CryStegIE: An Image Encryption Algorithm based on Symmetric and Asymmetric Cryptography and Steganography

or

ChaDRL: An RGB Image Encryption Scheme based on 3D Chaotic Map, DNA, RSA and LSB

or

An RGB Image Encryption Scheme based on 3D Chaotic Map, DNA, RSA and LSB

- Nirali Parekh, Lynette D'Mello

Abstract

In this paper, a RGB image encryption algorithm based on DNA, chaos, RSA and LSB is proposed. The proposed algorithm leverages the advantages of symmetric and asymmetric cryptosystems. At the same time, it eliminates the step in which the secret key is shared during the encryption process. First, the image is encrypted using a hybrid DNA and Chaos algorithm with a user-input secret key, which is an symmetric algorithm, the plain image is encoded into a DNA matrix and then a permutation scheme is performed on it using the chaotic sequences produced by 3D Lorenz chaotic map. The secret key is encrypted by means of an RSA, an asymmetric algorithm and it is hidden in the ciphered image using a LSB steganographic scheme. This combination of both steganography and cryptography results in increased authority and security. The security analysis show histogram of a cipher image produced a uniform distribution, a higher entropy, a low correlation among image pixels that was significantly decreased. Also, the proposed algorithm has great performance in terms of established metrics such as UACI and NPCR, PSNR, SSIM and UQI. Hence, the simulation results show that our scheme not only can achieve good encryption, but can also resist exhaustive attack, statistical attack and differential attack.

Introduction // intro + lit review merged?

// attacks are increasing

Reliance on digital media for convenient data transfer and communication leads to security concerns in the web networks as criminal activities over the internet become more serious. The

exponential growth of computational power in the past couple of decades has led to stronger and more frequent brute force attacks than ever before [28].

// image data needs to be secure

Image data is used in internet communication for applications such as military communication, medical imaging, multimedia systems, telemedicine, etc. Among them, digital images and digital video have become the important content of data transmission in the network by virtue of its intuitiveness and convenience. They deal with confidential images about their patient, financial status, geographical areas, enemy positions. To make the data secure from various attacks the data must be encrypted before it is transmitted.

//what is cryptography, techniques

Cryptography is defined as the science of protecting information by transforming it into a secure format that can only be comprehended by the intended person. It transforms information from one format to another one that hides the characteristics of the original information. There are two common techniques for encrypting information: symmetric (i.e., secret key) and asymmetric (i.e., public key) [31]. Encryption is the process of transforming a piece of information, known as the plaintext, using an algorithm, known as the cipher, to make it unreadable to anyone except those possessing special secret knowledge, known as a key. The output is known as the ciphertext. The reverse process of transforming ciphertext to plaintext is known as decryption.

// why text encryption technique not valid for image

Various conventional encryption schemes have been studied, such as Data Encryption Standard (DES) [29], Advanced Encryption Standard (AES)[30] and the international data encryption algorithm (IDEA)[37]. However, these schemes have been invented for text or bit encryption and appear not to be ideal for image applications. Although digital images can be processed as two-dimensional data, cryptographic systems that directly use text-encryption techniques often face problems of inefficiency in encryption and decryption, low practicability, and low security [23, 24, 25, 26]. Unlike text messages, multimedia information including image data has some special characteristics like redundancy and high correlation among pixels. Most of the common encryption algorithms such as the AES, DES , RSA[8], and IDEA are built to handle text data only. These algorithms are not suitable for encrypting images [17][3].

// algorithms proposed by other researchers

Many researchers have turned their attention to these research areas and have been proposing new image encryption algorithms based on chaos theory, but a lot of new algorithms have several practical problems, such as keyspace, correlation, differential attack, and key sensitivity.

// why chaos is a good idea

Chaos is seemingly a random movement of a deterministic system. The Chaos system has the properties of ergodicity, boundedness, and sensitivity to initial conditions. Therefore, using a chaotic system in image encryption can meet certain necessary security requirements [47].

// previous algorithms in chaos

Various chaos-based image encryption algorithms [22][16][1][32][40][41]. In particular, the one-dimensional chaotic map like Logistic map is one of the popular chaotic systems because of its speed and simplicity [50]. Some algorithms merge chaotic systems with other algorithms like Hill Cipher [46].

// why only chaos is not enough

However, the chaotic encryption algorithms which utilize 1D or multidimensional chaos maps all include transforming the image pixel position and pixel values. Some works [51][52][53] point out the critical security vulnerabilities of using encryption algorithms constituted by a single and pure chaos map.

// only DNA algorithms

Nowadays, DNA computing, an emerging field permeating into cryptography, utilizes DNA as an information carrier and takes advantage of biological technology to achieve encryption [49]. However, DNA encryption methods have limitations such as complexity, high-cost pieces of equipment, and biotechnology, hence it still cannot be efficiently applied in the encryption field on a practical scale.

// Chaos + DNA

Due to this, hybrid algorithms based on DNA encoding and chaos maps have been explored by researchers [38][39][47][48]. Experimental results show that the algorithm which is simple to implement can successfully resist a variety of attacks, and can be easily applied to gray images as well as color images, hence making it very suitable to use in secure communication.

// DNA+chaos problem:

However, algorithms based on DNA encoding and chaos maps are symmetric cryptographic algorithms. i.e. the sender and receiver require a common secret key for encryption and decryption respectively. The biggest problem with these techniques is the exchange and storage of the secret key.

// Hence asymmetric, but asymmetric very time consuming

The other branch of cryptography algorithms is asymmetric (public) key cryptosystem, which uses the same algorithm for encryption and decryption but with a pair of keys, public and private. Computationally it is impossible to derive the private key from the public key. This branch of cryptography has of major interest, it removes the problem of transfer of the key. But it can not grab the place of a symmetric encryption algorithm because its computation time is comparatively long. Especially for a large amount of data such as images, it is not preferable to use asymmetric encryption, for example, the RSA is 1500 times slower than the symmetric DES algorithm [10]. A brief overview of previous works in the image encryption field have been presented in table 1

// hence my method

In order to leverage the advantages of and overcome the limitations for symmetric and asymmetric encryptions, we propose a hybrid approach. Our suggested method is based on DNA, chaos, RSA, and LSB. We encrypt the image using DNA and chaos maps, then, the secret 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. The presented approach is more efficient in terms of computation cost in image encryption when compared with algorithms that use asymmetric encryption. We also believe that the proposed approach is more secure due to the strength of RSA, DNA, chaos, and LSB methods.

method	**category**	**What issues did it solve?**	**Advantage of the method**	**Security objectives it achieves**
Chaos + DNA	Symmetric cryptography	Solves the slow encryption speed of asymmetric algorithms	faster and secure encryption for images	Authentication, Confidentiality, Data Integrity identification
RSA	Asymmetric cryptography	Solves the issue of key exchange of image encryption	Higher security of key	Authentication, Identification, Confidentiality, Data Integrity and Nonrepudiation
LSB	Keyless steganography	It eliminates the problem of key exchange	secret communication	confidentiality

Table 1

ref	**authors**	**Encryption method**	**Chaotic map used**
22	Haqian Yang et al.	Chaos	Tent map, standard map, logistic map
32	Kwok-Wo Wong et al.	Chaos	logistic map
16	X. Zhang et al.	Chaos	logistic map and piecewise linear chaotic map (PWLCM)
1	Safwan El Assad et al.	Chaos	Modified 2D cat map
41	Liang Zhao et al.	Chaos	1D logistic map

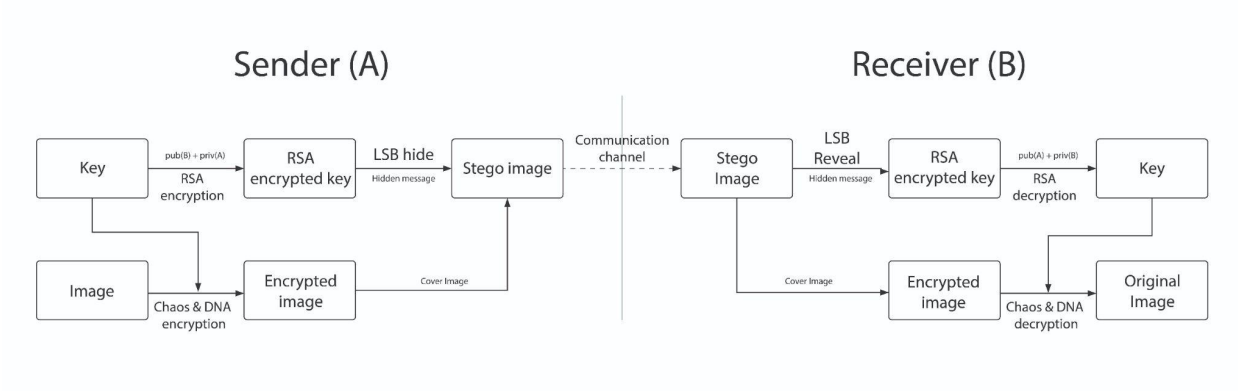
40	Chun-Yan Song et al.	Chaos	NCA map
38	X. Chai et al.	Chaos + DNA	2D logistic map
39	Q. Zhang et al.	Chaos + DNA	1D and 2D logistic maps
46	M. Essaid et al.	Chaos	1D logistic map, sine map,To and Chebyshev map
47	Lili Liu et al.	Chaos + DNA	Logistic map
48	Tian Tian Zhang et al	Chaos + DNA	1D logistic map
56	Borislav Stoyanov	chaos	Chebyshev map
61	Ashish Girdhar et al.	Chaos + DNA	Lorenz and Rossler map
60	R. Guesmi et al.	Chaos + DNA	Lorenz map
57	Ankit Uppal et al.	RC6 + LSB	-
58	S. Joseph Gladwin et al.	ECC + Hill Cipher + LSB	-
59	Abdelkader Moumen et al.	AES + RSA + LSB	-
64	Alireza Arab et al	Chaos + AES	Arnold map
our		Chaos + DNA+ RSA + LSB	Lorenz

// paper arrangement

This paper will be arranged as follows: In Sect. 2, the proposed digital image encryption algorithm based on the Lorenz chaos system, DNA, RSA, and LSB is described, and in Sect. 3, the experimental results of the proposed digital image encryption algorithm are discussed. Finally, analysis in terms of time and security metrics is presented in section 4. Finally, the paper is concluded in Sect 5.

Proposed Algorithm

Figure 1



Concepts in the Proposed Methodology:

1. **DNA**

DNA computing is the performing of computations using biological molecules, rather than traditional silicon chips. This emerging interdisciplinary area is based on the idea that individual molecules can be used for computation in technologies. With the rapid development of DNA computing, the researchers presented many biological operations and algebraic and xor operations based on DNA sequence [13]. A DNA sequence consists of four nucleic acid bases: A (adenine), G (guanine) C (cytosine), and T (thymine), where A and T are complementary, so are G and C. Modern computers process data in the form of binary digits. Ie. 0 and 1. But in DNA coding theory, data is represented by DNA sequences. So we use binary numbers to express the four bases in the DNA sequence. Because 0 and 1 are complementary in a binary system, 00 and 11 are considered complementary and so are 01 and 10. Due to the Watson– Crick complementary relation [42] between DNA bases, only eight kinds of coding combinations satisfy the principle of complementary base pairing. Table 1 gives the eight encoding rules:

(table 1)

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

Since two bits represent one DNA base, for an 8-bit image, each pixel can be expressed as a DNA sequence whose length is 4.

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], similarly according to the seventh decoding rule, it's the decoding sequence is [11001000].

Table 2 shows the XOR operations within DNA bases which are utilized in the proposed algorithm.

(table 2)

Xor operations	**A**	**G**	**T**	**C**
A	A	G	T	C
G	G	A	C	T
T	T	C	A	G
C	C	T	G	A

2. Lorenz Chaos system

Lorenz Systems are dynamic systems that are highly sensitive to small differences in their initial conditions. Chaos occurs even though such systems are deterministic, i.e. their future behavior is fully determined by their initial conditions, with no random elements involved. Given the same initial conditions, the same result is obtained

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

$$\begin{aligned}\frac{\mathrm{d}x}{\mathrm{d}t} &= \sigma y - \sigma x,\\ \frac{\mathrm{d}y}{\mathrm{d}t} &= \rho x - xz - y,\\ \frac{\mathrm{d}z}{\mathrm{d}t} &= xy - \beta z.\end{aligned}$$

.....(1)

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

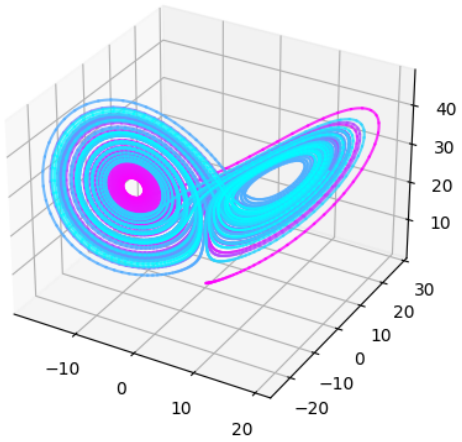
methods like RK45. The graph obtained resembles a butterfly of the dynamical system as shown in Fig. 1.

It is observed that for $\sigma = 10$, $\beta = 8/3\sigma$, β, and $\rho > 24.7$ most Lorenz orbits exhibit chaotic wandering[62].

In the proposed algorithm, we have chosen the Lorenz chaos system which is perhaps one of the best-known chaotic system diagrams, probably because it is not only one of the first, but it is also one of the most complex and random systems.

For the proposed image encryption algorithm, we shall fix $\sigma = 10$, $\rho = 28$ and $\beta = 8/3$ 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 [5].

Figure 2



3. RSA

RSA is an encryption algorithm [8], widely used to securely transmit messages over the internet. RSA algorithm is an asymmetric cryptography algorithm which means that it works on two different keys i.e. Public Key and Private Key. The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, known as the "factoring problem". RSA is a relatively slow algorithm which is why it is not practically used to directly encrypt images. It is only used for encryption of small pieces of data, especially for key transportation or digital signatures. Hence, in our proposed algorithm, we encrypt our key input by the user using the RSA algorithm.

4. LSB

Steganography is the science of concealing secret information in other non-secret data, long before the invention of the computer.Over the years, many different techniques of steganography exist for hiding information in digital data [7, 12]. LSB is the most versatile and efficient known method. LSB is to change the least significant bit of the cover media [6, 11, 12].

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. The LSB technique replaces the Least Significant bit of the pixel value to accommodate one of the secret message bits. If the cover image is well chosen, the message can be successfully hidden and the naked eye cannot perceive the presence of the secret message.

For example, cover image data:

10001101, 10000010, 01110110, 01100001, 00101000, 10000100, 01001010, 01110111

Secret character: C (01000011)

After hiding this secret character (C) in these pixels, the pixel values in binary format are obtained as follows:

10001100, 10000011, 01110110, 01100000, 00101000, 10000100, 01001011, 01110111

In the proposed method, we use the LSB technique to hide the

5. SHA256

A cryptographic hash or digest is like a 'signature' for a data file. SHA-256 generates an almost-unique 256-bit i.e. 32-byte signature for a text [2]. A hash cannot be decrypted back to the original data, thus making it suitable as a secure storage mechanism for passwords [4]. The reason for this is that if a password has been encrypted with only an encryption algorithm, then an attacker would bypass all gates of security if he already has gained access to the secret key. 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, we utilize the SHA256 hashing algorithm to randomize the key and convert the user input key to a fixed size output.

Encryption:

Input: In the proposed algorithm, the sender only needs to input the image to be encrypted I, and a secret key K. This secret key K need not be known by the receiver. To encrypt the image, the sender needs to know the receiver's public key and his private key.

The proposed encryption process is shown in the flowchart in Fig 3, and also steps are mentioned below:

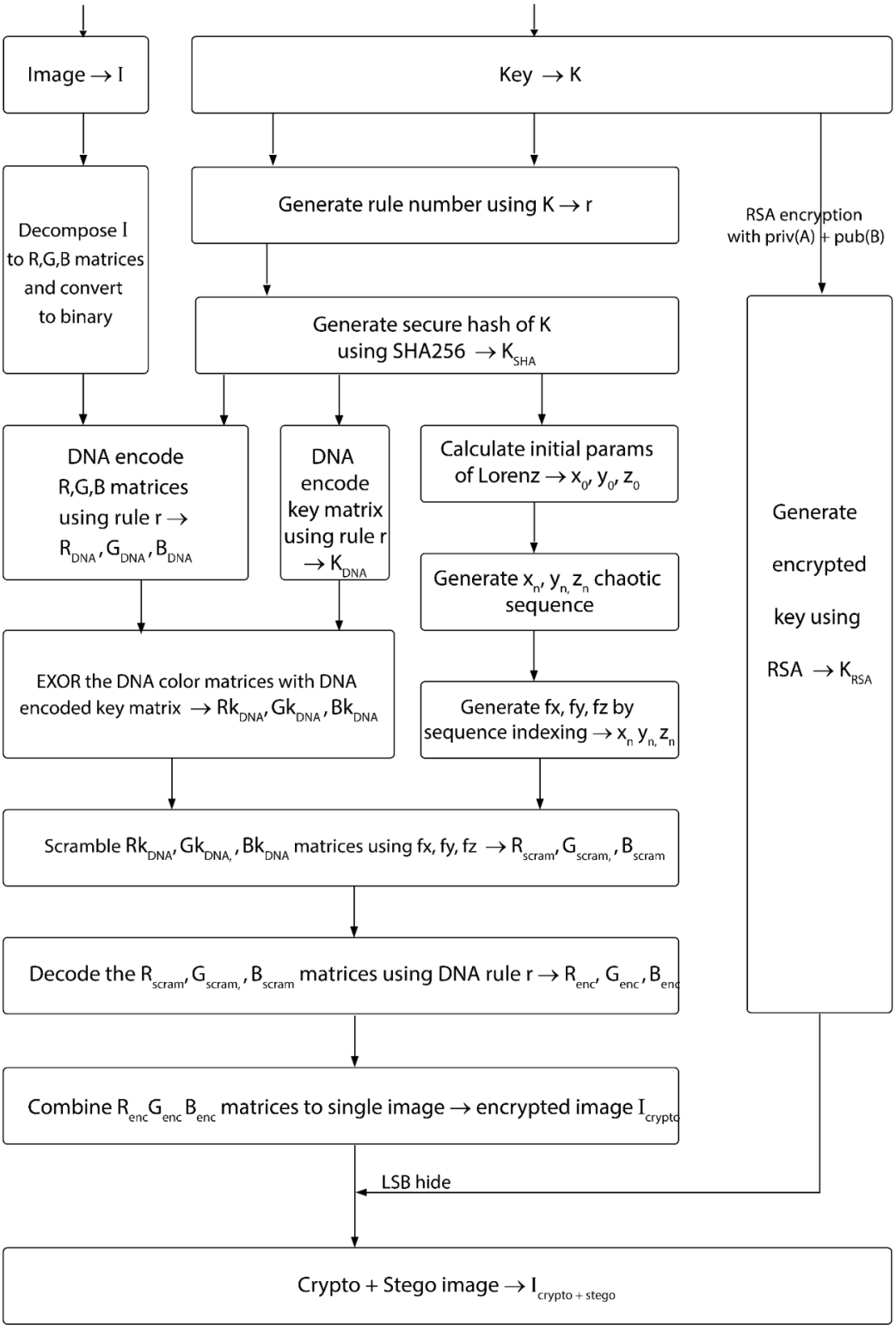
Encryption algorithm:

1. Input 8-bit color image I(m,n,3), where m, n are the image dimensionalities of rows and columns, respectively.
2. Input the key K from the sender.
3. Calculate DNA rule number r by
   $r = (\Sigma\, ascii\ values\ of\ characters\ of\ key\ K)\ mod\ 8\ ]$
4. Splitting the RGB image I into R(m*n), G(m*n), B(m*n) components, and transform the decomposed matrixes of R, G, B to binary matrixes R(m,n *8), G(m,n* 8) and B(m,n *8).
5. Encode the three binary matrices respectively as per the DNA encoding rules selected by rule number r where $r \in [1, 8]$ and get three DNA sequence matrixes R_{DNA}(m,n *4), G_{DNA}(m,n* 4), and B_{DNA}(m,n *4)
6. Compute Hash(K) of 256 bits using the SHA256 algorithm. K_{SHA} (256*1)
7. Convert K_{SHA} to (m*2, n*4) key matrix by repeating K_{SHA} as many times as necessary. Encode this key matrix in accordance with the DNA encoding rule r where $r \in [1, 8]$ and obtain K_{DNA}(m,n* 4).
8. Exclusive OR the R_{DNA}, G_{DNA} and B_{DNA} with K_{DNA} using DNA XOR rules. Eg $R_{DNA}[i,j] = R_{DNA}[i,j] \wedge K_{DNA}[i,j]$
9. Compute Lorenz initial parameters x0, y0, z0 by chain-XOR of K_{SHA}.
10. Generate the chaotic sequence x_n, y_n and z_n whose length l = m*n*8/2 by using Lorenz chaos where the initial conditions are x0, y0, z0, and system parameters are σ, β, and ρ. FiguresThen we use threshold functions using equation (1) to get binary
11. Generate fx, fy, fz by sequence indexing x_n, y_n, and z_n sequences where fx[i] holds the index of where x[i] belongs in the sorted order of x_n
12. Scramble R_{DNA}, G_{DNA}, and B_{DNA} matrices using fx, fy, and fz to obtain R_{scram}, G_{scram}, and B_{scram}
13. Decode the three matrices R_{scram}, G_{scram}, and B_{scram} respectively in accordance with the DNA decoding rule r where r and get R_{enc}(m,n), G_{enc}(m,n), and B_{enc}(m,n)
14. Recover the RGB image by combining R_{enc}(m,n), G_{enc}(m,n) and B_{enc}(m,n) to obtain I_{crypto} - encrypted image.
15. Encrypt key K by RSA algorithm using the private key of sender A - priv(A) and public key of receiver B - 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 $I_{crypto+stego}$

Figure 3

Encryption Process

Sender (A)



Decryption:

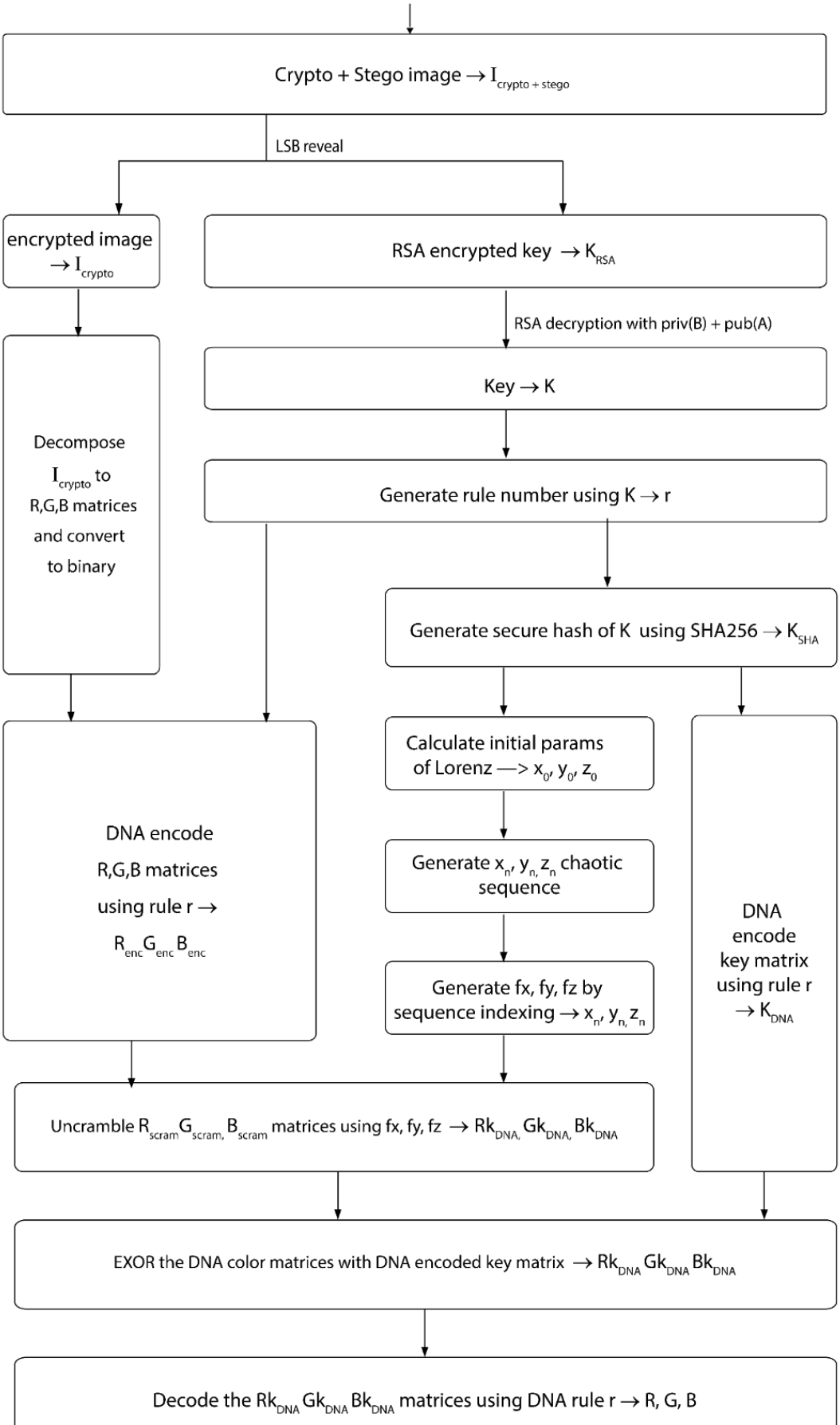
> **Input:** In the proposed decryption algorithm, the receiver only needs to receive the encrypted image via the communication channel. And to decrypt the image, the receiver needs to know the sender's public key and his private key.

The algorithm decryption process can be seen as the inverse of the encryption process. In the decryption process, we must have the following: private key of the receiver, the public key of the sender and the image to be decrypted. Thus, there is no exchange or transfer of key needed. The proposed decryption process is shown in the flowchart in Fig 4.

Figure 4

Decryption Process

Receiver(B)



Experimental results

The proposed algorithm is tested using a python interpreter, 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 applied to the test color image of respective sizes given in table 2. The color images were obtained from USC-SIPI Image Database [63].

Test images: (table2)

image	**Height**	**width**	**pixels**
Lena	512	512	262144
baboon	512	512	262144
tulips	768	512	393216
Frymire	1118	1105	1235390
peppers	512	512	262144

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. As an example, Figure 1a shows the original image Lena, Figure 1b shows its encrypted version, Figure 1c shows its crypto+stego image and Figure 1d shows the recovered image. The encrypted image doesn't show any segmented color clusters or any resemblance to the source figures. Similarly, Figure 2a, 2b, 2c, and 2d show figures the respective image stages for Baboon.

Figure 1 (a, b, c, d)

Lena lena encrypt lena cryptot+stego lena recovered

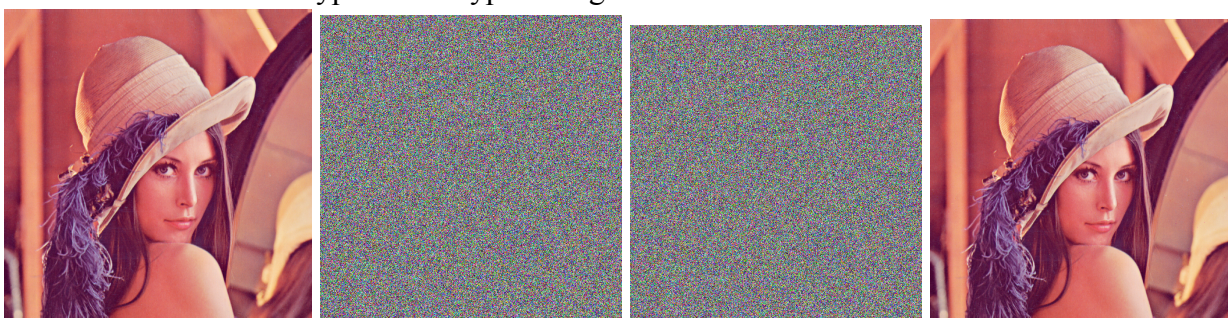
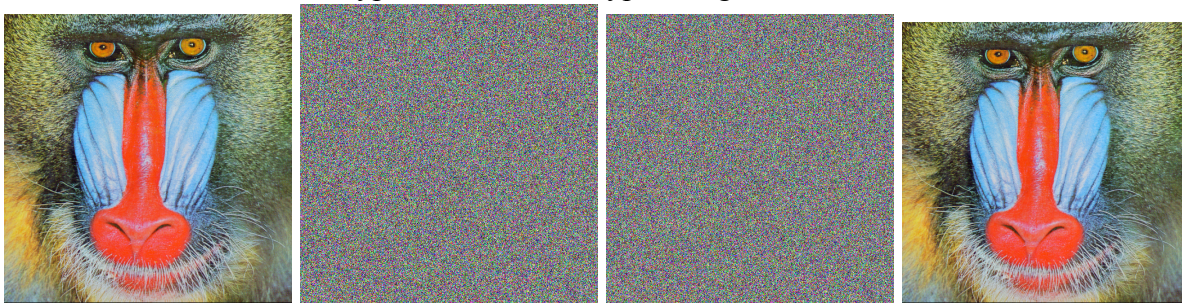


Figure 2 (a, b, c, d)

baboon baboon encrypt baboon crypto+stego baboon recovered



Performance in terms of time consumption and security analysis

1. Time consumption

The average image encryption/decryption times, the average LSB hide/reveal times, and the average time to encrypt and decrypt the key using RSA are given in Table 3.
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 respectively.

Table 3 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 Assad et al. [1] and Zhang et. al., algorithm [16], which shows marked better computational performance.

Time for each stage (table 2)

image	Time to encrypt	Time to use the key	Time for hiding using LSB	Total encryption time	Time to reveal stego	Time to decrypt RSA key	Time to decrypt the image	Total decryption time
Lena	80.005542516708374	0.0399122238159179 7	0.009225368499755 86	80.05468011	0.037821292877197266	0.028674364089965 82	85.910418033599854	85.97691369
baboon	80.690471172332764	0.0462510585 78l	0.018993616104125977	80.70946479	0.044554233551025 39	0.028733968734741 21	86.222368001937866	86.2956562

tulips	115.33051300048828	0.03956413269042969	0.015948295593261 72	115.3860254	0.042144298553466 8	0.031843423843383 79	124.18020462989807	124.2541924
Frymire	375.69150233268738	0.04241156578063965	0.024935960769653 32	375.7588499	0.057080984115600586	0.025938034057617188	.25579810142517	0.3388171196
peppers	80.533897399902344	0.05945825576782226 6	0.015956401824951172	80.60931206	0.039325714111328125	0.033577442169189 45	33.04449200630188	33.11739516

Comparison of timings of referenced algorithms on Lena (table 3)

reference	image	size	Encryption time	Decryption time
our	Lena	512 color	80.05468011 millisec	85.97691369 millisec
22	Lena	512 color	93.8 millisec	102.6 millisec
32	Lena	512 color	95.6 millisec	104.31 millisec
16	Lena	512 color	30 millisec	30 millisec
64	Lena	256 gray	2.9 sec	-
1	Lena	512 color	31.72 millisec	32.17 millisec
AES	Lena	256 gray	454.1 sec	465.7 sec

2. Security analysis

Cryptanalysis is the science of studying the security properties of primitives and analyzing their weaknesses

Imperceptibility - MSE, PSNR, SSIM, UQI

MSE and PSNR

The mean-square error (MSE) and the peak signal-to-noise ratio (PSNR) is used to compare image encryption quality. The MSE is the average squared error between the two given images, whereas PSNR computes the peak signal-to-noise ratio, in decibels, between two images.

The mean-squared error is calculated using the following equation:

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

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 equation:

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

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

A higher value of PSNR is good because of 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. Here, the signal is the original image, and the noise is the reconstruction error.

SSIM:

The structural similarity (SSIM) [21] index is a metric used for measuring the similarity between two images. The fundamental idea of structural information is that there is strong inter-dependency within pixels that are spatially close. These dependencies hold important intelligence about the structure of the information in the image. The SSIM index is a decimal value between -1 and 1, where two identical images have an SSIM value of 1. Let x = {xi | i = 1, 2, ...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 [20]:

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

With

- μ_x the average of x;
- μ_y the average of y;

UQI:

The UQI defined in [19] corresponds to the special case that C1 = C2 = 0, which produces unstable results when either $(\mu_x^2+\mu_y^2)$ or $(\sigma_x^2+\sigma_y^2)$ is very close to zero. Hence, UQI is the ability to measure the information loss that occurred during the image degradation process. The universal quality index is defined as:

$$Q = \frac{4\sigma_{xy}\bar{x}\bar{y}}{(\sigma_x^2 + \sigma_y^2)\,[(\bar{x})^2 + (\bar{y})^2]}$$

Table 4 tabulates the MSE, PSNR, SSIM, and UQI values that are performed between plain and encrypted images and then between plain and decrypted images.

In the first case, between plain and encrypted 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 decrypted images, the obtained values of SSIM and UQI are very close to 1, those of PSNR high, and MSE values close to 0, as shown in Table 4. As a result, the different resultant values of MSE, PSNR, SSIM, and UQI show the effectiveness of the proposed encryption algorithm applied to secure medical image transmission.

(table 4)

Name		MSE	PSNR	SSIM	UQI
lena	lena.png & lena_encrypt.png	8828.6	8.6719	0.0200691347914802	0.6996871913002396
	lena_encrypt.png & lena_stego.png	6.7520e-04	79.836	0.9999999847365891	0.9999999979553396
	lena.png & lena_recovered.png	0.7372	49.455	0.998753125760862	0.9999422803580426
baboon	baboon.png & baboon_encrypt.png	8597.6	8.7870	0.020097573705781236	0.7235666616079698
	baboon_encrypt.png & baboon_stego.png	6.6630e-04	79.894	0.9999999849456226	0.999999997938643
	baboon.png & baboon_recovered.png	0.7975	49.113	0.9995542294832855	0.9999720500955025
tulips	tulips.png & tulips_encrypt.png	1.1032e+04	7.7043	0.01799095328632238	0.5494510979114048

	tulips_encrypt.png & tulips_stego.png	4.4590e-04	81.638	0.9999999901372519	0.9999999986522304
	tulips.png & tulips_recovered.png	0.3182	53.104	0.9991712368676201	0.9999462296195 59
Frymire	frymire.png & frymire_encrypt.png	1.6022e+04	6.0835	0.012397199443158776	0.471360816508164 14
	frymire_encrypt.png & frymire_stego.png	1.4247e-04	86.594	0.9999999967300597	0.9999999995675 11
	frymire.png & frymire_recovered.png	0.1226	57.246	0.9997625728080708	0.9995402343956846
peppers	peppers.png & peppers_encrypt.png	1.0318e+04	7.9950	0.019511758614893664	0.590748390571352 6
	peppers_encrypt.png & peppers_stego.png	6.5740e-04	79.953	0.9999999851053697	0.9999999980057 46
	peppers.png & peppers_recovered.png	0.5684	50.585	0.9985791639510093	0.9994603939362466

Resisting the chosen plaintext attack:

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. In the worst case, the attacker can get the key for decryption directly.

Differential Attack - NPCR, UACI

We analyze a chosen-plaintext attack named differential attack.

In general, a common characteristic of an image encryption scheme is to be sensitive to minor modifications in plain images. The differential analysis allows an adversary to create small changes in the plain image and revise the encrypted image. The alternation level can be computed employing two formulae, namely, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) [35].

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:

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

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

where D is a two-dimensional set, having the same size as image $C1$ or $C2$, 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 5.
The optimal NPCR value is almost 99.61%, and the optimal UACI value is almost 33.46%.[43][44]

(table 5)

image	**NPCR**	**UACI**
Lena	0.996177673339844	0.304466850929011
baboon	0.995958964029948	0.298377382365707
peppers	0.996293385823568	0.326202158211103
tulips	0.996026780870226	0.336530518375970
Frymire	0.996224943809917	0.407739127338635

Statistical analysis: histogram and correlation, entropy

The following measures [3] show that the confusion and diffusion properties are preserved in the proposed image encryption and authentication scheme.

(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 3 shows the histogram of two 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.

Figure 3 (a, b)
Lena, Lena encrypt

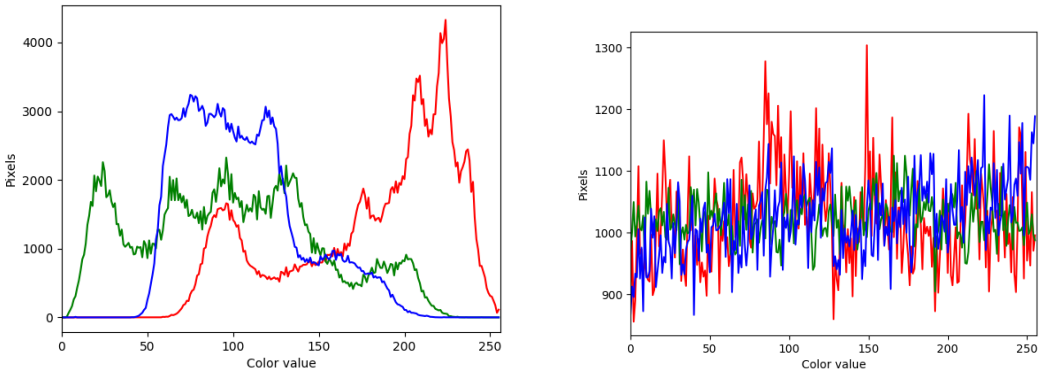
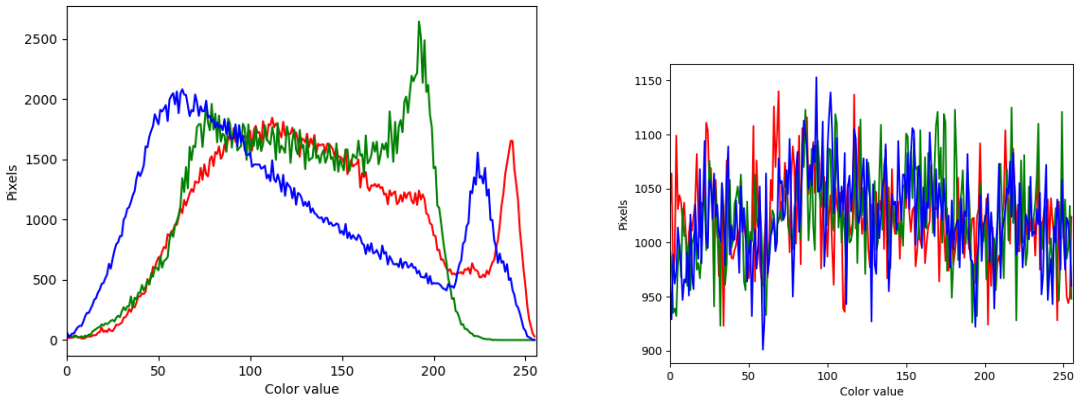


Figure 4 (a, b)
Baboon, Baboon encrypt



Histogram analysis of three channels (red, green, and blue) of the plain and encrypted images is given. It is observed that the histograms of the encrypted image are significantly different from that of the plain image.

(B.) Correlation Analysis

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 ways to measure this property. Indeed, it is well-known that adjacent pixels in the plain images are very redundant and correlated.

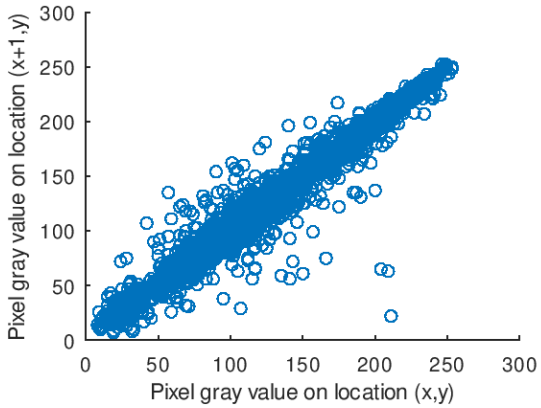
The correlation coefficient is calculated using the formula [14, 15]:

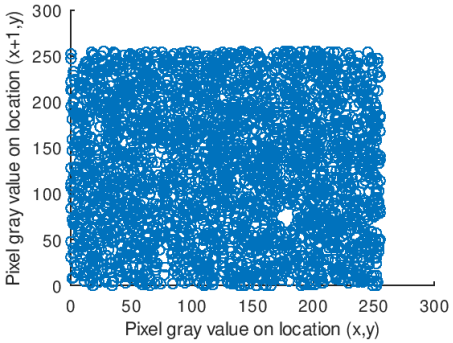
$$CC = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{n=1}^{N} (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{n=1}^{N} (x_i - E(x))^2} \sqrt{\sum_{n=1}^{N} (y_i - E(y))^2}} \quad (4)$$

Where $E(x) = \frac{1}{N} \sum_{n=1}^{N} x_i$, x and y are the pixel values of the same indices of the original image and the ciphered image respectively.

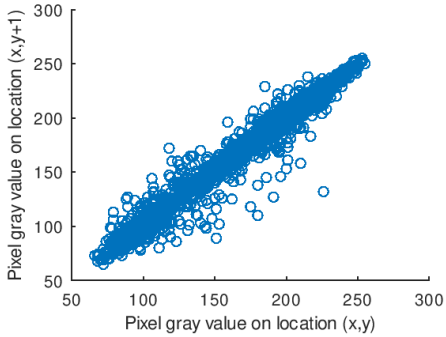
If the correlation coefficient is near 1, this means that the original image and the encrypted image are very dependent on each other, i.e. the original image can be reproduced easily from the encrypted image[15].

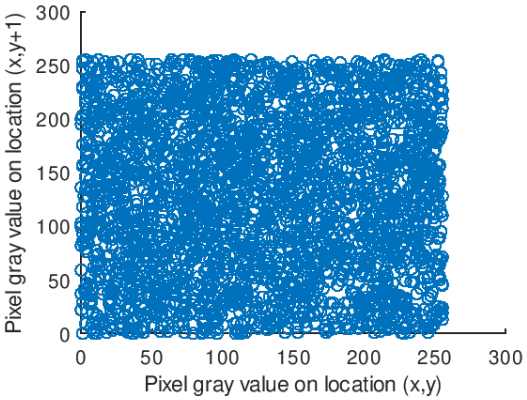
Lena original and LenaFrymire encrypt Figure 5 (a, b, c, d, e, f)
Horizontal



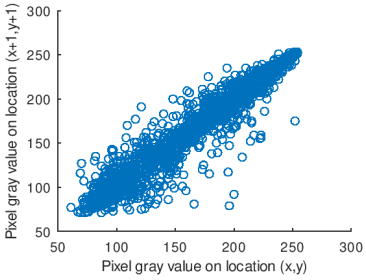


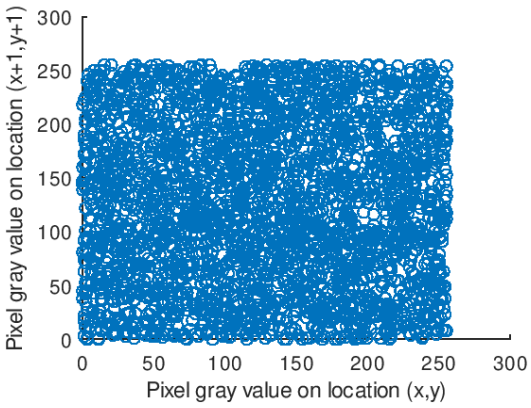
Vertical





Diagonal





			Plain image			**Cipher image**		
reference	**Image name**	**Image size**	**H plain**	**V plain**	**D plain**	**H cipher**	**V cipher**	**D cipher**
41	Lena	128*128 gray	0.94800	0.88510	0.85460	0.02480	-0.00940	-0.01830
46	Lena	512*512 color	-	-	-	-0.0004541	0.0005994	-0.0029000
47	Lena	128*128 color	0.9099	0.9390	0.8659	0.0059	-0.0042	0.0180
64	Lena	256*256 gray	-	-	-	0.0027	0.0012	0.0003015
AES	Lena	256*256 gray	-	-	-	0.2724	0.2681	0.0765
38	Lena	512*512 color	0.9755	0.9603	0.9443	-0.0045	-1.62e-04	0.0053
39	Lena	256*256 gray	0.9468	0.9697	0.9153	0.0036	0.0023	0.0039
our	Lena	512*512 color	0.9781	0.9871	0.9713	**-0.004308**	0.019724	**3.2492e-03**
22	Lena	512*512 color	0.98022	00.98663	0.96468	-0.00209	-0.01618	0.01780
32	Lena	512*51	0.97510	0.98892	0.96704	0.00681	0.00782	0.00323

		2 color						
40	Lena	256*256 gray	0.96592	0.94658	0.92305	0.00550	0.00411	**0.00021**
our	peppers	512*512 color	0.9799	0.9711	0.9605	0.012016	**1.27097e-03**	7.4266e-03
59	Lung Cancer	256*256	0.9603	0.9251	0.9143	0.0045	0.0204	0.0425
our	baboon	512*512 color	0.9016	0.8618	0.8568	0.017719	0.018558	0.012468
our	tulips	512*768 color	0.9818	0.9904	0.9827	8.0345e-03	-0.018558	-0.022625
our	frymire	1105*1118 color	0.9039	0.8778	0.9256	**3.6052e-03**	0.023570	**3.2432e-03**

(C.) 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 plaintext of a message to minimize the amount of structure that is present in the insecure plaintext message.
The information content Hx of a value x that occurs with probability Pr[x] is:

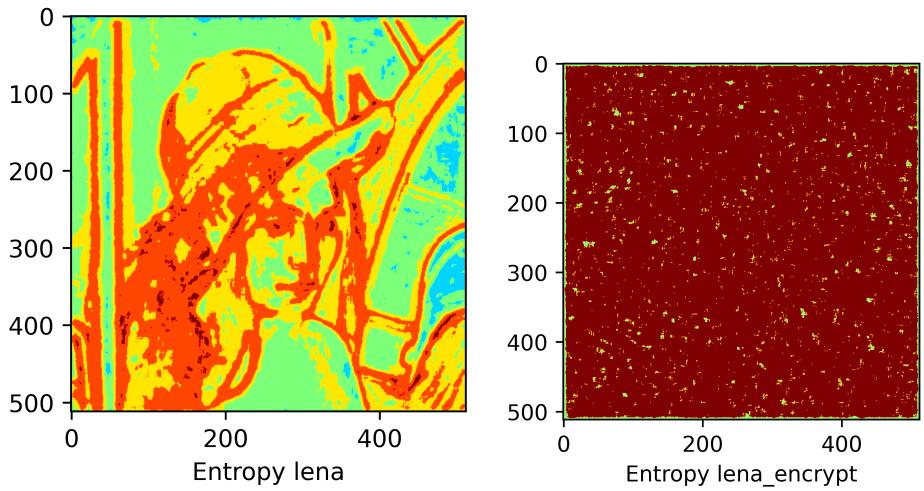
$$H_x = -\log_2(\Pr[x]).$$

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

$$H(X) = E[H_X] = \sum_x \Pr[x] H_x = \sum_x -\Pr[x]\log_2(\Pr[x]).$$

Figures 6a and 6b show the entropy graphs of the original Lena and encrypted Lena respectively.

Lena and Lena_encrypt Figure 6 (a, b)



Conclusion:

In this paper, we present a novel image encryption scheme based on symmetric, asymmetric encryption, and steganography. To begin, the image is encrypted using a symmetric algorithm that combines DNA sequence operations and Lorenz chaotic system. On the other hand, the key which is used to encrypt the image is now encrypted with an asymmetric algorithm i.e. RSA. Furthermore, we hide our encrypted key in the cipher image using LSB steganographic techniques. Experimental results and security analyses show that the proposed scheme has a good encryption effect, and high sensitivity to the secret key and the plain image. Furthermore, the algorithm can resist most known attacks, such as differential attack, entropy attack, and known-plaintext attack. The security analysis outcomes can be seen in Tables 2, 3, 4, 5, 6, and 7 and it is evident that the proposed algorithm is invulnerable against renowned attacks. So we can make use of it for secure and economical image encryption.

References:

[1] https://sci-hub.se/https://doi.org/10.1016/j.image.2015.10.004

[2] https://iopscience.iop.org/article/10.1088/1742-6596/978/1/012116/pdf //sha256

[3] https://link.springer.com/article/10.1007/s11071-013-1074-6

[4] https://dusted.codes/sha-256-is-not-a-secure-password-hashing-algorithm //why only AES should not be used.

[5] https://sci-hub.se/https://doi.org/10.1063/1.4912758 //change in initial values of Lorenz gets new pattern

[6] LSB -- J. Fridrich and P. Lisonek, "Grid coloring in steganography", *IEEE Transactions on Information Theory*, 53 (4): 1547–1549, (2007)

[7] S. M. Douiri, M.B. O. Medeni, S. Elbernoussil, E. Souidi. "A New Steganographic Method For Grayscale Image Using Graph Coloring Problem". *Applied Mathematical Sciences*. 7, No. 2, 521–527 (2013). --- steganography method

[8] https://people.csail.mit.edu/rivest/Rsapaper.pdf //RSA

[9] Systematic literature review: comparison study of symmetric key and asymmetric key algorithm (Priasnyomo Prima Santoso et al , 2018) // why RSA not used for images

[10] Douglas R. Stinson. *Cryptography: Theory and Practice, (Discrete Mathematics and Its Applications)*. Chapman & Hall/CRC Press, New York, November (2005)
(RSA 1500 times slower than DES)

[11] LSB -- C.M. Wang, N.I. Wu, C.S. Tsai and M.S. Hwang, "A high quality steganography method with pixel-value differencing and modulus function", *J. Syst. Softw*. 81, 150–158, (2008).

[12] LSB -- D.W. Bender, N.M. Gruhl and A. Lu, *Techniques for data hiding, IBM Syst*. J. 35, 313–316, (1996)

[13] Wasiewicz P, Mulawka JJ, Rudnicki WR, Lesyng B. Adding numbers with DNA. IEEE International Conference on Systems Man and Cybernetics 2000;2000:265–70.

[14] https://www.researchgate.net/profile/Nawal-El-Fishawy/publication/46055851_Quality_of_Encryption_Measurement_of_Bitmap_Images_with_RC6_MRC6_and_Rijndael_Block_Cipher_Algorithms/links/546f56110cf2d67fc0310d89/Quality-of-Encryption-Measurement-of-Bitmap-Images-with-RC6-MRC6-and-Rijndael-Block-Cipher-Algorithms.pdf

[15] https://ieeexplore.ieee.org/abstract/document/1502142

[16] https://www.sciencedirect.com/science/article/abs/pii/S0923596514001064

[17] Xiao D, Liao X, Wong K (2005) An efficient entire chaos-based scheme for deniable authentication. Chaos Solitons Fract 23:1327–1331 //why AES DES not used for image encryption

[18] https://www.degruyter.com/document/doi/10.1515/nleng-2016-0010/html //stego + rsa + aes image encryption

[19] https://sci-hub.se/https://ieeexplore.ieee.org/document/995823 // OG UQI paper

[20] // ssim -> https://ieeexplore.ieee.org/abstract/document/1284395

[21] https://www.cns.nyu.edu/pub/eero/wang03b.pdf // ssim OG paper

[22] H. Yang, K.-W. Wong, X. Liao, W. Zhang, P. Wei, A fast image encryption and authentication scheme based on chaotic maps, Commun. Nonlinear Sci. Numer. Simul. 15 (11) (2010) 3507–3517.

[23] T. Caulfield, C. Ioannidis, D. Pym, Discrete Choice, Social Interaction, and Policy in Encryption Technology Adoption (Short Paper). In the International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg (2016), pp. 271-279

[24] Z. Cai, D. Huang, Research on DES Data Encryption Technology in Network Information Security [J]. Computer Measurement & Control. 25, 241-247 (2017)

[25] Sun Y Q, Wang X H. Information encryption technology with strong robustness based on QR code and matrix mapping [J]. Packaging Engineering. 38, 194-199 (2017)

[26] S.W. Lee, S.M. Park, K.B. Sim, et al., Smart Door Lock Systems using encryption technology [J]. 27(1), 65–71 (2017)

[27] https://www.ijeat.org/wp-content/uploads/papers/v3i4/D2998043414.pdf // review paper of image encryption

[28] https://www.csoonline.com/article/3563352/brute-force-attacks-explained-and-why-they-are-on-the-rise.html // why brute force attacks are on the rise

[29] Yun-Peng Z, Wei L, Shui-ping C, Zheng-jun Z, Xuan N, Wei-di D. Digital image encryption algorithm based on chaos and improved DES. In: Systems, man and cybernetics. SMC. International conference on. IEEE; 2009. p. 474–9.

[30] Subramanyan B, Chhabria V, Babu T. Image encryption based on AES key expansion. In: Emerging applications of information technology (EAIT), 2011 second international conference. IEEE; 2011. p. 217–20.

[31] https://ieeexplore.ieee.org/document/8308215 //symmetric and asymmetric algos

[32]] K.-W. Wong, B.S.-H. Kwok, W.-S. Law, A fast image encryption scheme based on chaotic standard map, Phys. Lett. A 372 (15) (2008) 2645–2652

[33] Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos 8:1259–1284

[34] Hao B-L (1993) Starting with parabolas: an introduction to chaotic dynamics. Shanghai Scientific and Technological Education Publishing House, Shanghai, pp 10–12 //chaos

[35] https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.390.2127&rep=rep1&type=pdf#:~:text=The%20NPCR%20and%20UACI%20are,(usually%20a%20single%20pixel)

[36] https://www.researchgate.net/publication/259190481

[37] Chang H.S., "International Data Encryption Algorithm" CS627-1 Fall, 2004. //IDEA base

[38] https://sci-hub.se/https://www.sciencedirect.com/science/article/abs/pii/S0143816616301701

[39] https://sci-hub.se/https://doi.org/10.1016/j.mcm.2010.06.005

[40] C.-Y. Song, Y.-L. Qiao, X.-Z. Zhang, An image encryption scheme based on new spatiotemporal chaos, Opt.—Int. J. Light Electron Opt.

[41] L. Zhao, A. Adhikari, D. Xiao, K. Sakurai, On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption, Commun. Nonlinear Sci. Numer. Simul. 17 (8) (2012) 3303–3327

[42] https://www.nature.com/articles/171737a0 // DNA table

[43] Y. Wu, J.P. Noonan, S. Agaian, Npcr and uaci randomness tests for image encryption, Cyber J.: Multidiscip. J. Sci. Technol., J. Sel. Areas Telecommun. (JSAT), 2011, pp. 31–38.

[44] F. Maleki, A. Mohades, S.M. Hashemi, M.E. Shiri, An image encryption system by cellular automata with memory, in: Third International Conference on Availability, Reliability and Security, 2008. ARES 08, IEEE, 2008, pp. 1266–1271

[45] Singh P, Singh K. Image encryption and decryption using blowfish algorithm in Matlab. Int J Sci Eng Res 2013;4(7):150–4.

[46] https://sci-hub.se/https://www.sciencedirect.com/science/article/abs/pii/S2214212618302400

[47] https://sci-hub.se/https://www.sciencedirect.com/science/article/abs/pii/S0045790612000201

[48] https://iopscience.iop.org/article/10.1088/1742-6596/1004/1/012023/pdf

[49] https://arxiv.org/pdf/0903.2693.pdf //pseudo DNA paper

[50] Wang H, Song B, Liu Q, Pan J, Ding Q. FPGA design and applicable analysis of discrete chaotic maps. Int J Bifurc Chaos 2014;24(04):1450054. //why 1D chaos map are low resource

[51] Shujun L, Xuan Z. Cryptanalysis of a chaotic image encryption method, Proceedings of IEEE, International Symposium on Circuits and Systems, Omni Press. Phoenix-Scottsdale 2002;2002:87–91.

[52] Qinan L. Color image encryption algorithm and its decryption method protecting from shearing attack. Comp Engineer Design 2011;32:509–16.

[53] Laptyeva TV, Flach S, Kladko K, The weak-password problem: Chaos, criticality, and encrypted p-CAPTCHAs, EPL. 95 (2011).

[56] https://www.mdpi.com/1099-4300/17/4/2117/htm

[57] http://www.iraj.in/journal/journal_file/journal_pdf/3-85-141216665285-87.pdf // combination of crypto + stego

[58] https://sci-hub.se/10.1109/AISP48273.2020.9073306 // combination of crypto + stego

[59] // symmetric, asymmetric and stego
https://www.degruyter.com/document/doi/10.1515/nleng-2016-0010/html#:~:text=Steganography%20is%20a%20technique%20that,to%20extract%20the%20secret%20data.&text=We%20encrypt%20the%20image%20using,ciphred%20image%20using%20LSB%20technique

[60] https://link.springer.com/article/10.1007/s11071-015-2392-7

[61] https://link.springer.com/article/10.1007/s11042-018-5902-z

[62] https://www.sciencedirect.com/science/article/pii/B9780128122563000142

[63] Sipi usc database from where took photos
“The USC-SIPI Image Database,” [Online]. Available: http://sipi.usc.edu/database. [Accessed April 3, 2021].

[64] https://link.springer.com/article/10.1007/s11227-019-02878-7#Sec11