INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 3 - V7I3-1643)
Available online at: https://www.ijariit.com

Combined Sine-Logistic chaotic map and its application in an image encryption scheme

Aasha Suresh
aashasa078@gmail.com
SASTRA Deemed To Be University, Thanjavur, Tamil Nadu

ABSTRACT

With the rapid growth of technology, Information Security has become a significant concern in the contemporary world. Today, many new-fangled methods have been developed to transmit data in a fast and secure way. Among all the data that is being transmitted, digital images play a vital role. About 60 percent of the data that is being transmitted is in the form of digital images. These digital images require a safe and concealed method of transmission. Researchers have developed many concepts to execute image encryption like chaos theory, data encryption standard (DES), image filtering technology, advanced encryption standard (AES), neural network-based image encryption, DNA coding, fractional Fourier transforms, quantum theory, and compressive sensing. In the late years, additional scholars have focused on executing chaos theory in image encryption schemes due to large key space's advantages and high-level security. In the project, we have provided a new logic for digital image encryption. This method combines the usage of the logistic map and sine map to create a new chaotic map. By doing this, the randomness, sensitivity and robustness are further increased. The proposed system used row by row and column by column confusion and diffusion mechanisms, which increases the security multi-fold. Unlike conventional methods, this method uses scrambling pixels from their actual rows and columns and applies bit-level manipulation to each pixel. This disrupts the interrelationship between adjacent pixels of the ciphered image. Further, the security and simulation analysis show that 1DSP-1E has a greater level of reliability than the other encryption schemes.

Keywords*— *Encryption, Decryption, Key Space, Logistic Space, Sine Map

1.1 INTRODUCTION

In this age where everything is wrapped up in technology, secure data transmission is a pivotal process. Remarkable developments have been made in the creation of a secure channel for transmission and protect the data against differential attacks. Among various methods (chaos theory, data encryption standard (DES), image filtering technology, advanced encryption standard (AES), neural network-based image encryption, DNA coding, fractional Fourier transforms, quantum theory) that are already available for the secure transmission of images, the use of chaotic map has proved to be one of the most efficient ways.

The chaotic system utilised within the crypto-system is split into one-dimensional (1D), and high dimensional (HD) chaos. 1D chaos such as Logistic map, Sine map, and Tent map has fast computational performance. In contrast, HD chaotic systems like Lorenz system, hyperchaos, and chaotic standard map have large parametric space and high security. 1D chaotic maps have a straightforward structure and are also easy to implement them.

Presently, we design to develop a one-dimensional sine map which possesses large keyspace and high randomness. 1DSP is used in creating a new encryption scheme that has high robustness and security. This scheme is also efficient because it requires fewer computations and fewer simulation time to encrypt colour images. High keyspace, high security, high efficiency in computational complexity, simplicity, and simulation time are some advantages of this scheme. The simulation outputs and the security analysis indicate that the proposed method has better performance in encryption efficiency, security, and resistivity for many common attacks.

This project report remainder is organised as follows: Chapter 2 reviews the comparison of two 1D chaotic maps. Chapter 3 presents the proposed 1DSP chaotic map. Chapter 4 shows the proposed 1DSP-IE encryption scheme and the process. Chapter 5 presents the simulation and security analysis of the proposed 1DSP-IE.

2. LOGISTIC MAP

The logistical map's mathematical meaning is

$$x_{i+1} = 4\gamma x_i(1 - x_i)$$

Where, In the range of [0,1], γ is a parameter. For γ ∈ [0.89, 1}.

2.1 SINE MAP

Output Performance of the sine map falls between [0,1]. The mathematical definition is

$$xi{+}1 = \eta \sin(\pi xi)$$

where η∈ [0, 1] is the control parameter. The sine map displays chaotic activity when η falls within the range of [0.87, 1].

Fig1 (a) and 1(b) demonstrate the bifurcation diagrams of the logistic and sine maps. We observe that both sine map and logistic map shows chaotic behaviour as the respective control parameters approach 1. Both these maps have the disadvantage of small parameter space.

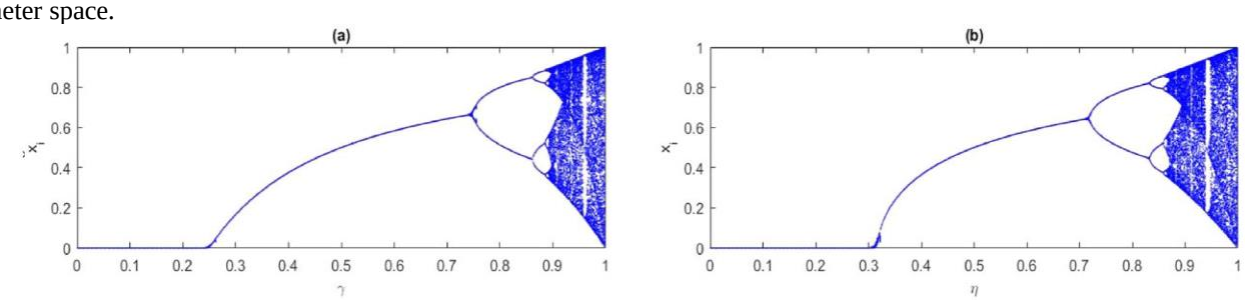


Fig 2.1: (a) Bifurcation diagram of Logistic map (b)Bifurcation diagram of Sine Map

3. 1D COMBINED SINE-LOGISTIC CHAOTIC MAP

In this chapter, we propose a new chaotic map driven by combining both logistic map and sine map. It is defined mathematically, as

x(n+1) = r*x(n)*sin(1-x(n));

The control parameter r is always greater than 0, and the initial value of x is assumed to be 0.7. The first part f(x i , α) = (x I (α+ 1)) is designed to produce increasing values for x 0 ∈ [0, 1]. We use the sine map-inspired function to prevent an increase in exponential value. For the initial value x(0)∈[0, 1], g (xi, β) always falls within the range of [0,1], which produces a good performance limit. The sine map offers greater complexity, and also the parameter xi makes this algorithm less predictable and more complex.

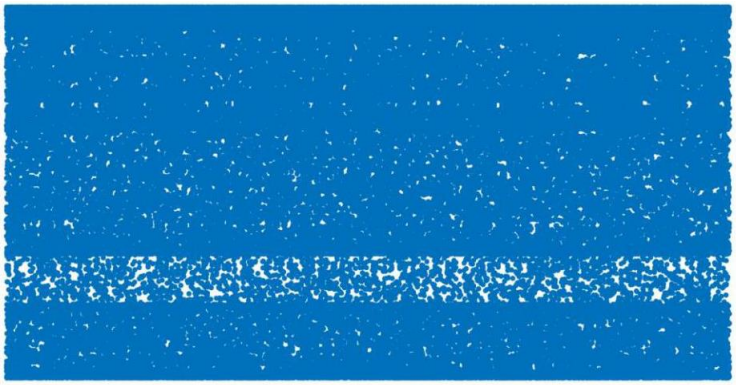


Fig 3.1: Key map of the proposed algorithm for n=0:25536

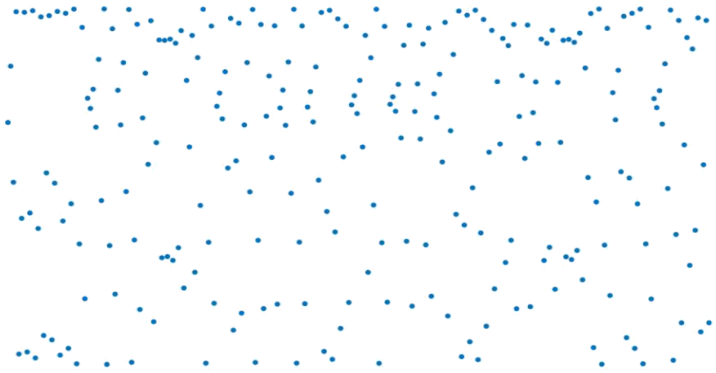


Fig 3.2: Key map of the proposed algorithm for n=0:255

3.1 Performance Analysis

Every chaotic map has its own behavioural traits and how it differs from other evolutional maps. Similarly, 1DSP has its unique traits and benefits which will be analysed through the following trajectory and sensitivity analysis. This will further analyse the performance and utopianism of the proposed algorithm.

3.1.1 Analysis of trajectory: Any dynamic system's chaotic behaviour can be analysed using the trajectory of its time series. The randomness of the algorithm can also be obtained from the amount of space that the trajectory occupies. Theoretically, it has been proved that any chaotic system cannot have a closed trajectory and applicable to our algorithm also. To analyse this, we take the bifurcation diagram and the 3D image of the same. It can be noted from the bifurcation diagrams (figures 1 and 2) that the sine map and logistic map have a chaotic behaviour only when their respective control parameters (γ and η) approach 1. But in an1DSP, the chaotic behaviour remains even when r>3 This shows the wide range chaotic behaviour of the algorithm. Following this, in the second test, we consider3D phase plan of the sine, logistic, and 1DSP for various parameter values.

The sine map and logistic map have a closed trajectory from the above diagrams, whereas our proposed algorithm has an open trajectory. This proves the limited range of chaotic nature in conventional methods and an open range in 1DSP.

3.1.2 Sensitivity analysis: Sensitivity analysis is one of the most important for any encryption algorithm. It is used to measure the system's ability to return different values for any two inputs with slight differences. Sensitivity analysis is, in general checks the robustness of the system. We use the Lyapunov exponent (LE) to perform this analysis.

$$LE = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \mid h'(x_i) \mid$$

The larger the value of LE, more significant is the chaotic nature. We note that, unlike the logistic map and sine map, the 1-DSL has a wide parameter range where LE is positive.

In addition, for r>3, LE is purely positive, implying a persistent chaotic behaviour.. In addition to LE, based on the number of iterations, we test the sensitivity of the 1-DSP with respect to its initial values. With a minimal value difference, we pick two initial values.

4. 1D COMBINED SINE-LOGISTIC BASED ENCRYPTION

The above proposed one-dimensional logistic-sine powered chaotic map is used in an encryption scheme to create secret keys and add sequences to plain image. It is then used to create 2 chaotic sequences which are then used in the confusion and diffusion processes. The confusion process uses pixel scrambling in row by row and column by column manner while the diffusion process includes bit-level XOR operation.

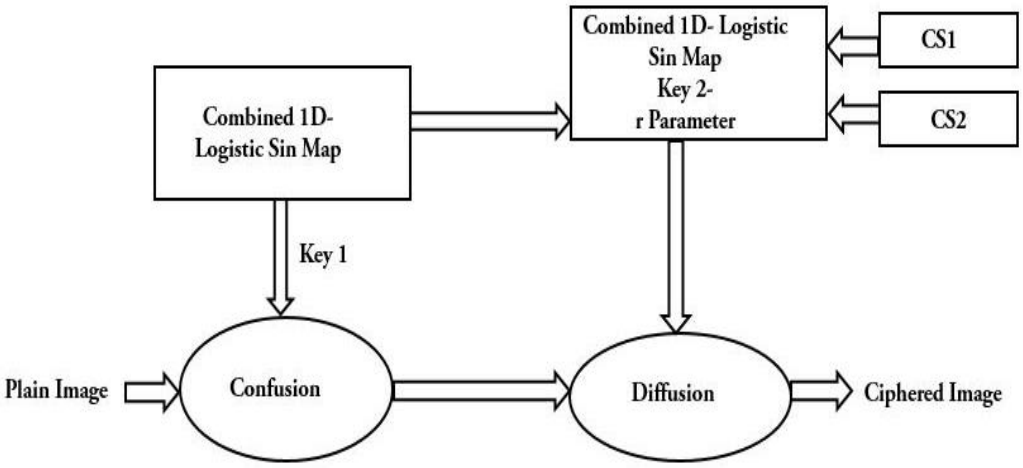


Fig. 4.1: Block diagram of 1D combined Sine-Logistic Map encryption Algorithm

4.1 Secret Key Generation

Key space refers to the set of all a key's permutations possible. The keyspace is typically designed to be large enough to make such a search impossible, to avoid an attack to locate the key used to encrypt a message. Any image encryption scheme can resist brute force attack when the algorithm's keyspace is greater than 2^{100}. 1DSL is proved to have a keyspace of 5×10^{164}.

4.2 Confusion and diffusion

The proposed algorithm is now used to create two keys with different control parameter values. One of the keys is used for confusion, and other is used for diffusion. Both keys vary by the parameter r. key1 has no r parameter whereas key2 has an r parameter of value 3.2. The key1 created with the combined Logistic and Sine map is used to confuse the plain image in a row-after-row and column-after-column process.

Confusion refers to making the relationship as complex and active as possible between the cypher text and the symmetric key; diffusion refers to dissipating the plain text statistical structure over the bulk of the cypher text. The concepts of uncertainty and diffusion consist of developing an encryption process.

The process of confusion can break the correlation between adjacent pixels. Data redundancy is likely to occur in any digital image due to the 8-bit representation of pixels. But with the confusion process, data redundancy can be reduced drastically. In this process, we apply pixel scrambling and value manipulation for each row from 1 to m followed by each column. To achieve this, we use two sequences key1, key2:

Key1:x(n+1) = x(n)*sin(1-x(n));

Key2: x(n+1) = r*x(n)*sin(1-x(n));

The Sequence key1 is used for row by row and column by column confusion whereas key2 is used for the respective diffusion. The below figure gives a detailed pictorial description of the confusion and diffusion process that has been implemented in this encryption scheme.

As we can see from the below diagram, two-pixel scrambling levels are applied for key used by bit level xor operation. The key is rotated in a clockwise manner twice. Following this, the sequence.

Key2 is bit XOR'ed with the result R2. The result R3 is the new row. A similar procedure is applied for the columns as well.

4.3 Using AWS to store the encrypted image

Despite saving data storage of large storage applications, Cloud depositories also offers high end security and accessibility to various authorised users at different locations. In this project, the Simple Storage Service(S3) of Amazon Cloud Services is used as an illustration of RTA with a LabView interface. Firstly, the user is supposed to have an AWS username and password to store or obtain data from AWS. Secondly, either a new or existing S3 bucket is used along with the Access key id and Secret Key to store the encrypted images as objects in the cloud. The access key id and secret key are <given> only to the statutory users Thirdly, to download images from the S3 bucket to system, users ought to enter the captcha. In addition to this, to obtain the original image from cipher image, the user should have the decryption key to boot. Thus, one can say that the usage of AWS hybrid cloud services along with the conventional encryption mechanism offers 4^0 authentications.

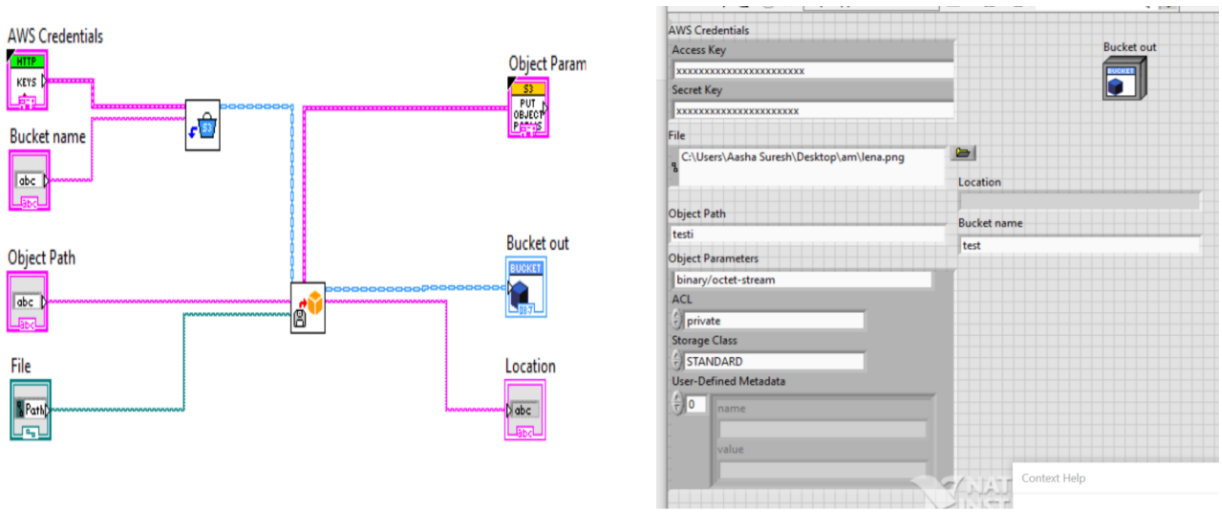


Fig 4.2 (a) shows the front panel of uploading data into the bucket/cloud and (b) shows the downloading of data from the bucket/cloud

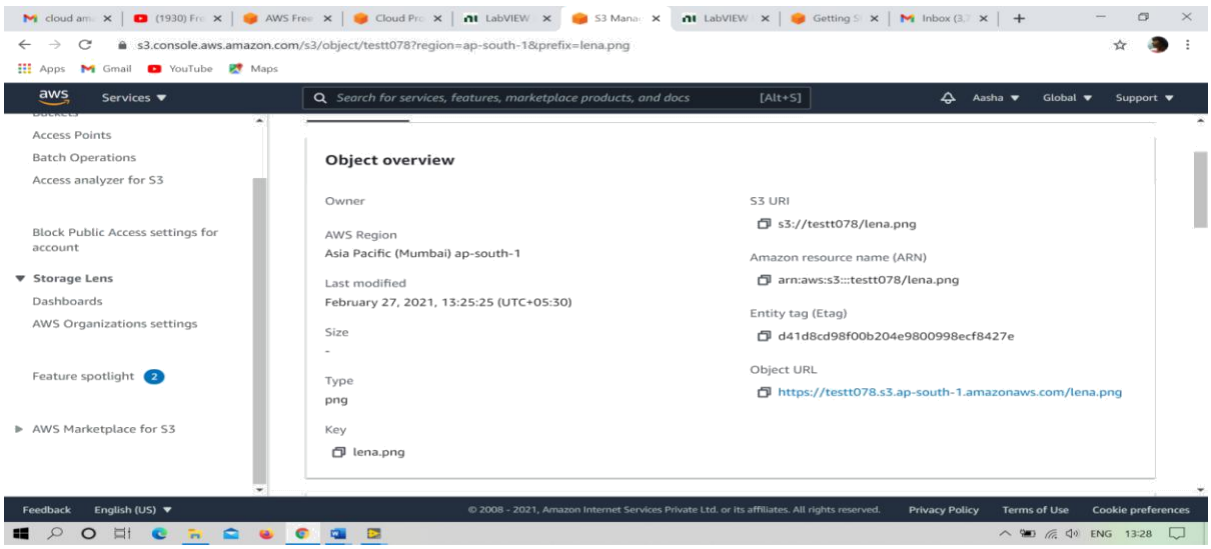


Fig 4.3 shows the encrypted image stored in AWS console.

5. ALGORITHM

In this project, we required stenographic image is obtained through the following 4 main For an image Im(m,n) and two chaotic sequences {*key1, key2*},

5.1 Pseudo Code

Shown below is the pseudo code of the algorithm:

1: **procedure** Row (*Im, key1* ,key2) _ Row phase

2: Input: Image Im of size (m,n), 2 chaotic sequences { *Sq*1 , *Sq*2 }

3: Output: *ImR*of size (m,n)

4: initiate *k* 1 = 1 ,*Ind*of size 3 and *R* 1 , *R* 2 , *R* 3 , *R* 4 of size n

5: **for** *i*= 1 to *m* **do**

6: *Ind*= *Sq*1 (*k* 1 :*k* 1 + 2) ; _ Start scrambling

7: *R* 1 = [*I m* (*i, I nd*(1) : −1 : 1) , *Im*(*i, end* : −1 : *Ind*(1) + 1)] ;

8: *R* 2 = [*R*1(*Ind*(2) : −1 : 1) , *R* 1(*end* : −1 : *Ind*(2) + 1)] ;

9: *R* 3 = [*R*2(*Ind*(3) : −1 : 1) , *R* 2(*end* : −1 : *Ind*(3) + 1)] ;

10: *R* 4 = *bitxor*(*R* 3 ,*Sq*2) ; _ Bitxor operation

11: *Sq*2 = *R* 4 ;

12: *ImR*(*i,* :) = *R* 4 ;

13: *k* 1 = *k* 1 + 3 ;

14: **end for**

15: **end procedure**

16: **procedure** Column (*ImR, Sq*3 , *Sq*4) _ Column phase

17: Input: Image ImR of size (m,n), 2 chaotic sequences { *Sq*3 , *Sq*4 }

18: Output: *ImC*of size (m,n)

19: initiate *k* 2 = 1 ,*Ind*of size 3 and *C* 1 , *C* 2 , *C* 3 , *C* 4 of size m

20: **for** *j* = 1 to *n***do**

21: *Ind*= *Sq*3 (*k* 2 :*k* 2 + 2) ; _ Start scrambling

22: *C*1 = [*I mR*(*I nd*(1) : −1 : 1 , *j*) , *ImR*(*end* : −1 : *Ind*(1) + 1 , *j*)] ;

23: *C*2 = [*C*1(*Ind*(2) : −1 : 1) , *C*1(*end* : −1 : *Ind*(2) + 1)] ;

24: *C*3 = [*C*2(*Ind*(3) : −1 : 1) , *C*2(*end* : −1 : *Ind*(3) + 1)] ;

25: *C*4 = *bitxor*(*C*3 , *Sq*4) ; _ Bitxor operation

26: *Sq*4 = *R* 4 ;

27: *ImC*(: , *j*) = *C*4 ; 28: *k* 2 = *k* 2 + 3 ;

29: **end for**

30: **end procedure**

6. SECURITY AND SIMULATION ANALYSIS

6.1 Simulation Analysis

Any encryption algorithm should be able to transform the original image into a ciphered image with no relation between them. As we can see from the plain and ciphered image histograms, there are no recognisable patterns. The decrypted image can be obtained by using a proper key. This algorithm has proved to be time-efficient than other encryption schemes.

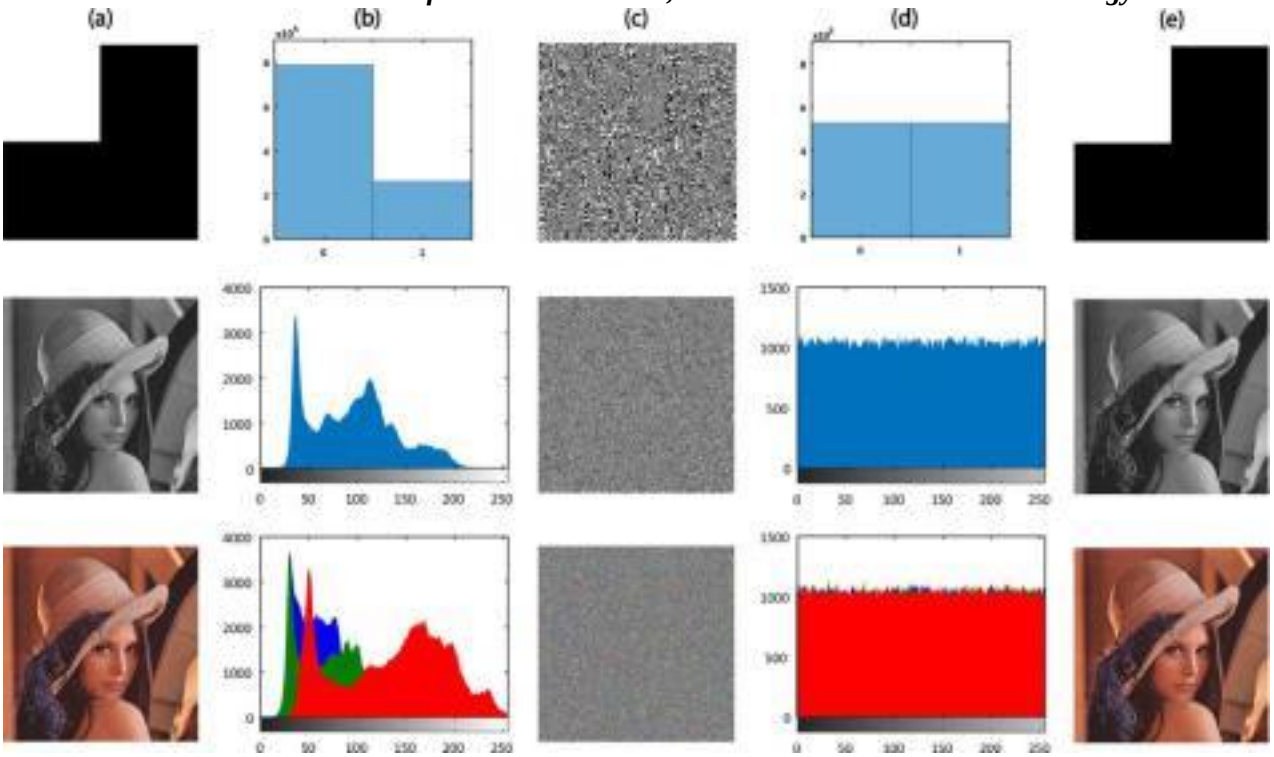


Fig. 6.1. Simulation results of 1-DSL-IE in the(a) original images; (b) histogram (c) encryption results (d) histogram of the ciphered images; (e) decrypted images.

6.2 Security Analysis

6.2.1. Correlation analysis

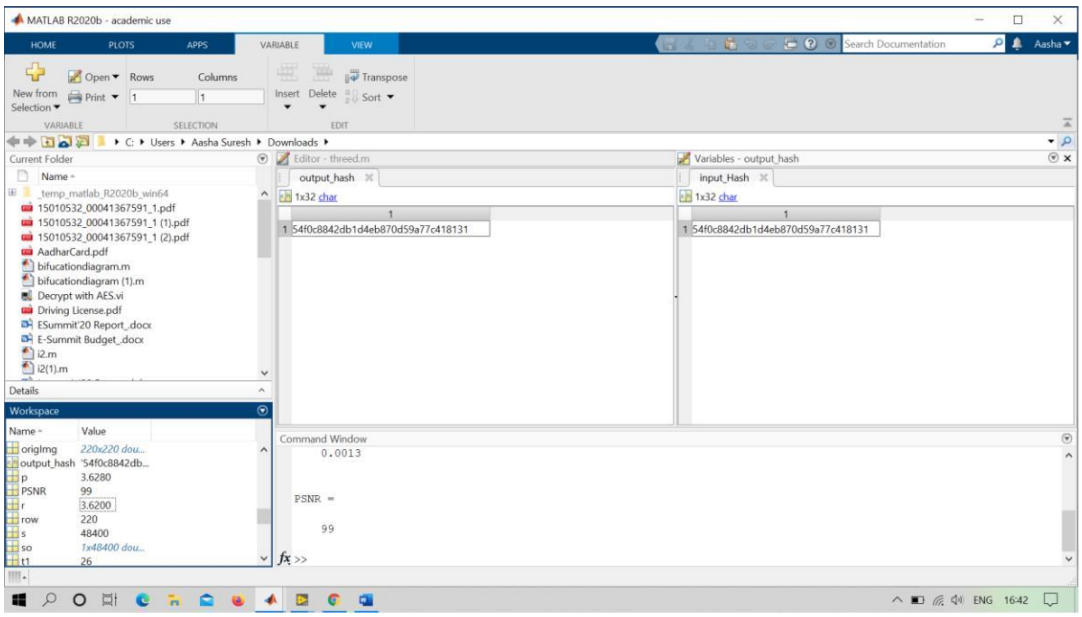
Correction Analysis is an observable method used to determine the intensity of the relation between two quantitative pixels. High correlation points out that the adjacent pixels are firmly related, whereas weak correlation means the pixels are hardly related. Usually, images have an influential association between neighbouring pixels. A good encryption algorithm is one which breaks this correlation. The results of correlation analysis:

The correlation coefficient of:
(a)Lena =-0.03
(b)Dog=0.0018

An ideal correlation coefficient lies between -1 to +1. Hence, it is observed that the encrypted image have weak correlation with adjacent pixels in all directions. Thus we can say that 1DSL-1E algorithm breaks the strong correlation.

6.2.2 Integrity

With all the computations completed, the integrity of the images should not be recompensed. The integrity test of this paper is effectuated using SHA256 algorithm which is one amongst the most secure cryptographic hash algorithms available. The figure *a and *b shows that the 32*8-bit hash values of input and output images are alike thus corroborating the integrity of the algorithm.



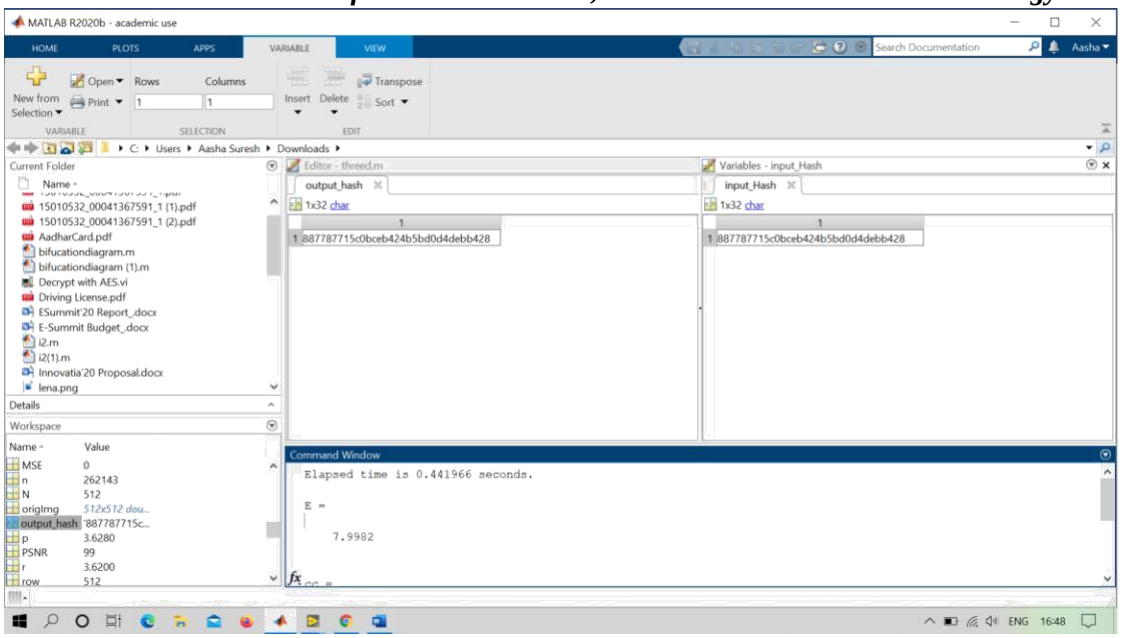


Fig 6.2: 256 bit hash values of the input and output images of (a) 256*256 lena image (b) 512*512 baboon image

6.2.3 Randomness analysis

In cryptography, the property of randomness is significant to avoid any pattern in the output image, to provide security against attacks, privacy and anonymity. To evaluate the proportion of randomness, we use Local Shannon Entropy (LSE). By considering images encrypted using various algorithms, we calculate the LSE. We can observe that many images from 1DSP-1E have the LSE test, which reiterates the fact that our algorithm offers elevated randomness.

6.2.4 Resistance against differential attacks

By evaluating the impact of any shift in the plain image on the encryption result, This Cryptanalysis finds the relationship between the plain image and its corresponding ciphered image that the attacker probably uses. The cryptanalyst uses statistical analysis to search the encrypted images for signs of non-randomness, figuring out the regions where the plain images differ. Any associated pixel should have a 50/50 chance of flipping; in areas where this is not accurate, the cryptanalyst searches. A clue to retrieving the key is some other underlying order. This is known as the differential attacks. Any encryption scheme to resist against these attacks must possess diffusion property. The property where any small variation in the plain image gives a varied output in the encrypted image. The Amount of Pixel Changing Rate (NPCR) and the Unified Average Modified Intensity (UACI) areused to test the image encryption system's diffusion properties.It is seen that all 1DSL-1E images clears the NPCR and UACI tests indicating it is an effective and secure algorithm against differential attacks.

6.2.5 Noise and data loss analysis

The encrypted image when transmitted, is subjected to various attacks. These attacks reduce the probability of obtaining 100% perfect image during decryption. These attacks can even go to an extent where we cannot recognise the recovered image. A good encryption scheme should minimise the effects of noise on an image while recovery. The encrypted images are exposed to several noise effects and the results of recovery of the same is observed. It can be observed that all decryption results are legibly visible. As such, 1DSL provides good resistance against the noise and data loss.

7. RESULTS AND DISCUSSIONS

This exploratory examination is implemented in Matlab, with a cover image of size 256 × 256. The robustness of the method is examined with the respective images' histogram analysis.

7.1 Output

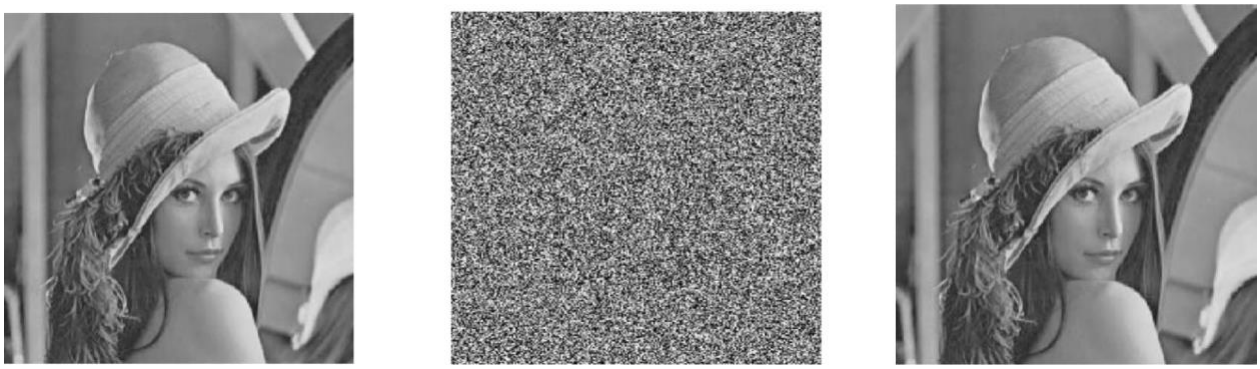


Fig 7.1 Plain, encrypted and decrypted images of Lena

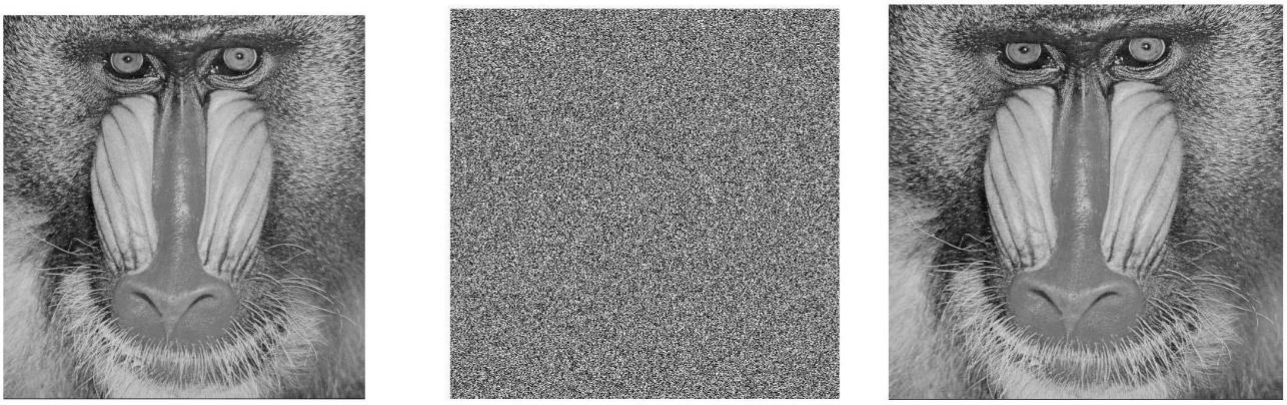


Fig 7.2 Plain, encrypted and decrypted images of Babboon

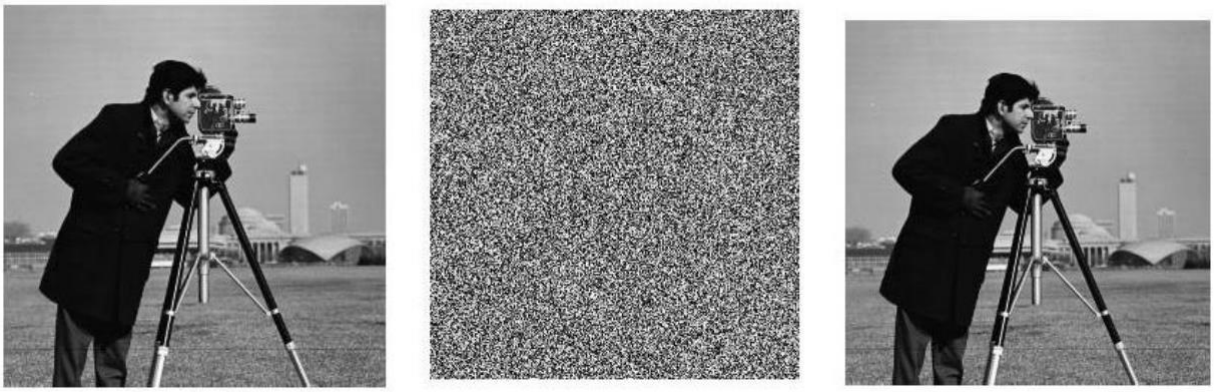


Fig 7.3 Plain, encrypted and decrypted images of Cameraman

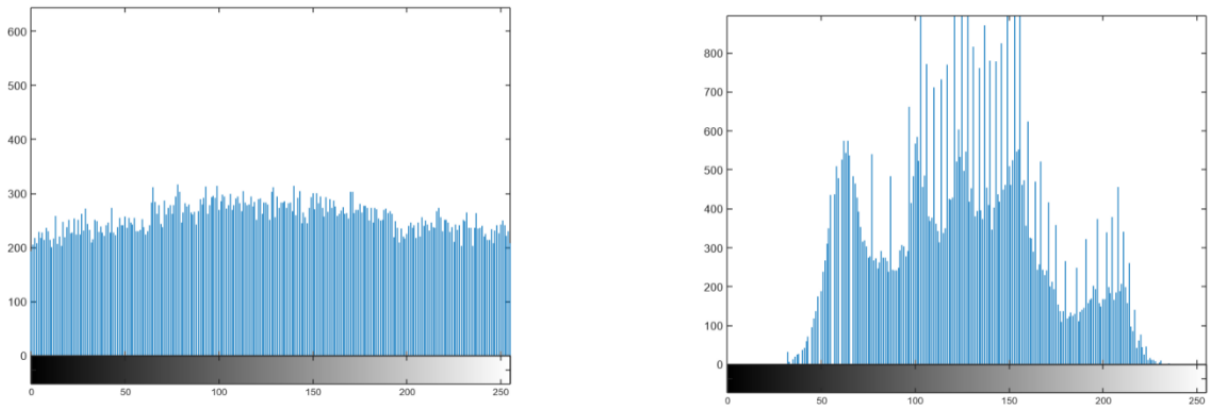


Fig 7.4 Histograms of plain and encrypted image of Lena

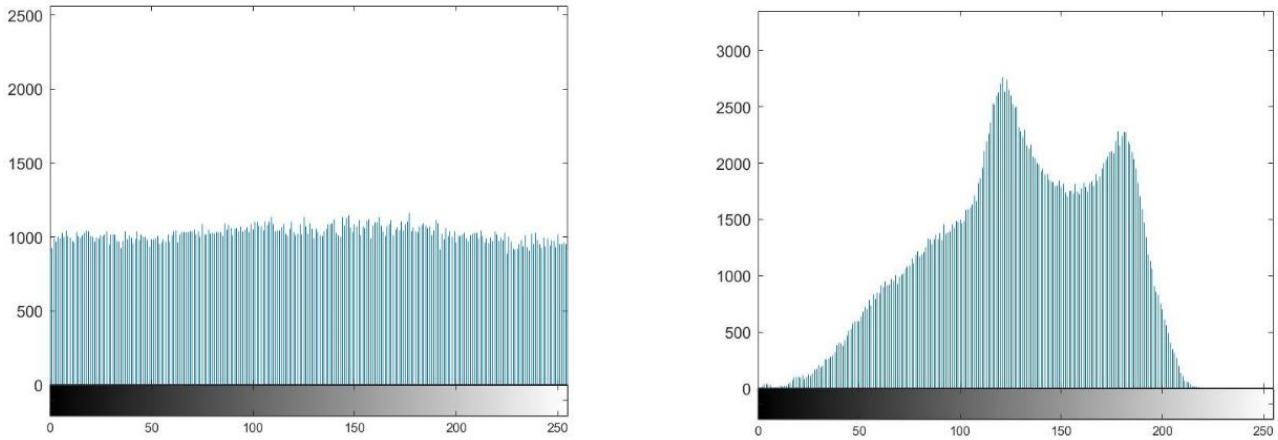


Fig 7.5 Histograms of plain and encrypted image of Baboon

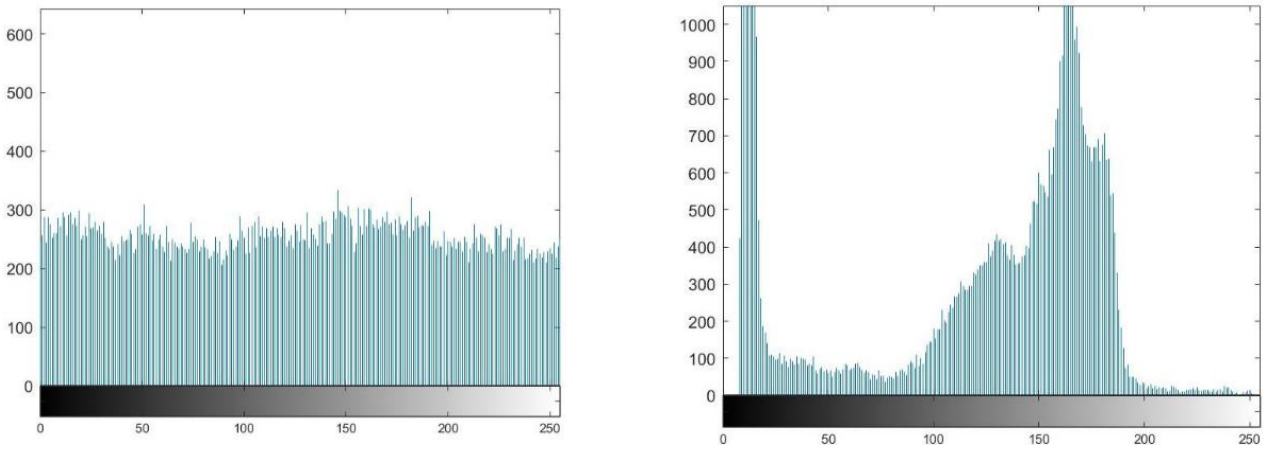


Fig 7.6 Histograms of plain and encrypted image of Cameraman

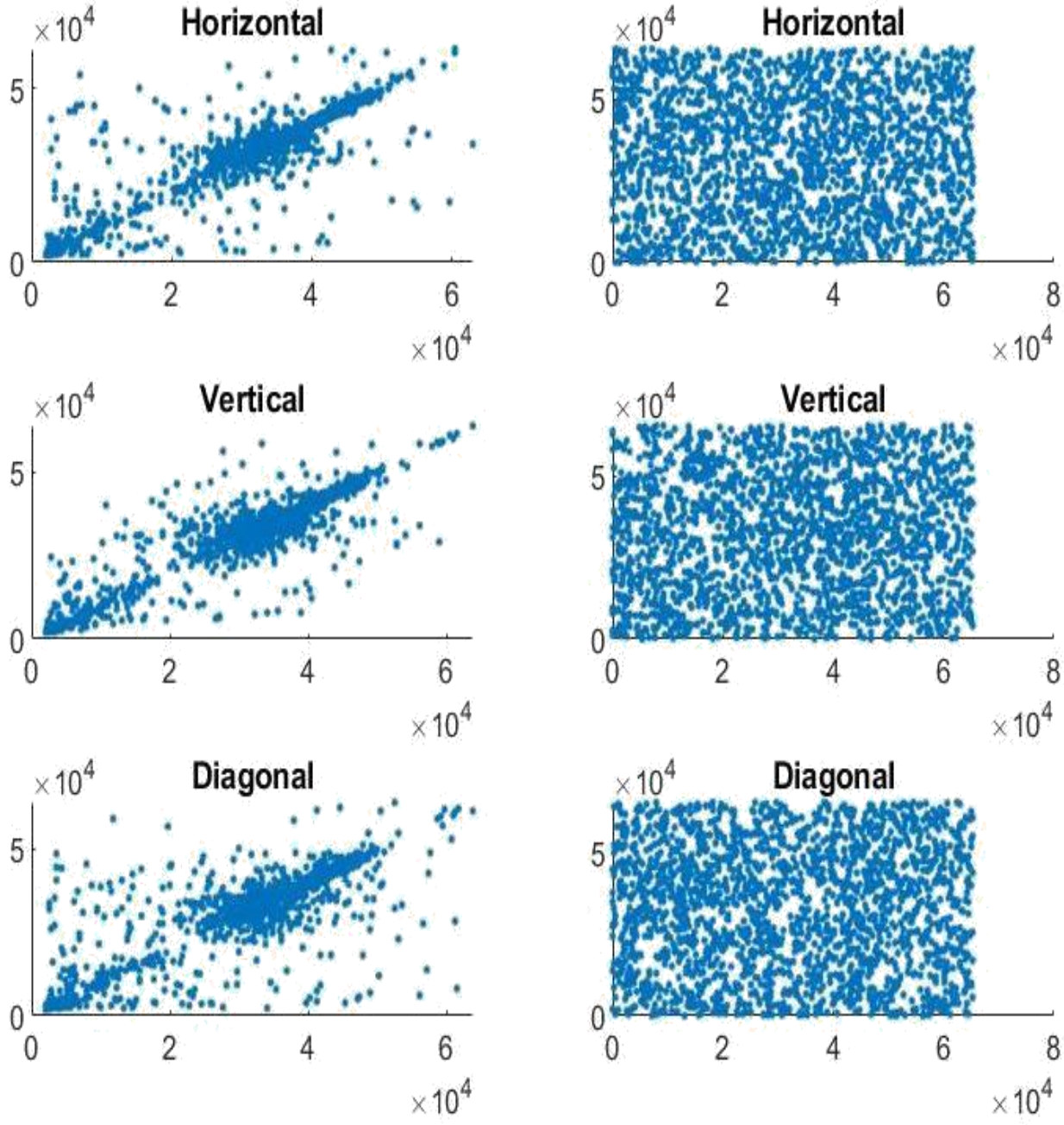


Fig 7.7 Correlation of pixels in (a) plain image (b) Encrypted image in the horizontal , vertical and diagonal directions of Lena.

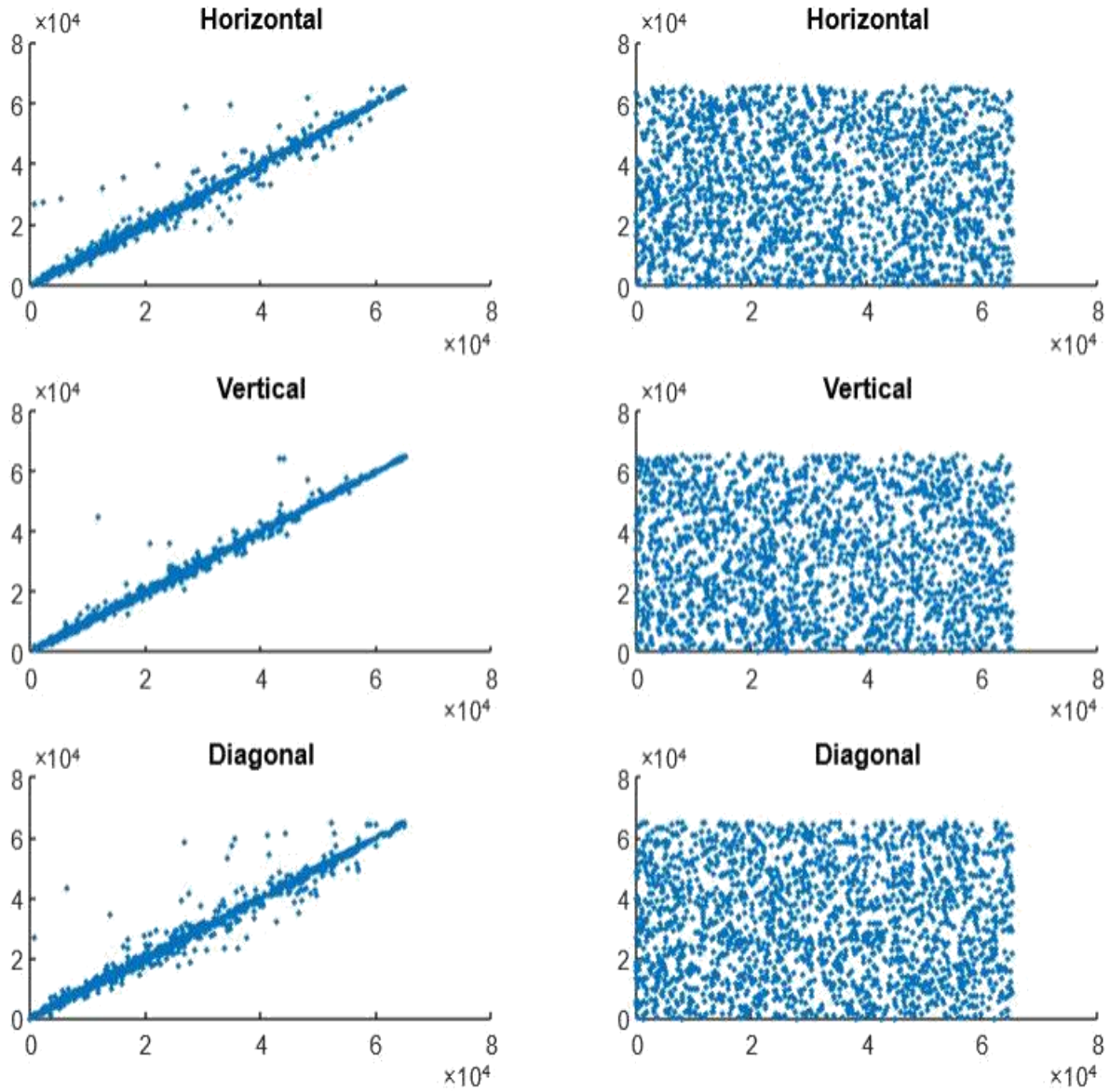
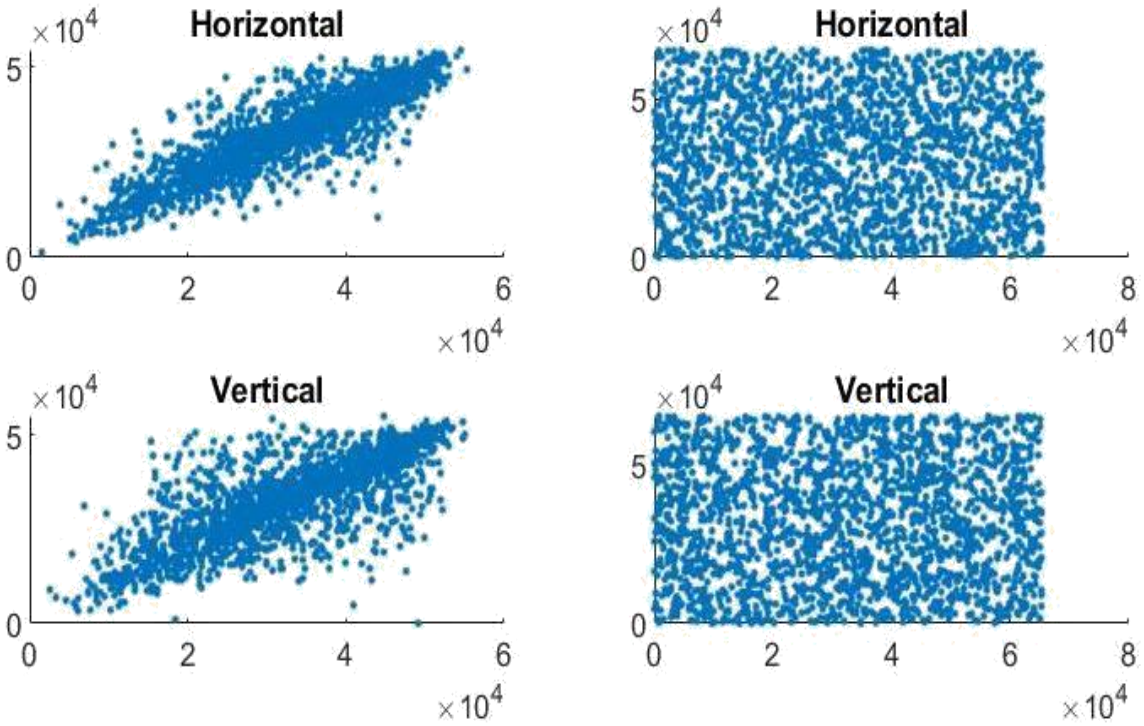


Fig 7.8 Correlation of pixels in (a) plain image (b) Encrypted image in the horizontal , vertical and diagonal directions of Baboon.



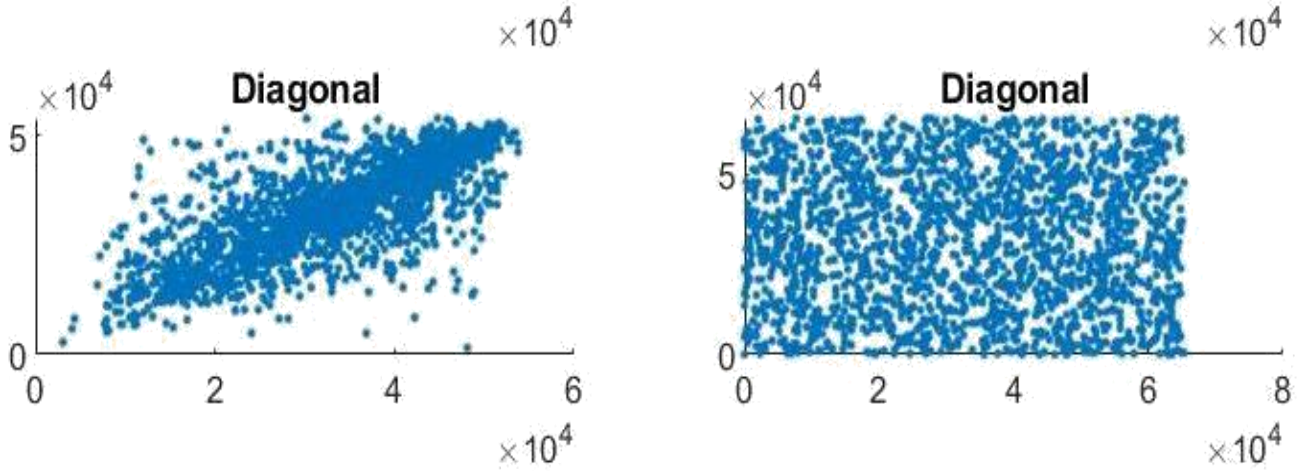


Fig 7.9 Correlation of pixels in (a) plain image (b) Encrypted image in the horizontal , vertical and diagonal directions of Cameraman.

8. CONCLUSION

In this project, we presented a new chaotic map. It is obtained from the combination of sine map and logistic map by using one variable parameter. The robustness and chaotic range of this map is verified using the trajectory and sensitivity analysis. We further use this map to implement in a new image encryption scheme where the security is guaranteed to its maximum. Using 1DSP, secret keys are created which are used in the image encryption process. The security and simulation analysis of the algorithm proves the effectiveness of the algorithm.

9. REFERENCES

[1] F. Özkaynak, Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals, IEEE, 2017. 2017 International Conference on Computer Science and Engineering (UBMK), 621–624.
[2] M.T. Rosenstein , J.J. Collins , C.J. De Luca , A practical method for calculating largest lyapunov exponents from small data sets, Phys. D 65 (1993) 117–134.
[3] B. Schneier , Data encryption standard (des), in: Applied Cryptography, second ed., 2015, pp. 265–301.
[4] C.E. Shannon , A mathematical theory of communication, Bell Syst. Tech. J. 27 (1948) 379– 423.
[5] M. Asgari-Chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," Signal Process., vol. 157, pp. 1_13, Apr. 2019.
[6] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," Inf. Sci., vol. 507, pp. 16_36, Jan. 2020.
[7] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurcation Chaos, vol. 08, no. 06, pp. 1259_1284, Jun. 1998.

