

CHAOS BASED CRYPTOGRAPHY AND RECTANGULAR SHAPE BASED STEGANOGRAPHY TECHNIQUE USING LSB

Aiswarya.S¹ and Gomathi.R²

Department of ECE,

¹University College of Engineering-Dindigul, Tamilnadu, India.

²Anna University Regional Campus-Coimbatore, Tamilnadu,India

¹aiswaryavinoth@gmail.com ²gomathiaudece@gmail.com

ABSTRACT

Multimedia means text, image, audio or video file and transferring multimedia files through the internet are noticeable one. Multimedia securing techniques are additionally used to protect the file. Securing multimedia image file is difficult by using formal encryption techniques such as AES, RSA because of high correlation between pixels. For encryption, chaotic map with XOR function is used and to provide double protection, steganography technique is used. After the encryption, encrypted image is hidden into the cover image file using LSB-steganography. For that, from the cover image, the rectangular positioned pixel values are selected and the encrypted image values are hidden into the selected rectangular positioned pixel locations of the cover file. Embedded image i.e., stego image is transmitted to the recipient through the internet and the reversal process is carried over at the retriever side. The performance of this proposed algorithm is evaluated by using many numerical calculations such as NPCR, UACI and PSNR. Correlation analysis is also performed and the values of the secret image is compared with the chaotic map encrypted image. The obtained average NPCR, UACI and PSNR values are 99.8004%, 37.6773% and 46.41 respectively. These values are compared with existing methods. After retrieving the secret image, the PSNR value is calculated and is high as 46.41dB. From the analysis, it is clear that the chaotic map based image cryptography and steganography method provides more security and robustness in the wireless secret image transmission.

Keywords: Chaotic Encryption, Histogram, LSB, Steganography.

1.0 INTRODUCTION

Information is more important and is wealth in real time applications such as banking, military field, telemedicine [2] etc., In real time applications, the information must be kept secret and transferred from one to another should be need more secrecy. For that purpose, data hiding techniques are designed to provide security against intruders and the classifications are Cryptography, steganography & watermarking which protects the secret data in an enhanced manner. Crypto techniques convert the secret data into the unreadable data by using the mathematical operations. Steganography embed the secret data into the other file that is known as cover.

Combinations of Crypto and Stegano techniques provide more security and double protection to the secret data [10]. Initially, cryptography technique is used to alter the secret data into unreadable form. Text, image or audio file can be encrypted using cryptography technique. AES, DES, RSA are example of cryptography techniques for encrypting text [2]. Image encryption is different from text encrypting [5], [9]. Text cryptography techniques are inappropriate for image encryption because of pixel correlation in an image [3]. Chaotic based techniques are used for secret image data encryption. The cryptography technique provides first level of security to the secret data.

The encrypted data is look like a scrambled data so it is visible to the intruder that is some data is hidden into it. It is easily vulnerable to attacks by the intruders. So, the encrypted data is hidden into another file to improve the security to the secret data. For that purpose, steganography technique is used in which the encrypted data is hidden into the cover file using steganography technique which hides the presence of data and it gives the additional protection to the secret data. Image, audio or video [10] can be used as a cover file. Based on the embedding domain, the steganography is divided into spatial domain and frequency domain steganography. In time domain steganography, the cover file pixel values are directly altered by the secret data [9]. LSB, MSB, PVD technique are examples of time domain steganography technique. In frequency domain steganography, transforms are used to convert the cover file into frequency domain then the spatial domain techniques are preferred to implant the secret data in the frequency coefficients. DCT, DWT are examples of frequency domain steganography. In image steganography technique, the size of cover image must be greater than that of secret image.

In the proposed work, image is chosen as an input data which should be kept secret and is encrypted with the help of chaotic encryption. The encrypted image is hidden into the cover image file using LSB steganography technique. To improve the complexity of data hiding, the rectangular pixel values are chosen from the cover image

and in that the encrypted pixels are hidden. Finally, the stego image is generated which contains the encrypted image pixels. This type of communication provides enhanced security to the input image.

The paper arrangement is summarized as follows: the existing works correlated to crypto-stegano methods are discussed in Section 2. The proposed work is presented in Section 3. In Section 4, the performance metrics are analysed. Section 5 describes the results and discussions. In section 6, conclusion and future work is discussed.

2.0 EXISTING WORK

Veena et al., [13] discussed a different chaotic techniques for image encryption and decryption. Nine different techniques are analyzed related to chaotic method and chaotic image encryption is the best choice for encrypting the image. Due to high correlation between pixels, AES [6], and RSA techniques are not used for encrypting in an image.

Hossain et al., [9] proposed a technique of 3D chaotic image encryption by using position permutation followed by value transformation techniques. For encrypting image, 3D chaotic maps are used. This paper provides better security and enhanced NPCR and UACI values. But, the encrypted image is directly transmitted to the recipient without embedding the secret encrypted image into specific cover file using steganography technique which made the proposed technique more vulnerable to attackers.

Bandekar et al., [4] introduced a process of embedding text or image data into the image cover file using LSB. Initially, both the secret and cover files are converted into equivalent binary values. Using LSB method, in a binary cover image, the binary secret data is hidden. Then, the stego image is given as input to AES encryption process to encrypt the stego image. In this method, final encrypted image is vulnerable to attackers because of its visibility in the encrypted image; and there is no encryption technique for the secret text.

Qian [12] et al., proposed a technique of encrypting a color image using three dimensional chaotic map. For diffusion process, chaotic logistic map is used and for confusion, chaotic cat map is used. In this, encryption process is time consuming because of different chaotic maps. Also, no further data processing technique is used to secure the cipher image.

In order to reduce the above problems, in the planned process, the input secret image is initially encrypted by using the chaotic encryption with XOR function. It provides the first level security to the input image. After encryption, encrypted image is look like a blurred image so the intruder is easily understood that there is a secret image inside the blurred image. Because of that, there is a need of additional security to the encrypted image. For that, the rectangular pixels of the cover image is calculated and the pixels of the encrypted image is embedded by using LSB steganography technique. Crypto-stegano techniques provide an enhanced security that is double security to the input secret image which should be protected from the unwanted persons during wireless transmission.

3.0 PROPOSED METHOD

Chaos based cryptographic algorithm [7] is used in an image encryption. Chaos means confusion or the state of randomness. The random nature of chaos is used for an effective image encryption by using confusion and diffusion process. In chaotic based algorithm, random sequence of numbers is produced and they are spread into the source image for producing an encrypted image. Chaotic image encryption is more sensitive to the initial condition and if there is a small change then it will produce greater changes in its output.

Chaotic map is a map of randomized number and is generated based on key values. It is used to mix up the image pixels for confusion process. Single bit variation in chaotic map affects the whole image. Chaotic image encryption is classified into 1D chaotic image encryption [8] and high dimensional chaotic image encryption [5]. In 1D technique, cosine transform based map, tent map and logistic map are used. 2D logistic map, 2D collapse map and 2 D sine transform based maps are used in 2D image encryption.

Chaotic image encryption process is similar to symmetrical plain text encryption technique that is sender and receiver should use the same key then only encrypting and decrypting process will be succeed. In encryption, the key values are more important because based on the key, the images is encrypted perfectly. Key values are of

two types. They are predefined key values and randomized key values. If the key is predefined by the sender and the same key is utilized in the receiver side then it is called as predefined key value. If the Pseudo Random Number Generator (PRNG) is used to produce the key value, then it is referred to as randomized key value. Based on key values, chaotic maps are varied. So that the key values should be properly chosen to encrypt and decrypt the image securely.

Chaotic image encryption process consists of two steps namely (i) pixel scrambling or confusion [1] and (ii) pixel value substitution process or diffusion. Confusion is a process of changing the pixel position without changing its value. It is known as permutation also. Diffusion changes the entire values of pixel in an image. Both the confusion and diffusion processes are based on key values and these processes should be carried out until all pixel values in an image are changed. Fig. 1 shows the chaotic image encryption process with XOR operation.

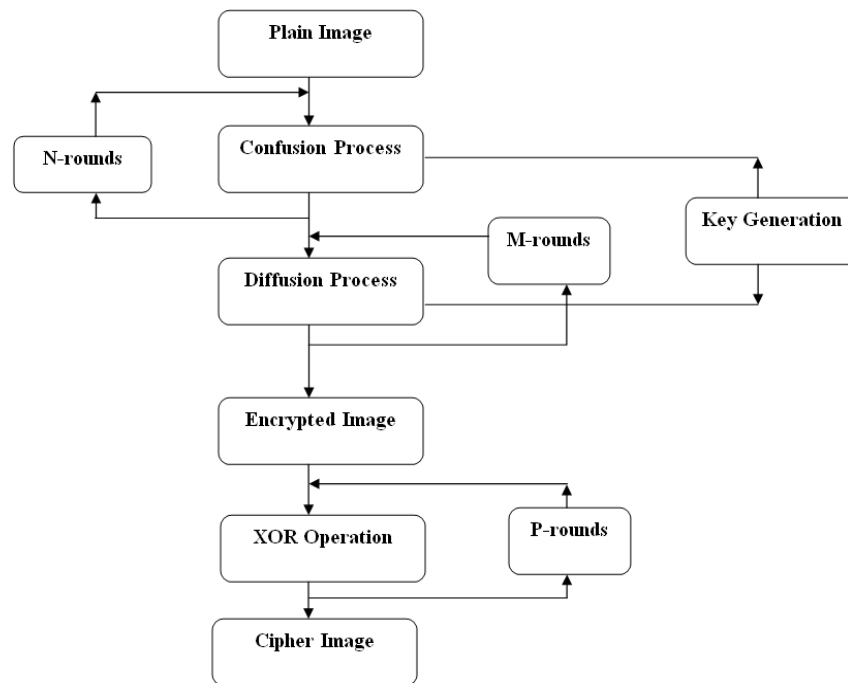


Fig. 1: Chaotic image encryption

The test input image known as plain image is suitably chosen for encryption. The plain image is subjected with confusion process for ‘N’ rounds until all pixels in an image are altered. After ‘N’ rounds, the confused image is subjected with diffusion process for ‘M’ rounds until the pixel values are changed. Both confusion and diffusion processes are based on key values. Key is generated by using randomized key generation method. Based on key values, the logistic map is designed and confusion and diffusion processes are carried over. After that, the encrypted image is given to the XOR operation for additional protection. In this, encrypted image pixels are XORed with the predefined binary value until all pixels are altered that is upto P rounds. For example, three bit binary representation i.e., 000 to 111 is used here. From that, a single binary value that is 001 is selected. But, in an encrypted image, each pixel has 8 bits representation so that the input 3 bit binary value 001 is changed to 8 bit representation by adding redundancy bits in MSB position and now it becomes 00000001. Then it is XORed with encrypted image pixel value. Thus the cipher image is generated and is transferred to the receiver through the wireless medium. In this way, by using chaotic image encryption with XOR operation, the plain image is converted to unreadable cipher image and it provides double security to the secret image.

Steganography is known as embedding the secret data unknown to anyone in a cover file. LSB method is an easiest method for an efficient data embedding. It has a high embedding capacity. LSB is the minimum weighted bit. Due to the minimum weight, after embedding the secret data, the changes appeared in cover file are invisible to human eye. Single bit or multibit LSB embedding is possible. In single bit embedding, the least 1 bit value is altered. In multibit embedding, depends upon the bit value for example 2 bits means, least 2 bit values are altered by the secret message bit. In the proposed work, single bit LSB technique is used. LSB method can be

performed either on entire image or on selected pixels of an image. In the proposed work, rectangular shape is defined and pixels corresponding to the rectangular shape are utilized for LSB embedding. After that, the cover image is known as the stego image and it is send to the recipient using wireless medium. Fig. 2 shows the planned work flow diagram.

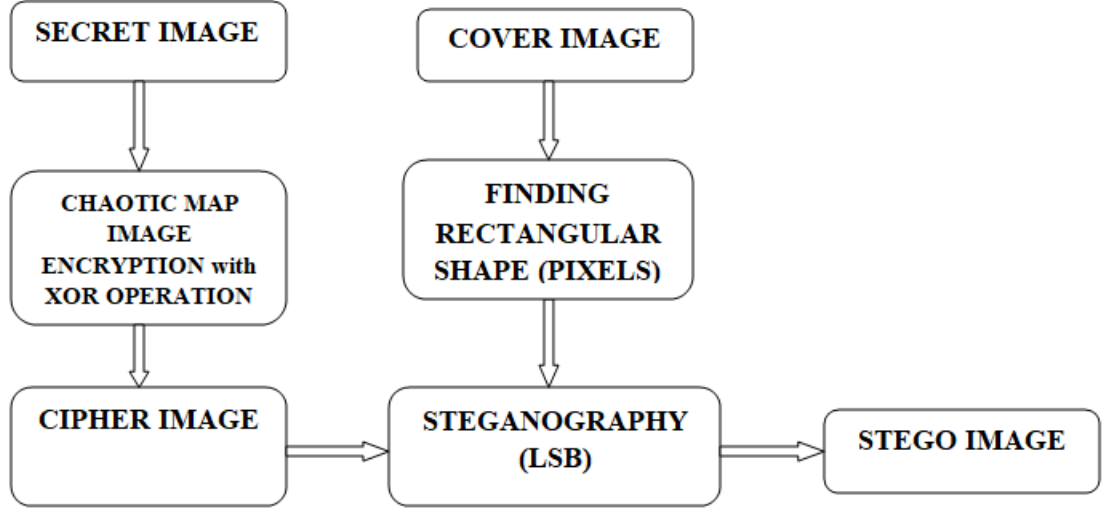


Fig.2: Planned work flow diagram

From the received stego image, the encrypted image pixel values are retrieved by using reversal LSB technique on the rectangular positioned pixels and the encrypted image is obtained. Then, using the XOR operation and the right key value for chaotic map, the original secret image is retrieved at the receiver side. The proposed method provides double protection to the secret image by using both cryptography and steganography techniques together.

4.0 PERFORMANCE METRICS

4.1 Performance Evaluation of Chaotic Map Based Encryption

4.1.1 Sensitivity Analysis

In key based chaotic map encryption, randomized key generation method is used to produce key. For sensitivity measure, Number of Pixels Changing Rate (NPCR) and Unified Average Changing Intensity (UACI) are used. They are described as follows,

$$NPCR = \frac{\sum_{k,l} D(k,l)}{A \times B} \times 100\% \quad (1)$$

$$UACI = \frac{1}{A \times B} \sum_{k,l} \frac{|E_1(k,l) - E_2(k,l)|}{255} \times 100\% \quad (2)$$

Where

$$D(k,l) = 0 \quad \text{if } E_1(k,l) = E_2(k,l)$$

$$= 1 \quad \text{Otherwise}$$

A and B are image dimensions. $E_1(k,l)$ is the encrypted image and $E_2(k,l)$ represents the input image. In Table 1, NPCR and UACI for different input images are tabulated. 99.8004% and 37.6773% are the average values of NPCR and UACI are correspondingly.

Table 1: Sensitivity analysis for sample input images

Sample Input Images	NPCR (%)	UACI (%)
Lena	99.7988	28.2563
Pepper	99.7936	44.7623
Deblur	99.7761	33.9024
House	99.8335	43.7881
Average	99.8004	37.6773

In Table 2, NPCR and UACI values are compared with previous works.

Table 2: NPCR and UACI comparison with existing works

Methodologies Used	NPCR (%)	UACI (%)
Ref. [1]	99.6094	33.4635
Ref. [7]	99.4932	22.4902
Ref. [8]	99.613	33.466
Ref. [9]	99.6	33.6
Ref. [12]	99.62	33.52
Proposed Work	99.8004	37.6773

NPCR and UACI values are improved in the projected method compared with existing methods is noted from the above table.

4.1.2 Encryption Time Analysis

Chaotic map with XOR operation consumes less time compared with existing techniques. Table 3 compares the encryption time of the projected method with existing methods.

Table 3: Analysis of encryption time for “Lena” (256X256) image

Image	Proposed Method	Ref. [8]	Ref. [12]	Ref. [14]	Ref. [15]	Ref. [16]
Lena (256X256)	0.065575 s	0.310429s	0.85s	1.1168s	1.25s	1.112s

4.1.3 Correlation Analysis

Correlation indicates the connection between neighboring pixels [8]. Similar correlated pixels in images give more information. Plain image have highly correlated neighboring pixels in horizontal (H), vertical (V) and diagonal (D) directions. Reducing the similarity between the neighboring pixels (i.e.,) correlation reduction is the purpose of image encryption. It is defined by,

$$r_{kl} = \frac{Cov(k,l)}{\sqrt{D(k)}\sqrt{D(l)}} \quad (3)$$

Where,

$$Cov(k,l) = \frac{1}{M} \sum_{x=1}^M (x_x - E(k))(y_x - E(l)) \quad (4)$$

$$E(k) = \frac{1}{M} \sum_{x=1}^M k_x \quad (5)$$

and

$$D(k) = \frac{1}{M} \sum_{x=1}^M (k_x - E(k))^2 \quad (6)$$

Table 4 shows the computed correlation coefficient values for different input images and its resultant cipher images. Correlation coefficient values of both secret and encrypted image along the H, V and D directions are shown in Table 5. Correlation values of proposed work and existing methods along H, V and D directions for both secret image and an encrypted image of test input 'Lena' is compared in Table 6.

From the Table 4, Table 5 and Table 6, it is predicted that the secret image that is original test input image correlation is closer to 1. At the same time, the cipher image pixels have the correlation is closer to zero or negative. This indicates that the reduced correlation between the neighboring pixel values i.e., in the image, pixel values are uniformly distributed. So that, the proposed method withstands with correlation coefficient attack.

Table 4: Correlation coefficient value for secret image and cipher image

Images	Lena	Pepper	Deblur	House
Secret Image	0.9436	0.9368	0.9838	0.9517
Cipher Image	-0.0233	0.0304	-0.0049	0.0273

Table 5: Correlation coefficient value for both secret and cipher image along H, V and D directions

Images	Secret Image			Cipher Image		
	H	V	D	H	V	D
Lena	0.9421	0.9710	0.9176	0.0028	0.0038	0.0048
Pepper	0.9502	0.9518	0.9084	-0.0015	-0.0010	3.8374e-04
Deblur	0.9901	0.9847	0.9767	0.0056	0.0087	-0.0051
House	0.9688	0.9529	0.9335	-6.2662e-04	-9.7306e-04	-0.0029

Table 6: Evaluation of correlation values of Lena image and compared with existing methods

Images	Secret Image			Encrypted Image		
	H	V	D	H	V	D
Projected Work	0.9421	0.9710	0.9176	0.0028	0.0038	0.0048
Ref.[8]	0.9700	0.9409	-	-0.0043	0.0014	-
Ref.[11]	0.9893	0.9798	0.9686	-0.0012	-0.0015	-0.0012

4.2 Performance Evaluation of LSB-Steganography after Embedding and Reconstruction

4.2.1. Noise Attack Analysis

MSE and PSNR are utilized to analyze the effect of noise on the recovered images. MSE is defined as the average of the squared error. The ratio between signal power to noise power is known as the PSNR. Error is defined by,

$$Error(E) = \sum_{a=0}^{U-1} \sum_{b=0}^{V-1} [I_R(a,b) - I_O(a,b)] \quad (7)$$

$$MSE = \frac{(E)^2}{M * N} \quad (8)$$

$$PSNR = 10 \log_{10} \frac{(255)^2}{MSE} \quad (9)$$

I_O and I_R denote the original image (test input 'Lena') and the recovered image (Decrypted image). U and V are defined as a total rows and columns in an image.

Table 7 shows the sample input images and their corresponding MSE and PSNR values. The average PSNR value of the proposed method is 46.419575.

Table 7: PSNR values for sample input images

Images	MSE	PSNR (dB)
Lena	0.0715	46.8371
Pepper	0.0721	46.4804
Deblur	0.0740	46.1398
House	0.0734	46.2210
Average PSNR		46.419575

Table 8 shows the overall analysis of the proposed work. From the above analysis, it is shown that the projected method provides improved protection to the secret image using double encryption process. The encryption time is minimum compared with existing techniques. For the different input images and cipher images along H, V and D directions, correlation values are calculated. From the calculated values, it is observed that the reduced correlation between pixels after encryption. NPCR and UACI values are also calculated and that are better compared with other techniques. After encryption, embedding is carried over. The recipient receives the embedded image and the reversal process is done to get the input image successfully. For the retrieved image, PSNR value is calculated to measure the performance. The computed PSNR values indicate that the projected method provides improved security and withstands against many attacks.

Table 8: Investigation of the proposed model

Images	NPCR %	UACI %	Enc Time(Sec)	Correlation Coefficients			PSNR (dB)
				Horizontal	Vertical	Diagonal	
Lena	99.7988	28.2563	0.065575	0.0028	0.0038	0.0048	46.8371
Pepper	99.7936	44.7623	0.037699	-0.0015	-0.0010	3.8374e-04	46.4804
Deblur	99.7761	33.9024	0.043819	0.0056	0.0087	-0.0051	46.1398
House	99.8335	43.7881	0.080693	-6.2662e-04	-9.7306e-04	-0.0029	46.2210

5.0 RESULTS AND DISCUSSIONS

In the projected method, secret image is encrypted using chaotic encryption with XOR operation and the encrypted image is hidden inside the pixels of chosen rectangular shape of the cover image using LSB technique. The proposed algorithm is applied on different source images. MATLAB-R 2018a software is used with Windows 10 Operating System and Intel core processor with 4GB RAM.

Fig. 3 shows the test input 'Lena' image and its resultant chaotic map encrypted image.



Fig . 3: (i) Lena image (ii) chaotic map encrypted Lena image

Fig. 4 shows the cover image and the embedded image i.e., which has the chaotic map encrypted image of 'Lena'.

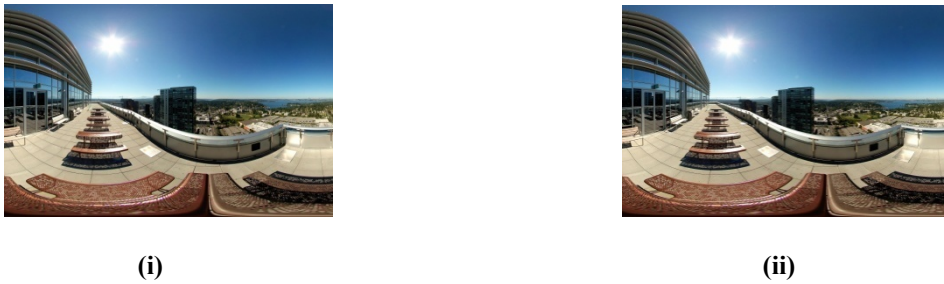

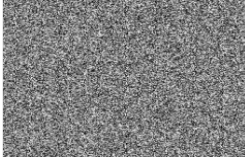


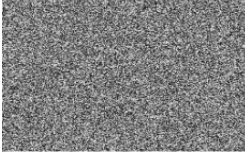


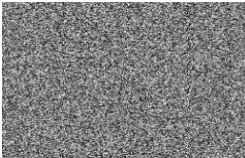
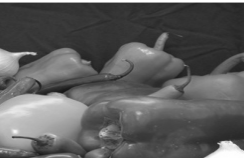

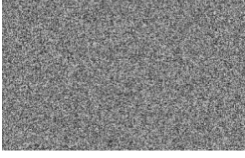



Fig.4: (i) Cover image (ii) stego image

After embedding, the embedded image is communicated to the beneficiary through wireless transmission. By doing the suitable steps in reverse order, the encrypted image is obtained from the stego image and it is decrypted using chaotic map and reversal XOR operation. Table 9 shows different set of input, Stego and decrypted images.

Table 9: Stego image and decrypted image of sample input images

Input Secret Images	Chaotic Map Encrypted Images	Decrypted Images
		
		
		
		

5.1 Performance Evaluation of Chaotic Map based Encryption

5.1.1 Histogram Analysis


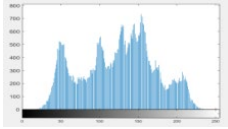
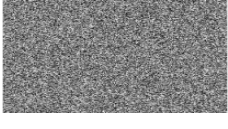
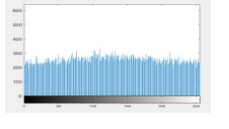

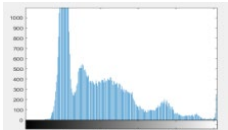
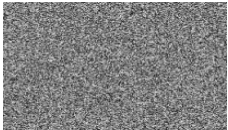
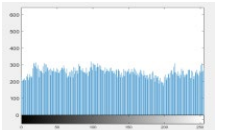

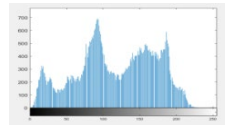
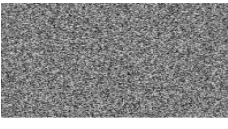
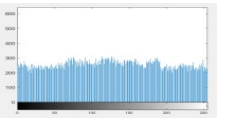

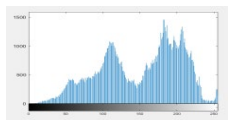
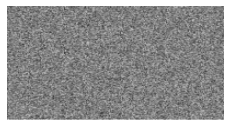
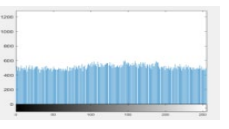
Graphical illustration of the pixel or data sharing over the image is known as histogram. The pixels distribution in the secret image and the encrypted image is different. In secret image, the pixel distribution is random and so the histogram image has different shapes of range of bars. For encrypted image, the distribution of data is uniform and in the histogram image, the shape of the bars is in uniform. Histograms of test 'lena' image and the corresponding chaotic map encrypted image is showed in Fig. 5.



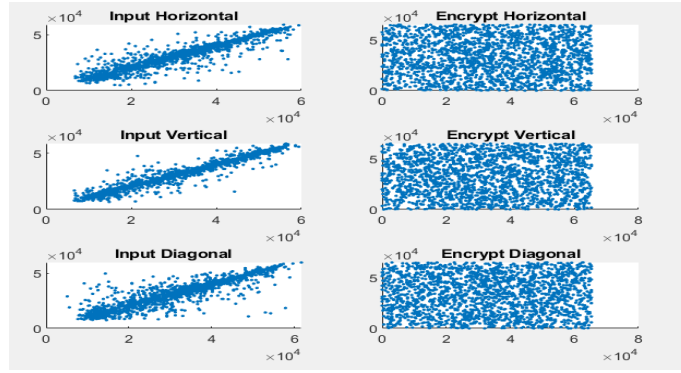
Fig.5: Plot of histograms (a) For test input 'Lena' (b) For chaotic map encrypted image

Table 10 shows different input images with their histograms and the corresponding encrypted images with their histograms. From Table 10, it is shown that the input image histograms are in unusual shapes and the encrypted images histograms are in consistent shape. This indicates the uniform distribution of secret image pixel values. So that for intruders, from the histogram of an encrypted image, the secret image identification is difficult. So the proposed method survives in the statistical attack.

Table 10: Outputs of the proposed system

Test Input Secret Images	Histogram of Test Input Secret Images	Chaotic Map Encrypted Images	Histogram of Chaotic Map Encrypted Images
			
			
			
			

The correlation coefficients of both test input 'Lena' and the corresponding chaotic map encrypted image along H, V and D directions is shown in Fig.6. From Fig.6, it is noted that the correlation in an encrypted image is minimized and distributed over the entire image. Correlation analysis of different sample input images are tabulated in Table 11.


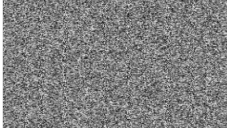
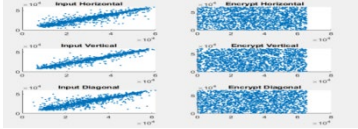

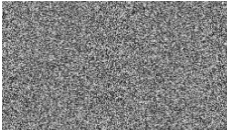
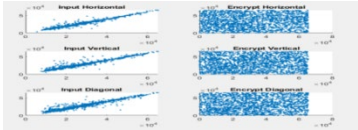

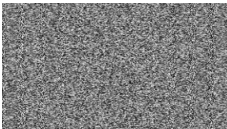
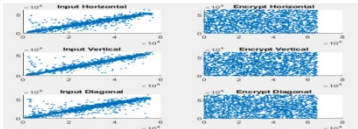

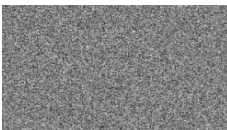
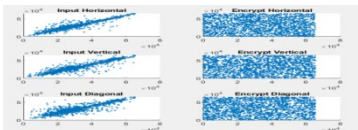


(a)

(b)

Fig.6: Plot of correlation analysis (a) For test input 'Lena' (b) For a chaotic map encrypted image

Table 11: Correlation analyses of the sample input images

Input Secret Images	Encrypted Cipher Images	Correlation Analysis
		
		
		
		

6.0 CONCLUSION & FUTURE WORK

In the proposed method, chaotic image encryption with XOR operation is used for encrypting the secret image. For providing additional security XOR operation is carried over. The cipher image is hidden into the cover image using LSB- steganography technique. The encrypted image pixel values are hidden into the pixels which are in rectangular shape of the cover image. The embedded image is transmitted to the recipient and reversal process is carried over in the receiver side and the secret input image is retrieved. NPCR, UACI, PSNR values are calculated and average values are 99.8004%, 37.6773% and 46.41dB respectively. Histogram and correlation between pixels are plotted and from that we observed that the proposed method break the correlation between neighboring pixels. Several analysis techniques were carried over to analyze the performance of the projected method. The investigated results indicate that the projected method provides high security and stability to the secret image against several attacks.

In future, video will be chosen as a cover file for secret image data transmission. Neural based video steganography technique will be used for steganography process.

7.0 SUBMISSION NOTICE

I ensure that the manuscript submitted to this journal has never been published before.

REFERENCES

- [1] Abbas.A.M, A. A. Alharbi and S. Ibrahim, "*A Novel Parallelizable Chaotic Image Encryption Scheme Based on Elliptic Curves*" in IEEE Access, vol. 9, pp. 54978-54991, 2021, doi: 10.1109/ACCESS.2021.3068931.
- [2] Aiswarya.S, Gomathi.R, "*Review on Cryptography and Steganography techniques in video* ", IEEE International Conference on Computational Intelligence and Computing Research 2018
- [3] Anuja.P & Song, Wen-Zhan. (2016), "*Encryption Algorithms for Color Images: A Brief Review of Recent Trends*", in International Journal of Advanced Computer Science and Applications. 7. 10.14569/IJACSA.2016.071001.
- [4] Bandekar, PP & Suguna, GC 2018, "*LSB Based Text and Image Steganography Using AES Algorithm*", in 3rdInternational Conference on Communication and Electronics Systems (ICES), pp. 782-788, doi: 10.1109/CESYS.2018.8724069.
- [5] Bu.Y, "*Overview of Image Encryption Based on Chaotic System*" 2021 2nd International Conference on Computing and Data Science (CDS), 2021, pp. 100-103, doi: 10.1109/CDS52072.2021.00023.
- [6] Dhande.K and R. Channe, "*A Brief Review on Reversible Data Hiding in Encrypted Image*" 2019 International Conference on Communication and Signal Processing (ICCSP), 2019, pp. 0135-0138, doi: 10.1109/ICCSP.2019.8697953.
- [7] Dsouza.C.A and K. Sonawane, "*Securing folder directory using image encryption by Chaos and Rijndael Algorithm*" 2021 International Conference on Communication information and Computing Technology (ICCICT), 2021, pp. 1-7, doi: 10.1109/ICCICT50803.2021.9510107.
- [8] Elghandour. A. N, A. M. Salah, Y. A. Elmasry and A. A. Karawia, "*An Image Encryption Algorithm Based on Bisection Method and One-Dimensional Piecewise Chaotic Map*" in IEEE Access, vol. 9, pp. 43411-43421, 2021, doi: 10.1109/ACCESS.2021.3065810.
- [9] Hossain. M. B, M. T. Rahman, A. B. M. S. Rahman and S. Islam, "*A new approach of image encryption using 3D chaotic map to enhance security of multimedia component*" 2014 International Conference on Informatics, Electronics & Vision (ICIEV), 2014, pp. 1-6, doi: 10.1109/ICIEV.2014.6850856.
- [10] Jasra.B and A. H. Moon, "*Image Encryption techniques: A Review*" 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2020, pp. 221-226, doi: 10.1109/Confluence47617.2020.9058071.
- [11] Mustafa.G, R. Ashraf, I. U. Haq, Y. Khalid and R. U. Islam, "*A Review of Combined Effect of Cryptography & Steganography Techniques to Secure the Information*" 2019 5th International Conference on Computing Engineering and Design (ICCED), 2019, pp. 1-6, doi: 10.1109/ICCED46541.2019.9161128.
- [12] Qian.Q, Q. Yang, Q. Li, Q. Liu, Y. Wu and W. Wang, "*A Novel Color Image Encryption Algorithm Based on Three-Dimensional Chaotic Maps and Reconstruction Techniques*" in IEEE Access, vol. 9, pp. 61334-61345, 2021, doi: 10.1109/ACCESS.2021.3073514.
- [13] Veena. G & M, Ramakrishna. (2021). "*A Survey on Image Encryption using Chaos-based Techniques*" International Journal of Advanced Computer Science and Applications. 12. 10.14569/IJACSA.2021.0120145.

- [14] Xiuli Chai, Jianqiang Bi, Zhihua Gan, Xianxing Liu, Yushu Zhang, Yiran Chen, “*Color image compression and encryption scheme based on compressive sensing and double random encryption strategy*” *Signal Processing*, Volume 176, 2020.
- [15] Wu, Xiangjun & Li, Yang & Kurths, Juergen. (2015) “*A New Color Image Encryption Scheme Using CML and a Fractional-Order Chaotic System*” *PLOS ONE*. 10. e0119660. 10.1371/journal.pone.0119660.
- [16] Zhang, Xuncai & Wang, Lingfei & Wang, Yanfeng & Niu, Ying & Li, Yinhua. (2020), “*An Image Encryption Algorithm Based on Hyperchaotic System and Variable-Step Josephus Problem*” *International Journal of Optics*. 2020. 1-15. 10.1155/2020/6102824.