iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: VII Month of publication: July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36314

Image Security using Steganography and Cryptography

Kavia[1], K. Anushudha[2]
[1, 2]Department of Electronics Engineering, Pondicherry University, Puducherry

Abstract: Cryptography and Steganography could be used to provide data security, each of them has a problem. Cryptography problem is that, the cipher text looks meaningless, so the attacker will interrupt the transmission or make more careful checks on the data from the sender to the receiver. Steganography problem is that once the presence of hidden information is revealed or even suspected, the message is become known . According to my proposed work in which both steganography and cryptography are combine and give good security for data. Firstly, the encrypted images has been hidden using image steganography method. Secondly, the Hash function algorithm has been modified and used to encrypt the stego image by using 128 digit hexa-key. Therefore, two levels of security have been provided using the proposed technique. In addition, the proposed technique provides high embedding capacity and better quality stego images.

Keywords: Cryptography, Steganography, Least Significant Bit (LSB), Advance Encryption Standard (AES), RGB Shuffling, Encryption, Decryption

I. INTRODUCTION

The Steganography, Cryptography and Digital Watermarking techniques can be used to obtain security and privacy of data [1]. Steganography is the art and science of communicating in an approach which hides the existence of the communication [2]. Image steganography system is comprised two algorithms, one for embedding and another one for extraction. Cryptography and steganography are two approaches used to secure information, either by encoding the information with a key or by hiding it [3]. The embedding process will hides a secret message within a cover media (cover image), and the result of embedding process is stego image. Cryptography is the study of methods of sending messages in disguised form (not understood) so that only the intended recipients can remove the disguise and read the message. It protects information by transforming it into an unreadable format [4]. Cryptography is visible communication and steganography is invisible communication in terms of message. The critical aspect related with the importance of data that is transferred on the cloud is the security of the data, since the data can be confidential.

A new approach to encrypt the image by shuffling the RGB pixels, in that research, the cipher image were retrieved by extracting the RGB pixels of the input image, and then the RGB values were swapped by changing the position and the values of the RGB pixels [5]. Encryption technique by shuffling the RGB pixel values by displacing the RGB pixels and also interchanging the RGB pixel values, and at the end the total image size before encryption is the same as the total image size after encryption[6]. Securing image digital data could be done using ANN Method [7].

II. RELATED WORK

There are many methods have been used to provide data security whether by using encryption, steganography or combination between them. Advance encryption standard (AES) method, it is also known as Rijndael, is a symmetric-key block cipher [8]. Unlike DES method, AES method is a non Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. In AES method, the input and output sequences have the same length [9],[10]. According to AES method, substitution byte, shift rows, mixing column and key adding steps are implemented in every encryption round to encrypt the message, but the Mixing Column step doesn't included in the last round. In the decryption, the four steps are implemented in the reverse way. Also, the inverse of mixing column step doesn't include in the last round of the decryption. AES algorithm is more secure, support larger key sizes than DES, faster in both hardware and software, reasonable cost, and its main characteristics flexibility and simplicity [9]. Based on spatial domain instead of using LSB1 (First Least Significant Bit) of the cover image for embedding the message bits, LSB-3 (Third Least Significant Bit) has been used to hold the message bits and LSB-1, LSB-2 may also be modified [11].

Steganography method by implement a random key generator as a method. Stream cipher (LFSR) is the basic idea behind random key generator. Choosing the randomness for the embedding locations creates poor visual effects despite the large capacity [12]. Improvements over the visual quality is made by choosing the edge pixels Secret key and a weight matrix to protect the hidden data, it also uses a weight matrix to enhance the data hiding ratio [13].

LSB is the most popular Steganography method used to hide the secret messages by using algorithm 1. LSB makes the changes in the image resolution quite clear as well as it is easy to attack [14], [15]. LSB steganography and cryptography combined techniques used for the secret information is encrypted using RSA or Diffie Hellman algorithm before embedding in the image [16]. Optimal discrete wavelet transform (DWT) based steganography for the peak signal noise ratio (PSNR) [17]. The combined Integer Wavelet Transform (IWT) and Discrete Cosine Transform (DCT) which embeds secret image in frequency domain of cover image with high matching quality [18].

III. PROPOSED WORK

The proposed approaches based on embed the secret image information into another images in a way that can be invisible and doesn't degrade or much affect the quality of the original image. The target users of the presented system are those who want to make their information secure or protect their work form other or illegal use. This system provides an efficient way for secure transfer of information. This system able to manipulate with different file fo.rmats e.g. Bitmap, jpeg/jpg, GIF, and TIFF and able to hide secret image in another image of same format simultaneously it give security by using hash function cryptography. Security analyses indicate that the proposed image encryption scheme not only has good encryption effect and able to resist against the known attacks ,but also is sufficiently fast for practical applications.

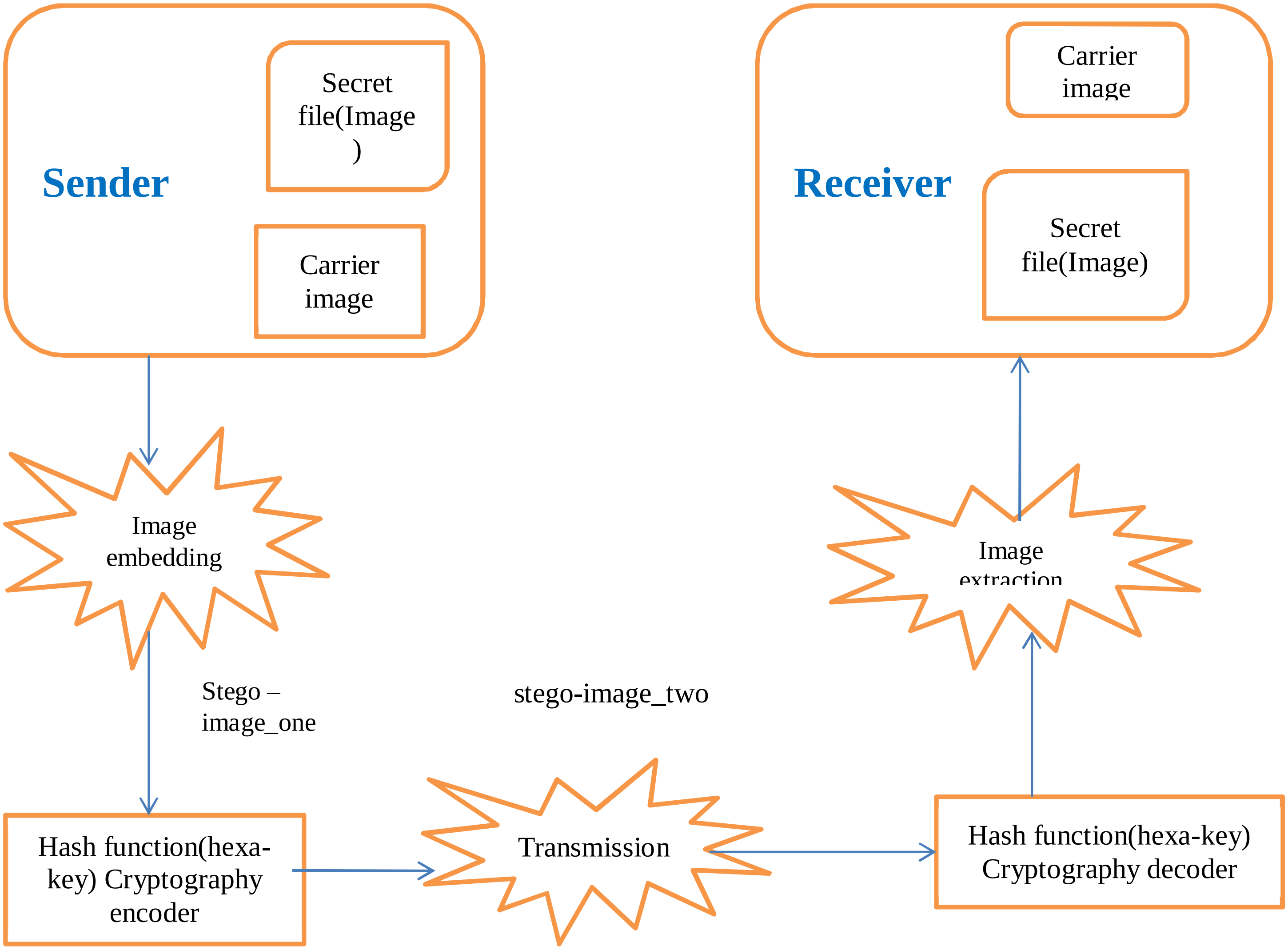


Fig.1 Block diagram of proposed work

A. Carrier and Secret Image

Carrier image are those in which secret image is going to embed for data privacy and the image should be medium sized to get better results, as very large sized image will use more bandwidth on internet and very small sized images may lost their bit of quality for bulky size of input text data

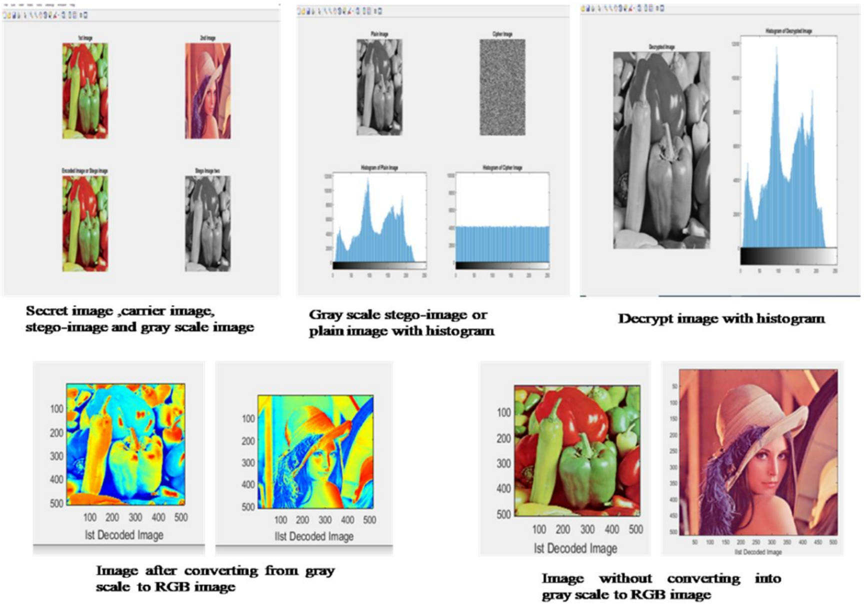
Secret image should be different from carrier image but make sure that the carrier image and secret image are same format type (bmp, jpg, gif).

B. Hash Function

Hash based algorithm is used to encoded stego image by using hex-key for secure cryptography encryption. Perfect hashing is defined for set N to map distinct elements in N to distinct integers, without any collisions. Perfect hashing is faster than other techniques to avoids any hash collision. Hence, there is no need to use any collision resolution techniques (such as linear probing or quadratic probing) and supports very large key sets so we can use it for very bulky data sets and it is equally effective and efficient for large data sets as for small data sets.

IV. RESULT AND DISCUSSION

In MATLAB, different colour image with different size and format is used to embed secret image into carrier image of same format. The system proved to be compatible to all the image file format and yielded good results and correlation coefficients of corresponding cipher images are close to zero.



Secret image ,carrier image, stego-image and gray scale image

Gray scale stego-image or plain image with histogram

Decrypt image with histogram

Image after converting from gray scale to RGB image

Image without converting into gray scale to RGB image

Fig. 2 Encryption and decryption output

A. Parameter Analysis

Parameters are analysed such as key security, Histogram analysis, Correlation coefficient, Information entropy, NPCIR and UACI , Robustness and Executation time analysis.

1) Key Security Analysis

The key security includes two aspects: Key space and Key sensitivity [19].

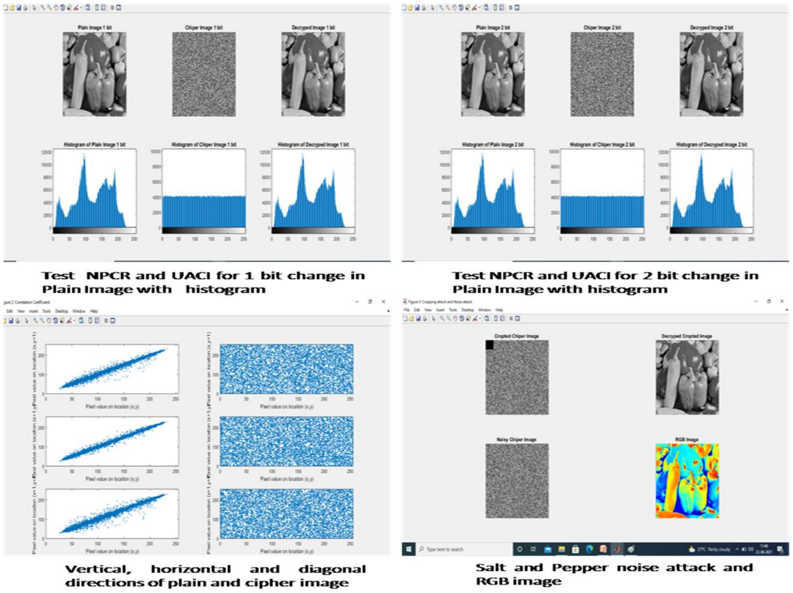
The key space is the set of all possible key that can be used for the encryption algorithm. It is clear that the larger the key space, the more secure the encryption image algorithm. When the key space is larger than $2^{100} \approx 10^{30}$, the image encryption algorithm will be able to resist the brute-force attacks [20]. The cipher image can be decrypted with secret key consists of two parts (the 256-bit external key and the 256-bit hash value). The key space size will be2^{512}, which is much larger than 2^{100}. Therefore, the proposed image encryption scheme has a large enough key space which would lead to higher security level of resisting the brute-force attack.

A robust encryption algorithm should be extremely sensitive to the change of its secret key. When any bit of the secret key is changed, the NBCR of the two obtained cipher images in the encryption process and the NBCR of the two obtained decrypted images in the decryption process are 50% in average. This means that the two obtained cipher images and the two obtained decrypted images are completely different and the proposed encryption scheme has an extremely sensitive to the secret key.

2) *Histogram Analysis:* The image histogram represents the number of pixels for each gray intensity level. When the cipher-image histogram should be close to a uniform distribution, then the image encryption scheme is more robust against statistical attack. From fig(2) and fig(3) the cipher-images histograms are fairly uniform which makes statistical attacks more difficult.

Table. 1 Different output parameters for both transmitter and receivers

Secret image	Carrier image	Encryption time	Stego-image entropy	Decryption time	Cipher image entropy	PSNR of cropping cipher image	PSNR of noisy cipher image	NPCR	UACI
Peppers.jpg	Lena.jpg	11.3297	7.5827	43.03874	7.9998	26.7367	31.8135	0.996154	0.334095


Plain Image 1 bit
Chiper Image 1 bit
Decryped Image 1 bit
Histogram of Plain Image 1 bit
Histogram of Chiper Image 1 bit
Histogram of Decryped Image 1 bit
Plain Image 2 bit
Chiper Image 2 bit
Decryped Image 2 bit
Histogram of Plain Image 2 bit
Histogram of Chiper Image 2 bit
Histogram of Decryped Image 2 bit
Pixel value on location (x,y)
Pixel value on location (x,y+1)
Cropted Chiper Image
Decryped Cropted Image
Noisy Chiper Image
RGB Image

Test NPCR and UACI for 1 bit change in Plain Image with histogram

Test NPCR and UACI for 2 bit change in Plain Image with histogram

Vertical, horizontal and diagonal directions of plain and cipher image

Salt and Pepper noise attack and RGB image

Fig.3 parameters analysis output

3) *Correlation Coefficient:* In a digital image, the correlation coefficient reflects the connection between its pixels. The correlation between adjacent pixels in vertical, horizontal and diagonal directions is usually high for the plain images. A good image encryption scheme should significantly reduce the correlation between adjacent pixels in the cipher image to resist the statistical attack. The ideal correlation value is zero. . In this paper, I randomly select pairs of adjacent pixels in the vertical, horizontal and diagonal directions from the plain image and cipher image, and compute the correlation coefficient of two adjacent pixels by

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x)(y_i - E(y))$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i \;- E(X))^2$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}X_i$$

Where N is the number of pixels pairs, x and y are the gray values of two adjacent pixels, E(x) is the mean, D(x) is the variance and cov(x, y) is the covariance. From fig(4) shows the correlation of two adjacent pixels in the cipher image significantly reduced. From below Table 2.The coefficients of corresponding cipher images are close to zero.

Table. 2 Correlation coefficient for plain and cipher image

CORRELATION COEFFICIENT					
Vertical		Horizontal		Diagonal	
Plain	Cipher	Plain	Cipher	Plain	Cipher
0.9927	0.0059	0.9963	0.0081	0.9887	0.0056

4) *Information Entropy Analysis:* The information entropy is most criterion to measure the randomness of a message, calculate by below formula

$$H(m) = \sum_{i=0}^{2^L-1} p(mi) log_2 \frac{1}{p(mi)}$$

Where l is the length of a pixel value in bit and p(mi) is the probability of symbol mi in message m. The entropy values of cipher images are extremely close to the theoretical value 8 and the cipher images have good random distributions. Therefore, the probability of information leakage is very negligible and the proposed encryption scheme is strong against entropy attacks.

5) *NPCR and UACI:* The NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are important criteria for differential attack analysis. Which can be calculated by below formula

$$NPCR(C_1,C_2) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\%$$

$$UACI(C_1,C_2) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%$$

$$D(i,j) = \begin{cases} 0 \ if \ C_1 \ (i,j) = C_2(i,j) \\ 1 \ if \ C_1(i,j) \neq C_2(i,j) \end{cases}$$

Where M and N are the width and height of the plain image, respectively. C1 (i, j) and C2 (i, j) are cipher images before and after changing the pixel value at location (i, j) of the plain image. The expected values of NPCR and UACI are 99.6094% and 33.4635%, respectively .The results summarized in Table 1. The NPCR and UACI results of the proposed image encryption scheme are extremely close to the expect values. Therefore, the proposed image encryption scheme is very sensitive to the plain image and can effectively resist the differential attack.

6) *Robustness Analysis:* We use cropping attack and noise attack to analysis the robustness of the proposed image encryption scheme. The PSNR (Peak Signal to Noise Ratio) between the plain image and the decrypted image is important criteria to measure the quality of decrypted image, defined

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(P(i,j) - D(i,j))^2$$

$$PSNR = 10 \times log\frac{MAX_I^2}{MSE}$$

Where M and N are width and the height of the image, respectively. P (i, j) and D (i, j) are the plain image and decrypted image, respectively, and the MAX_I^2 is the square of the maximum pixel value of the image. The experimental results show that the proposed encryption scheme is robust against salt & pepper noise attack.

7) *Execution Time Analysis:* The time complexity of encryption algorithms is also an important criteria of algorithmic performance, especially for real-time Internet applications and the era of big data. All image encryption algorithms are implemented with MATLAB R2015a and run on a computer with 16.0 GB RAM and Intel(R) Core (TM) i7-6700HQ CPU 2.60GHz.

V. CONCLUSION

The designed system has robust ability to read secret image from a (bmp, git: jpeg, and tif) carrier image. This system specifically works for efficient and secure image hiding into another images to make possible large-sized data encryption and transmission over internet. In order to prove the efficiency of the proposed encryption scheme, I analyzed its security and performance in terms of key space analysis, key sensitivity analysis, histogram analysis, correlation analysis, information entropy analysis, robustness analysis and execution time. The experimental results showed that the proposed image encryption scheme can not only achieve good security, but also sufficiently fast for practical application.

VI. ACKNOWLEDGMENT

The authors are grateful to the Department of Electronics and communication, Pondicherry University, Pondicherry for providing technical assistance during the study.

REFERENCES

[1] Nutzinger, M.C Fabian and M. Marschalek. ”Secure Hybrid Spread Spectrum System for Steganography in Auditive Media”. In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Sixth International Conference, 2010.

[2] S.Bhattacharyya, A. Khan, A. Nandi, A. Dasmalakar, S. Roy and G. Sanyal. "Pixel mapping method (PMM) based bit plane complexity segmentation (BPCS) steganography," Information and Communication Technologies (WICT), 2011 World Congress ec. 2011.

[3] N Khan and K.S. Gorde. "Data security by video steganography and cryptography techniques," International Journal of Innovative Research in Science, Engineering and Technology,2015.

[4] A. Menezes, P. Oorschot, S. Vanstone and A. J Menezes.. “Handbook of Applied Cryptography”, CRC Press, Boca Raton, FL, 1997.

[5] N. Agarwal and P.Agarwal “An Efficient Shuffling Techniques on RGB Pixels for Image Encryption”, MIT International Jou.rnal of Computer Science & Information Technology, Vol. 3, No. 2, pp. 77-81, 2013.

[6] Quist-Aphetsi Kester. MIEEE “Image Encryption based on the RGB Pixel Transposition and Shuffling” International Journal Computer Network and Information Security, No.7 pp. 43-50, 2013.

[7] S. K.Pal and S. Anand."Cryptography Based on RGB Color Channels using ANNs", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.5, pp.60-69, 2018.

[8] A. Shoukat. “A Survey about the Latest Trends and Research Issues of Cryptographic Elements,” IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, PP. 140-149, May 2011.

[9] A Shoukat. “A Survey about the Latest Trends and Research Issues of Cryptographic Elements,” IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, PP. 140-149, May 2011.

[10] J. Daemen and V. Rijmen. “AES Proposal: Rijndael,” version 2, PP. 1- 45, 1999.

[11] A.I. Sada. “Hiding Data Using LSB-3”, J.basrah researches (sciences), vol. 33. No. 4, pp. 81-88, Dec. 2007.

[12] I. A.Sattar and M. T. Gaata. "Image steganography technique based on adaptive random key generator with suitable cover selection” Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Page(s):208-212 Iraq- 2017.

[13] H. Yang and A.C Kot. "Pattern-Based Data Hiding for Binary Image Authentication by Connectivity Preserving," Multimedia, IEEE Transactions on , vol.9, no.3, pp.475-486, April 2007.

[14] M.K. Khan, M. Naseem, I.M. Hussain and A. Ajmal. "Distributed Least Significant Bit technique for data hiding in images," Multitopic Conference (INMIC), IEEE 14th International , vol., no., pp.149-154, 22-24, Dec. 2011.

[15] M. Al-Shatnawi. “A new method in image steganography with improved image quality”Appl. Math. Sci., Vol. 6, no. 77-80, 3907-3915, 2012.

[16] S.Gupta, A.Goyal and B. Bhushan. “Information Hiding Using Least Significant Bit Steganography and Cryptography” International Journal Modern Education and Computer Science, vol. 6, pp. 27-34, 2012

[17] T. Narasimmalou and R. A. Joseph. “Optimized Discrete Wavelet Transform based Steganography” , IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT),2012.

[18] N. Raftari, A. Masoud and E. Moghadam. “Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT”, Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012.

[19] Z. Hua, B. Xu, F. Jin, and H. Huang. “Image encryption using josephus problem and filtering diffusion". IEEE Access 7:8660–8674, 2019

[20] P. Ping, J. Fan, Y. Mao, F. Xu and J. Gao “A chaos based image encryption scheme using digit-level permutation and block diffusion". IEEE Access 6:67581–67593, 2018