VII shows the comparison of correlation coefficient of ChaDRaL with a few other algorithms. Moreover, the correlation of 3000 pairs of adjacent pixels from the original image and cipher image of 'Lena' are shown in Figure 6.



(a) Horizontal - Plain (b) Horizontal - Cipher

(c) Vertical - Plain (d) Vertical - Cipher

(e) Diagonal - Plain (f) Diagonal - Cipher

Fig. 6: Correlation distribution results of two adjacent pixels of 'Lena' in original images: (a), (c), (e) and in encrypted images: (b), (d), (f) respectively

3) Entropy attack: Information entropy is an important tool to analyze the strength of an encryption scheme. Entropy must be supplied by the cipher for injection into the plain image to minimize the amount of structure that is present in the insecure plain image.

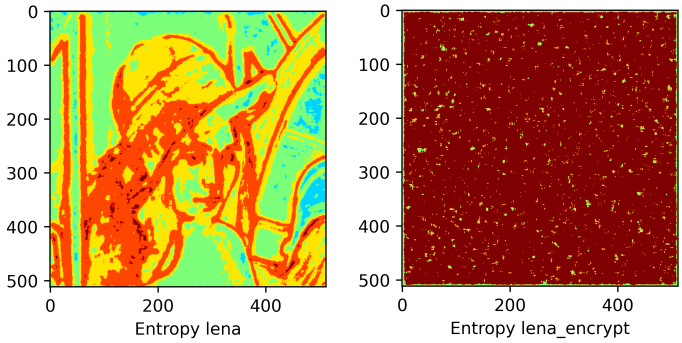
The entropy of a random source is the expected information content of the symbol it outputs, that is:

$$H(X) = E\left[H_X\right] = \sum_x \Pr[x] H_x = \sum_x -\Pr[x]\log_2(\Pr[x]) \tag{8}$$

Figure 7 shows the entropy graphs of the original Lena and encrypted Lena respectively.

Ref	Plain Image			Cipher Image		
	HC	VC	DC	HC	VC	DC
[13]	0.948	0.8851	0.8546	0.0248	-0.0094	-0.0183
[6]	0.9099	0.939	0.8659	0.0059	-0.0042	0.018
[19]	0.9755	0.9603	0.9443	-0.0045	-0.0002	0.0053
[20]	0.9468	0.9697	0.9153	0.0036	0.0023	0.0039
[10]	0.9802	0.9866	0.9647	-0.0021	-0.0162	0.0178
[11]	0.9751	0.9889	0.9670	0.0068	0.0078	0.0032
[12]	0.9659	0.9466	0.9230	0.0055	0.0041	0.0002
AES	0.9781	0.9871	0.9713	0.2724	0.2681	0.0765
ChaDRaL	0.9781	0.9871	0.9713	-0.0043	0.0197	0.0032

TABLE VII: Correlations of the plain and the encrypted images of 'Lena' (HC – horizontal correlation, VC – vertical correlation, DC – diagonal correlation).



(a) Plain Image (b) Cipher Image

Fig. 7: Entropy in 10 x 10 neighbourhood of 'Lena'

VI. Conclusion and Future Scope

Taking the merits of the RSA, LSB, DNA and Lorenz chaotic map into account, this paper puts forward a hybrid image encryption scheme based on symmetric, asymmetric cryptography, and steganography. Experimental results and security analyses show that the proposed scheme has a good encryption effect. Furthermore, the algorithm can resist most known attacks, such as differential attack, entropy attack, statistical attack and known-plaintext attack. The security analysis outcomes as seen in section V indicate the suitability of the proposed algorithm for image encryption applications. By combining the features of both cryptography and steganography, enhanced data privacy and ownership has been achieved. However, since the speed performance of the proposed algorithm is not ideal, our future work will focus on efficient run time performance and real time video encryption using the suggested hybrid algorithm.

REFERENCES

[1] Dan Swinhoe. Brute-force attacks explained, and why they are on the rise. https://www.csoonline.com/article/3563352/brute-force-attacks-explained-and-why-they-are-on-the-rise.html, 2020. Accessed June. 10, 2021.

[2] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, and Dai Wei-di. Digital image encryption algorithm based on chaos and improved DES. In *2009 IEEE International Conference on Systems, Man and Cybernetics*. IEEE, October 2009.

[3] B. Subramanyan, Vivek M. Chhabria, and T.G. Sankar Babu. Image encryption based on aes key expansion. In *2011 Second International Conference on Emerging Applications of Information Technology*, pages 217–220, 2011.

[4] Di Xiao, Xiaofeng Liao, and K.W. Wong. An efficient entire chaos-based scheme for deniable authentication. *Chaos, Solitons Fractals*, 23(4):1327–1331, 2005.

[5] Guodong Ye. A block image encryption algorithm based on wave transmission and chaotic systems. *Nonlinear Dynamics*, 75(3):417–427, 2014.

[6] Lili Liu, Qiang Zhang, and Xiaopeng Wei. A rgb image encryption algorithm based on dna encoding and chaos map. *Computers Electrical Engineering*, 38(5):1240–1248, 2012. Special issue on Recent Advances in Security and Privacy in Distributed Communications and Image processing.

[7] Douglas Stinson. *Cryptography : theory and practice*. Chapman & Hall/CRC, Boca Raton, 2006.

[8] Safwan El Assad and Mousa Farajallah. A new chaos-based image encryption system. *Signal Processing: Image Communication*, 41:144–157, 2016.

[9] Xuanping Zhang, Zhongmeng Zhao, and Jiayin Wang. Chaotic image encryption based on circular substitution box and key stream buffer. *Signal Processing: Image Communication*, 29(8):902–913, 2014.

[10] Huaqian Yang, Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang, and Pengcheng Wei. A fast image encryption and authentication scheme based on chaotic maps. *Communications in Nonlinear Science and Numerical Simulation*, 15(11):3507–3517, 2010.

[11] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law. A fast image encryption scheme based on chaotic standard map. *Physics Letters A*, 372(15):2645–2652, 2008.

[12] Chun-Yan Song, Yu-Long Qiao, and Xing-Zhou Zhang. An image encryption scheme based on new spatiotemporal chaos. *Optik-International Journal for Light and Electron Optics*, 124(18):3329–3334, 2013.

[13] Liang Zhao, Avishek Adhikari, Di Xiao, and Kouichi Sakurai. On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption. *Communications in nonlinear science and numerical simulation*, 17(8):3303–3327, 2012.

[14] Hongjun Wang, Bingbing Song, Qiang Liu, Jing Pan, and Qun Ding. Fpga design and applicable analysis of discrete chaotic maps. *International Journal of Bifurcation and Chaos*, 24(04):1450054, 2014.

[15] Shujun Li and Xuan Zheng. Cryptanalysis of a chaotic image encryption method. In *2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353)*, volume 2, pages II–II. IEEE, 2002.

[16] LIAO Qinan. Color image encryption algorithm and its decryption method protecting from shearing attack. *Computer engineering and design*, 32:509–512, 2011.

[17] TV Laptyeva, S Flach, and K Kladko. The weak-password problem: Chaos, criticality, and encrypted p-captchas. *EPL (Europhysics Letters)*, 95(5):50007, 2011.

[18] M. Essaid, I. Akharraz, A. Saaidi, and et A. Mouhib. Image encryption scheme based on a new secure variant of hill cipher and 1d chaotic maps. *Journal of Information Security and Applications*, 47:173–187, 2019.

[19] Xiuli Chai, Yiran Chen, and Lucie Broyde. A novel chaos-based image encryption algorithm using dna sequence operations. *Optics and Lasers in engineering*, 88:197–213, 2017.

[20] Qiang Zhang, Ling Guo, and Xiaopeng Wei. Image encryption using DNA addition combining with chaotic maps. *Mathematical and Computer Modelling*, 52(11-12):2028–2035, December 2010.

[21] Tian Tian Zhang, Shan Jun Yan, Cheng Yan Gu, Ran Ren, and Kai Xin Liao. Research on image encryption based on DNA sequence and chaos theory. *Journal of Physics: Conference Series*, 1004:012023, April 2018.

[22] Borislav Stoyanov and Krasimir Kordov. Image encryption using chebyshev map and rotation equation. *Entropy*, 17(4):2117–2139, April 2015.

[23] Ashish Girdhar and Vijay Kumar. A RGB image encryption technique using lorenz and rossler chaotic system on DNA sequences. *Multimedia Tools and Applications*, 77(20):27017–27039, March 2018.

[24] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet. A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2. *Nonlinear Dynamics*, 83(3):1123–1136, September 2015.

[25] Ankit Uppal, Rajni Sehgal, Renuka Ngapal, and Aakash Gupta. Merging cryptography& steganography combination of cryptography: Rc6 enhanced ciphering and steganography: Jpeg. In *Proceedings of 5th SAR C-IRF International Conference*, pages 62–64, 2014.

[26] S. Joseph Gladwin and Pasumarthi Lakshmi Gowthami. Combined cryptography and steganography for enhanced security in suboptimal images. In *2020 International Conference on Artificial Intelligence and Signal Processing (AISP)*. IEEE, January 2020.

[27] Abdelkader Moumen and Hocine Sissaoui. Images encryption method using steganographic LSB method, AES and RSA algorithm. *Nonlinear Engineering*, 6(1), January 2017.

[28] Alireza Arab, Mohammad Javad Rostami, and Behnam Ghavami. An image encryption method based on chaos system and AES algorithm. *The Journal of Supercomputing*, 75(10):6663–6682, May 2019.

[29] P. Wasiewicz, J.J. Mulawka, W.R. Rudnicki, and B. Lesyng. Adding numbers with DNA. In *SMC 2000 Conference Proceedings. 2000 IEEE International Conference on Systems, Man and Cybernetics. 'Cybernetics Evolving to Systems, Humans, Organizations, and their Complex Interactions' (Cat. No.00CH37166)*. IEEE.

[30] J. D. WATSON and F. H. C. CRICK. Molecular structure of nucleic acids: A structure for deoxyribose nucleic acid. *Nature*, 171(4356):737–738, April 1953.

[31] George Lindfield and John Penny. Chapter 5 - solution of differential equations. In George Lindfield and John Penny, editors, *Numerical Methods (Fourth Edition)*, pages 239–299. Academic Press, fourth edition edition, 2019.

[32] Martin Kotyrba. Influence of changes in initial conditions for the simulation of dynamic systems. AIP Publishing LLC, 2015.

[33] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[34] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, and Min-Shiang Hwang. A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, 81(1):150–158, 2008.

[35] Dian Rachmawati, Jos Tarigan, and A Ginting. A comparative study of message digest 5(md5) and sha256 algorithm. *Journal of Physics: Conference Series*, 978:012116, 03 2018.

[36] Allan G Weber. The usc-sipi image database version 5. *USC-SIPI Report*, 315(1), 1997.

[37] Z. Wang, E.P. Simoncelli, and A.C. Bovik. Multiscale structural similarity for image quality assessment. In *The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, 2003*. IEEE.

[38] Z. Wang, A.C. Bovik, H.R. Sheikh, and E.P. Simoncelli. Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4):600–612, April 2004.

[39] Yue Wu, Joseph P Noonan, Sos Agaian, et al. Npcr and uaci randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, 1(2):31–38, 2011.

[40] Farhad Maleki, Ali Mohades, S Mehdi Hashemi, and Mohammad Ebrahim Shiri. An image encryption system by cellular automata with memory. In *2008 Third International Conference on Availability, Reliability and Security*, pages 1266–1271. IEEE, 2008.

[41] Nawal El-Fishawy and Osama Zaid. Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms. *International Journal of Network Security*, 5, 01 2007.

[42] H.M. Elkamchouchi and M.A. Makar. Measuring encryption quality for bitmap images encrypted with rijndael and KAMKAR block ciphers. In *Proceedings of the Twenty-Second National Radio Science Conference, 2005. NRSC 2005.* IEEE, 2005.