Volume 66, Issue 2, 2022
Journal of Scientific Research
of
The Banaras Hindu University

A New Blended Approach of Data Hiding Using XNOR Operation

Kamaldeep Joshi*[1], Ravi Saini[2], Rajkumar Yadav[3], and Rainu Nandal[4]

*[1]UIET, Maharshi Dayanand University, Rohtak, Haryana, INDIA, kamalmintwal@gmail.com
[2]UIET, Maharshi Dayanand University, Rohtak, Haryana, INDIA, ravigpsanghi@gmail.com
[3]UIET, Maharshi Dayanand University, Rohtak, Haryana, INDIA, rajyadav76@rediffmail.com
[4]UIET, Maharshi Dayanand University, Rohtak, Haryana, INDIA, rainu_nandal@yahoo.com

***Abstract*—This paper proposed a new data hiding technique which uses a blended approach of security. It uses a blend of cryptography and steganography at the same time to provide two layers of security. At first, data is encrypted using Rail Fence cryptography algorithm and at the second level the encrypted data is inserted into an image by using insertion algorithm based on XNOR operation. Encrypted bits are put into the pixels of the image which becomes a difficult task for the attackers to find the hidden data. In this approach, the concept of spatial domain is used for hiding the message and retrieval of message. The preliminary experimental results based on PSNR, MSE, Histogram and Coefficient of Correlation show that the proposed method provides better imperceptibility and hiding capacity. It was also compared with some trade off methods on the basis of various metrics. It also provides very less deflection in cover image so that it becomes very difficult for a third person to differentiate between cover image and stego image.**

ImageData HidingSteganographyCryptography

***Index Terms*—Image, Data Hiding, Steganography, Cryptography.**

I. Introduction

Information security is becoming very important with the increased use of internet technology. So it has become crucial to protect secret information from unauthorized access. There are three main techniques to provide an information security steganography, cryptography, watermarking (1; 23). Steganography is used to hide the secret information. Steganographic techniques hide the existence of the message, whereas Cryptography is the process of hiding the meaning of secret message. In case of Watermarking, secret information is hidden in a digital signal. Usually, the watermark is unchangeable. So, Watermarking is used to protect copyright information (2). Cryptography is a process to encrypt the message so that only authorized person can access that information (3). The word Steganography is made from two words Stegno and Graphy. In Greek, meaning of Stegno is covert and meaning of Graphy is writing which together means Covert writing(4). The security of steganography system lies on the fact that the intruder does not know anything about the presence of message in cover media (5). It is better to combine Cryptography and Steganography for providing two layers of security. By combining, these two techniques, first of all the information are encrypted using cryptography and then the cipher text is embedded into a cover media like a cover image using steganography. The idea of combining these two techniques together gives more security to the secret information(6). The need for security and Integrity will be satisfied with this combination(7; 19; 20).In the LSB method, Johnson and Jajodia(8; 22) hide the message in the LSB least significant bit of an image. Wu and Tsai (9) discussed PVD pixel value differencing, which provided better embedding capacity and also provided good imperceptibility.Bilal et al.(10) proposed a new information hiding technique that hides the message according to the relationship of image, secret message, the chaotic sequence and chaotic map. Anees et al.(11) presented a new method of information hiding. In this technique, cover image is divided into two Parts, i.e. the Upper part and the lower part. The secret messages binary bits are divided into four MSBs and four LSBs. Tamimi et al.(12) presented a new method to hide messages in the LSBs least significant bits of an image pixels. In this method different numbers of hiding bits are used in each pixel. Raghavan et al. (16) gives a novel method by improved DNA insertion algorithm. DNA is used for inserting the secret information. This method enhances more security by adding XOR operation. Mukherjee et al. (17) introduced a novel approach which uses the Arnold transformation and an MPV technique to insert data into the image. Younus and Hussain(18) proposed a new method in which Vigenere Cipher is used for encryption and Huffman Coding is used for compression of bits. . Rajendiran et al.(25) proposed a Steganography Methodology Applied in Transposition Cipher for Hiding Text message and claim the increase in payload capacity, robustness and quality. The main research problem is

*DOI:*10.37398/JSR.2022.660216

that there is trend of developing the steganography techniques that uses selective part of the images for insertion of data. Most of the techniques changes the statistical properties of images due to which chances of statistical steganalysis increases. Most of the developed techniques also does not uses the dual layer of security by combining it with Cryptography. In proposed method, we have used both crptography and steganography for providing dual layer of security. Our method also uses complete image for insertion of message. It will not use selective part of image for embedding of secret message.

II. Proposed Method

This paper introduced a new blended technique of data hiding which uses steganography and cryptography together. The insertion process is shown by Figure 1. At first, secret data is encrypted through the Rail Fence technique. This encrypted secure data is now inserted in the cover image at some selected locations. The LSB and MSB of the selected pixel are extracted for hiding the message. XNOR operation is applied on the extracted LSB and MSB. Resultant value may be 0 or 1. The message bit will be inserted in the pixel as per resultant value. The extraction process is shown by Figure 2. Stego image will be sent to the receiver which would carry secure encrypted data. The LSB and MSB of the selected pixel are also extracted at the receiver end. After that XNOR operation is applied to find the resultant value. On the basis of resultant value all encrypted secret bits are received at the retrieval end. These encrypted data is now decrypted using Rail Fence technique to get the original secret data. The insertion and retrieval process is also shown by flowchart given in Figure 3 and Figure 4.

III. Algorithm

In this section, we will discuss about the insertion and extraction algorithm.

A. Assumptions

1. The cover image for securing the message will be grayscale image in which the pixel size must be of eight bits.
2. The secret key for generating the locations of pixels for message embedding is shared between sender and receiver.
3. The level of rail fencing will also be shared between sender and receiver.
4. The sender and receiver will also be agree on the cover images in which message would be inserted.

B. Insertion Algorithm

The insertion algorithm insert the message into cover image and generates the stego image. It comprises of the following steps:

1. Let I, the cover image of r*c pixels given by equation 1.

$$I = \{I_{ij}, 0 <= i <= r, , 0 <= j <= c, i, j \epsilon (0, 255)\} \quad (1)$$

2. Let B is a binary string of N bit secret data in a 1*N matrix given by equation 2.

$$B = \{B_{ij}, 0 <= i <= N, B_i, i \epsilon (0, 1) and N \epsilon (0, N)\} \quad (2)$$

3.Convert the binary string of secret data into encrypted secret data B' using Rail Fence technique. B' can be represented as follows:

$$B' = E(B) \quad (3)$$

4. Generate the random location of the pixels of cover image using linear equation 4 :

$$Loc(n+1) = (a * Loc(n) + b) Mod\ c \quad (4)$$

5. Convert the selected pixel in step 3 into binary form which can be represented as follows:

$$Binary(P) = \{b_{ij} | 0 < i <= r, 0 < j <= c\ and\ b_{ij} \epsilon (0, 1)\} \quad (5)$$

6. Extract the LSB and MSB of pixel P per equation 6 and 7 given below:

$$Bit(S, LSB) = \{S(i) | 0 < i <= 7\ and\ S(i) \epsilon (0, 1)\} \quad (6)$$

$$Bit(S, MSB) = \{S(i) | 0 < i <= 7\ and\ S(i) \epsilon (0, 1)\} \quad (7)$$

7. Find Resultant of step 5 using XNOR operation as per equation 8.

$$Resultant(P) = XNOR(Bit(S, LSB), Bit(S, MSB)) \quad (8)$$

8. Insert bit b got in step 3 into the pixel P selected using step 4. If b=0 and Resultant(P) =0 then no change in pixel value is required. If b= 0 and Resultant(P) =1 then add or subtract 1 to the pixel selected such that Resultant(P) becomes 0. If b=1 and Resultant(P) =1 then no alteration in pixel value is required. If b=1 and Resultant(P) =0 then add or subtract 1 to the pixel intensity so that the value of Resultant(P) becomes 1.
9. Repeat all the above steps until all the encrypted secret bits are inserted in the cover image.
10. When all bits are inserted in cover image then it became the stego image S(r,c) that would be sent to receiver end.
11. EXIT.

C. Extraction Algorithm

Extraction algorithm will extract the secret data inserted into the stego image.

1. Generate the same pixel locations where data is hidden using equation 4.
2. Step 5, 6 and 7 of insertion algorithm are applied same at the receiver end also.
3. If Resultant(P) comes 0 then encrypted message bit is 0 otherwise it is 1.
4. Sequence all the encrypted message bits to form the full

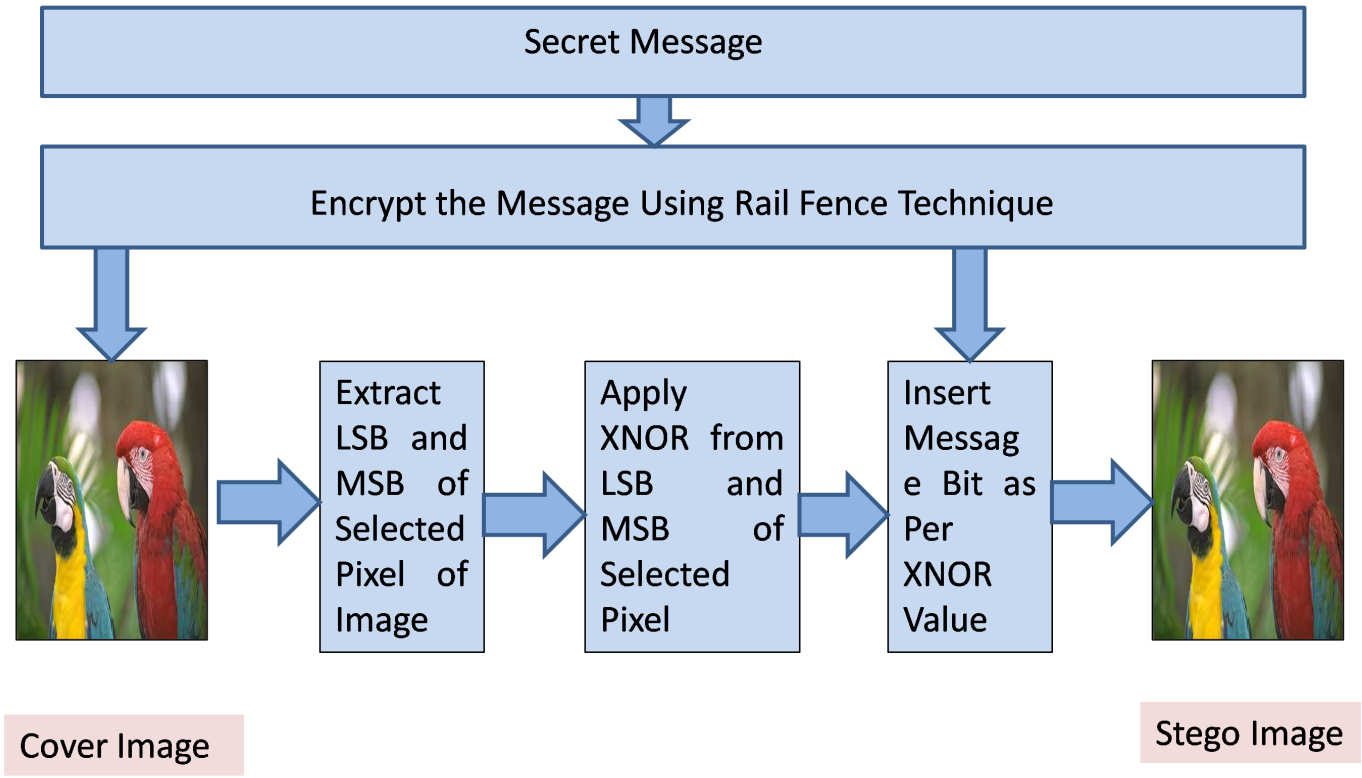

Fig. 1. Insertion Process

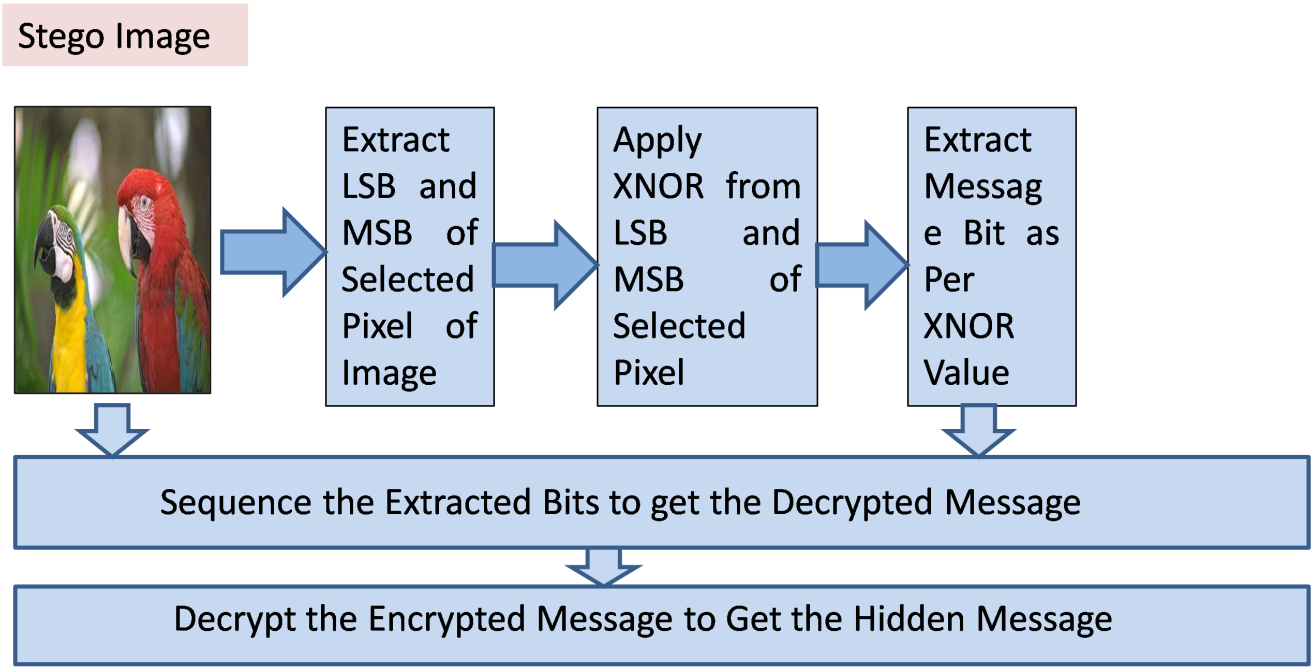

Fig. 2. Extraction Process

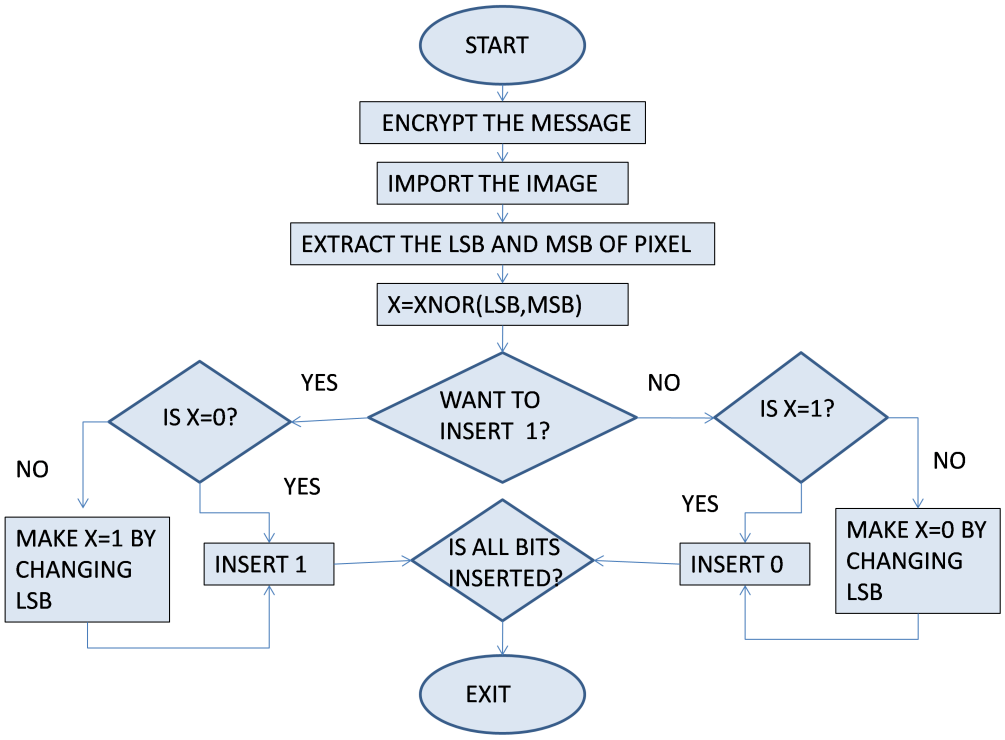

Fig. 3. Insertion Process Flowchart

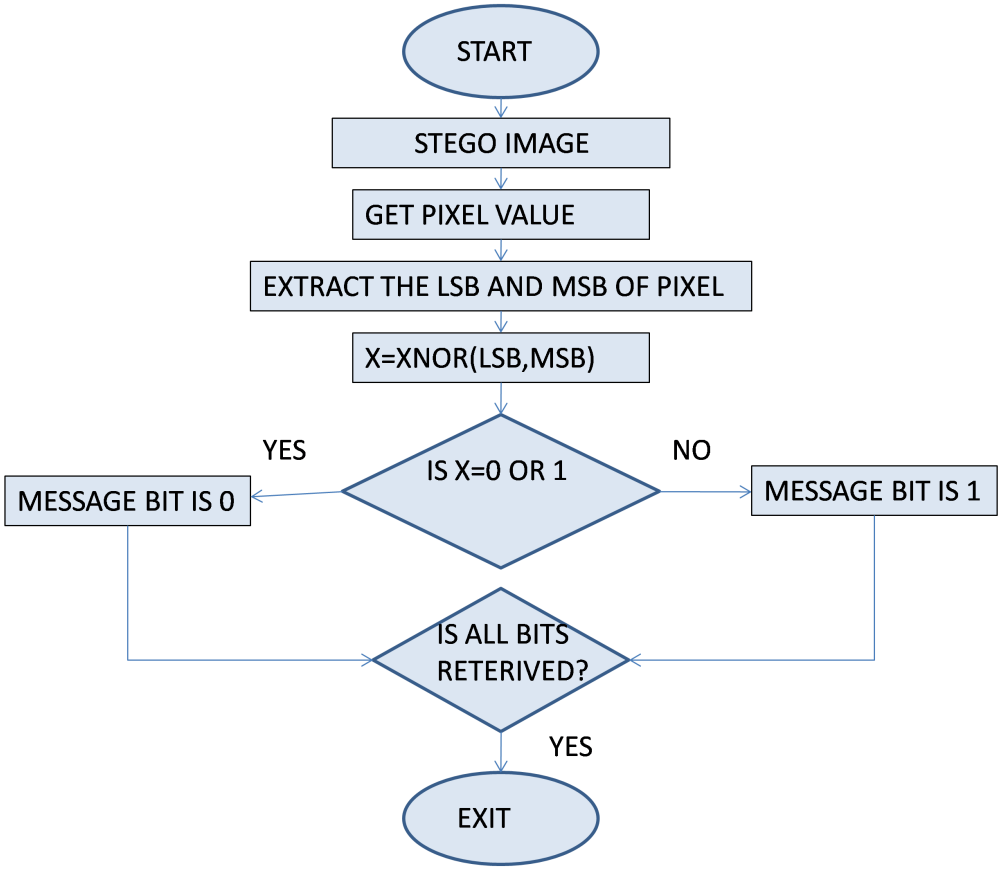

Fig. 4. Extraction Process Flowchart

encrypted message.
5. Decrypt the encrypted message using Rail Fence technique as which can be shown by equation 9.

$$B = D(B') \tag{9}$$

6. EXIT.

IV. Results and Analysis

In this section, we will analyze the proposed method on the basis of different parameters. In first subsection, PSNR and MSE based analysis with histograms have been done. In second subjection, the proposed method is compared with other methods. In last subsection, Coefficient of Correlation based analysis has been done.

A. PSNR and MSE based Analysis

This subsection shows the quality of image and performance of the proposed method. We have used MATLAB 2010 to implement our method on an i7 machine in Microsoft windows7. Four standard images LENA, BABOON, TRIFFY, PEPPERS, has been taken as inputs for result analysis. The proposed algorithm is analyzed on the standard parameters like PSNR, MSE, and HISTOGARAM etc. The results are shown by the figures 5 to 8. The size (capacity) of the secret data is taken 1024 bits, 2048 bits and 4096 bits to repeat the experiment on the proposed algorithm.The PSNR (13; 21) calculates signal to noise ratio between images. The PSNR is measured in decibels. The relation between the PSNR and MSE (Mean Square Error) is that they are inversely proportional to each other. MSE calculates the average of the square of errors between the original and the stego images. These values are kept low because near to zero values are better. The equation of PSNR is given below:

$$PSNR = 10\log_{10}(I^2 * MSE) \tag{10}$$

MSE calculates the average of the square of errors between the original and the stego images. These values are kept low because near to zero values are better. The equation of MSE given below:

$$MSE = \sum_{i=1}^{r}\sum_{j=1}^{c}(x_{ij} - y_{ij})^2 \tag{11}$$

Figure 5 shows the cover image Lena before insertion and after insertion of 1024 bits of data. Figure 6 shows the histogram of original image and stego image after insertion of 1024 bits of data.Figure 7 shows the histogram of original image and stego image after insertion of 2048 bits of data.Figure 8 shows the histogram of original image and stego image after insertion of 4096 bits of data.Table 1 shows the PSNR, MSE, Pixels used, Pixels Modified, Insertion Time and Retrieval Time for a different set of images on 1024 bits, 2048 bits and 4096 bits data.The higher value of PSNR shows that there is a very less deflection in the cover image after insertion of data. The insertion and reterival time is also very less which shows the effectiveness of the proposed approach.

B. Comparison with other Methods

In this subsection, the proposed method is compared with LSB method(8) and Chaotic method (10)on the basis of PSNR and BER. Bit Error Rate (BER) is the measure of total bits changed in the cover image. It is given by following equation.

$$BER = \sum_{i=1}^{r}\sum_{j=1}^{c}(x_{ij} - y_{ij}) \div (r * c) \tag{12}$$

The results are shown in Table 2 and Table 3. Proposed method provides better value of PSNR and BER than other methods for different sets of images. 1024 bits, 2048 bits and 4096 bits have been taken as the hiding capacity for this comparison.

C. Coefficent of Correlation Based Analysis

In this section, the imperceptibility of the LSB method has been tested by using Coefficient of Correlation metric. Coefficient of Correlation metric was initially given by Karl Pearson. Coefficient of Correlation (r) between two variables X and Y given by equation 13:

$$r = Covariance(X,Y) \div (S.D.(X) * S.D.(Y)) = \sigma_{xy} \div \sigma_x * \sigma_y \tag{13}$$

Here, X and Y are the pixel values in cover file and stego files respectively. Covariance(X,Y) is the covariance between X and Y given by equation 14:

$$Covariance(X,Y) = \sigma_{xy} = (\sum_{i=0}^{n}(x_i - \bar{x})(y_i - \bar{y})) \div n \tag{14}$$

Here, S.D.(X) is the standard deviation given by equation 15:

$$StandardDeviation(\sigma) = \sqrt{\sum_{i=0}^{n}(x_i - \bar{x})^2 \div n} \tag{15}$$

Coefficient of Correlation does not alter if there is any alteration in scale or location. It is used to check the bonding between two sets of variables. The result of Coefficient of Correlation lies in the range [-1, +1]. It is the unit free measurement of bonding. When the value of Coefficient of Correlation is close to +1 then there is a strong positive set of relationship between two associated variables. When the value of Coefficient of Correlation is close to -1 then there is a strong negative set of relationship between two associated variables. When the value of Coefficient of Correlation lies near to zero, then there is a very less deflection in associated variables. Coefficient of Correlation a value near to zero shows high imperceptibility and value near to +1 or -1 shows low imperceptibility.The Coefficient of Correlation values on four different test images for different set of message sizes, is shown in Table 4, Table 5, Table 6 and Table 7 respectively. After analyzing the results from Table 4, Table 5, Table 6 and Table 7, it has been found that the resultant value of Coefficient of Correlation (r) for different test images for different set of messages lies near to 0 which shows very less deflection in the cover image. The Coefficient of Correlation results shows that proposed method is highly imperceptibility to the human visual system as the maximum possible alteration in the pixel intensity lies in range [-1, +1].

Fig. 5. Cover Image and Stego Image Lena after insertion of 1024 bits data

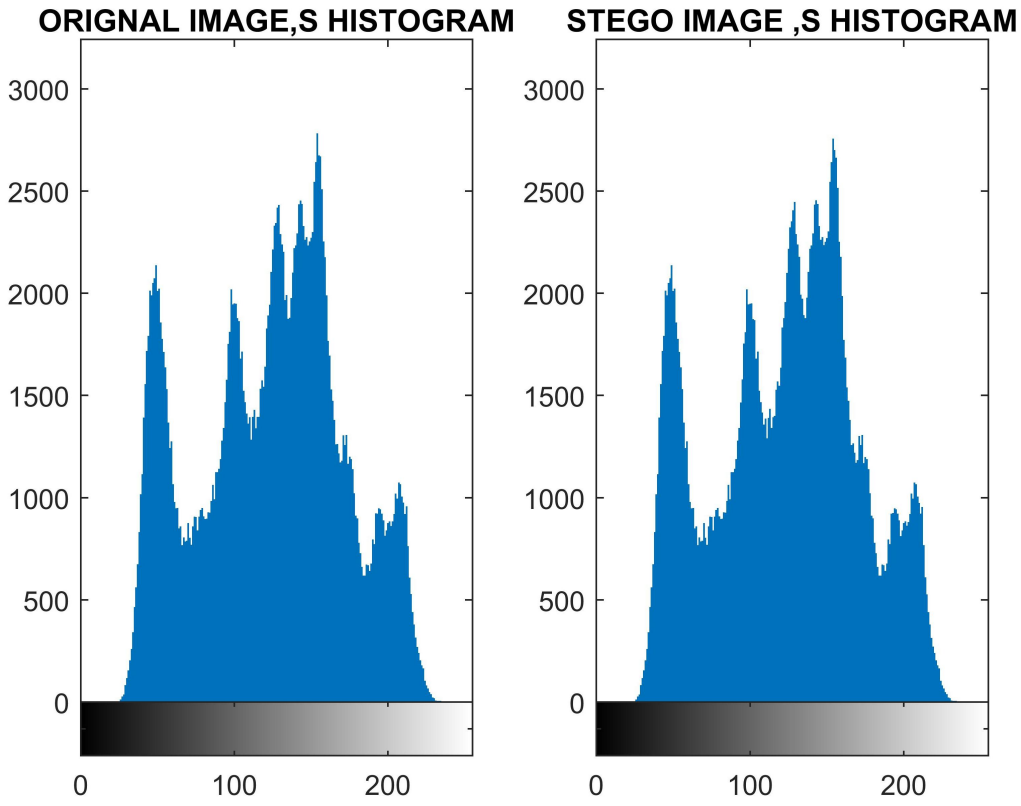

Fig. 6. Histogram of Cover Image and Stego Image Lena after insertion of 1024 bits data

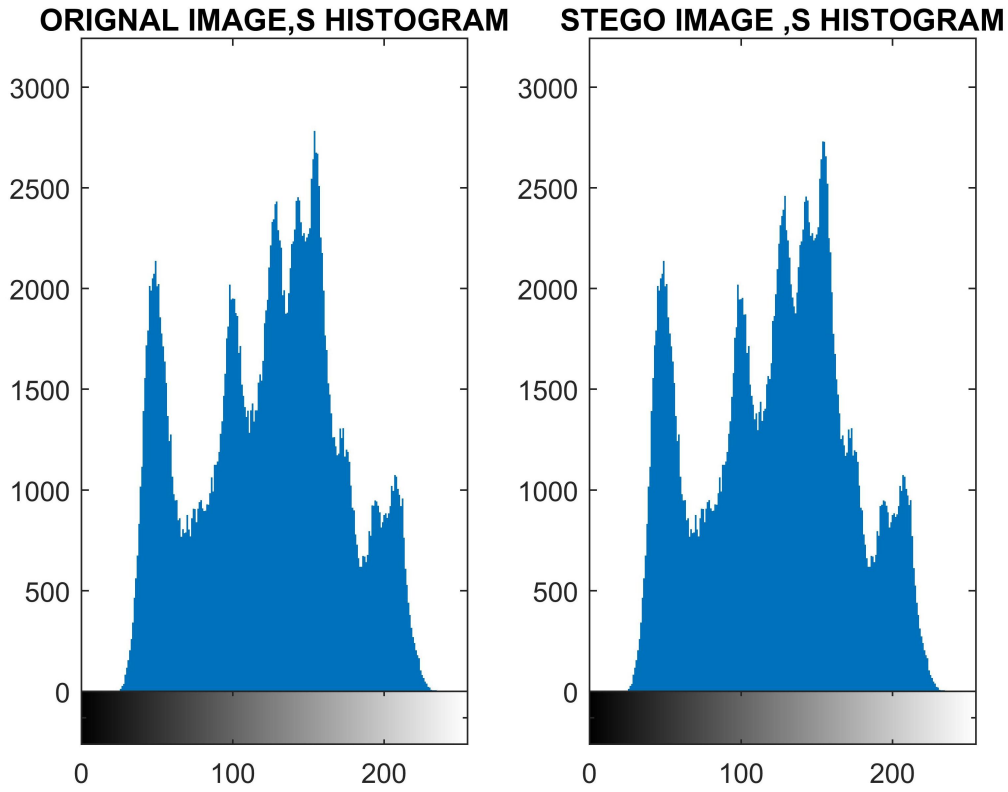

Fig. 7. Histogram of Cover Image and Stego Image Lena after insertion of 2048 bits data

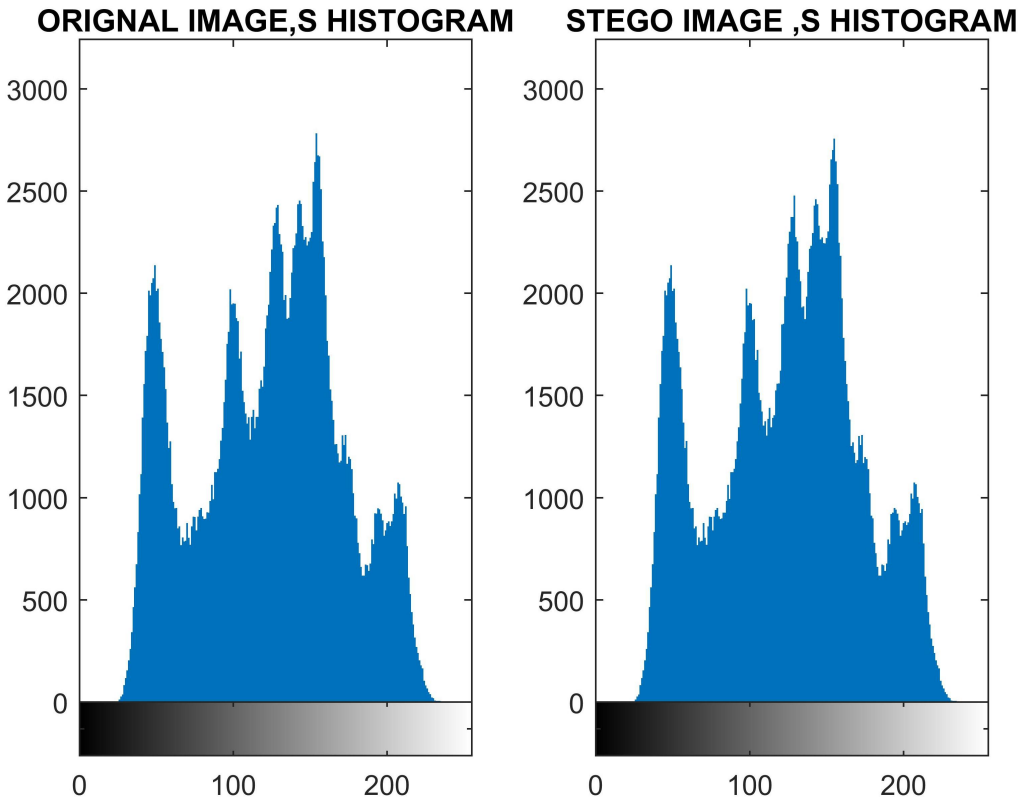

Fig. 8. Histogram of Cover Image and Stego Image Lena after insertion of 4096 bits data

TABLE I
PSNR AND MSE RESULTS FOR DIFFERENT IMAGES WITH DIFFERENT SETS OF EMBEDDING DATA.

Image	Image Size	Data(Bits)	Pixel Used(%)	Pixels Modified(%)	PSNR	MSE	Insertion Time	Reterival Time
Lena	512*512	1024	0.3906	.1919	75.3005	.0019	4.245640	.316513
Lena	512*512	2048	0.7813	.3746	72.3951	.0037	5.030054	.330170
Lena	512*512	4096	1.5625	.7496	69.3826	.0075	5.829563	.389363
Baboon	512*512	1024	0.3906	.2048	75.0165	.0020	2.358919	.307141
Baboon	512*512	2048	0.7813	.3902	72.2174	.0039	3.127978	.319159
Baboon	512*512	4096	1.5625	.7885	69.1628	.0079	5.513516	.335941
Triffy	512*512	1024	0.3906	.2022	75.0734	.0020	1.616181	.312585
Triffy	512*512	2048	0.7813	.3979	72.1334	.0040	3.34438	.330995
Triffy	512*512	4096	1.5625	.7969	69.1168	.0080	4.621555	.357088
Pepper	512*512	1024	0.3906	.1953	75.2235	.0020	3.919523	.307607
Pepper	512*512	2048	0.7813	.3811	72.3205	.0038	4.510146	.328196
Pepper	512*512	4096	1.5625	.7633	69.3037	.0076	4.650882	.385271

TABLE II
PSNR COMPARISON OF PROPOSED METHOD FOR DIFFERENT IMAGES WITH LSB AND CHAOTIC APPROACH FOR DIFFERENT SETS OF EMBEDDING DATA.

Image	Image Size	Data(Bits)	LSB Method PSNR	Chaotic Method PSNR	Proposed Method PSNR
Lena	512*512	1024	53.6442	38.6432	75.3005
Lena	512*512	2048	50.1237	35.5419	72.3951
Lena	512*512	4096	42.5700	32.5876	69.3826
Baboon	512*512	1024	53.3499	34.1444	75.0165
Baboon	512*512	2048	50.2320	31.3183	72.3951
Baboon	512*512	4096	47.2027	28.2366	69.1628
Triffy	512*512	1024	52.6112	37.6538	75.2885
Triffy	512*512	2048	49.3754	34.4149	71.4952
Triffy	512*512	4096	41.5777	33.7668	69.8265
Pepper	512*512	1024	54.5672	37.6835	75.5223
Pepper	512*512	2048	51.2386	36.5494	71.5178
Pepper	512*512	4096	42.4804	33.5632	70.3456

TABLE III
BER COMPARISON OF PROPOSED METHOD FOR DIFFERENT IMAGES WITH LSB AND CHAOTIC APPROACH FOR DIFFERENT SETS OF EMBEDDING DATA.

Image	Image Size	Data(Bits)	LSB Method BER	Chaotic Method BER	Proposed Method BER
Lena	512*512	1024	0.0025	0.0021	0.0016
Lena	512*512	2048	0.0043	0.0045	0.0019
Lena	512*512	4096	0.0048	0.0051	0.0021
Baboon	512*512	1024	0.0026	0.0024	0.0014
Baboon	512*512	2048	0.0032	0.0033	0.0016
Baboon	512*512	4096	0.0049	0.0043	0.0018
Triffy	512*512	1024	0.0034	0.0027	0.0019
Triffy	512*512	2048	0.0045	0.0034	0.0021
Triffy	512*512	4096	0.0051	0.0043	0.0023
Pepper	512*512	1024	0.0045	0.0038	0.0011
Pepper	512*512	2048	0.0048	0.0042	0.0013
Pepper	512*512	4096	0.0049	0.0043	0.0015

TABLE IV
COEFFICIENT OF CORRELATION VALUE FOR LENA IMAGE.

Image	Image Size in Bytes	Message Size	Coefficient of Correlation (r)
Lena Image	50625	1KB	0.013
Lena Image	50625	2KB	0.023
Lena Image	50625	3KB	0.054
Lena Image	50625	4KB	0.061
Lena Image	50625	5KB	0.069

TABLE V
COEFFICIENT OF CORRELATION VALUE FOR BABOON IMAGE.

Image	Image Size in Bytes	Message Size	Coefficient of Correlation (r)
Baboon Image	50625	1KB	0.017
Baboon Image	50625	2KB	0.021
Baboon Image	50625	3KB	0.044
Baboon Image	50625	4KB	0.049
Baboon Image	50625	5KB	0.061

TABLE VI
COEFFICIENT OF CORRELATION VALUE FOR TRIFFY IMAGE.

Image	Image Size in Bytes	Message Size	Coefficient of Correlation (r)
Triffy Image	50625	1KB	0.013
Triffy Image	16384	1KB	0.023
Triffy Image	16384	2KB	0.029
Triffy Image	16384	3KB	0.032
Triffy Image	16384	4KB	0.047
Triffy Image	16384	5KB	0.058

TABLE VII
COEFFICIENT OF CORRELATION VALUE FOR PEPPER IMAGE.

Image	Image Size in Bytes	Message Size	Coefficient of Correlation (r)
Pepper Image	50625	1KB	0.027
Pepper Image	50625	2KB	0.034
Pepper Image	50625	3KB	0.057
Pepper Image	50625	4KB	0.069
Pepper Image	50625	5KB	0.088

V. CONCLUSION AND FUTURE SCOPE

This paper shows the new approach of data hiding based on XNOR operation. By comparing the proposed method with LSB and Chaotic approach, the proposed method gives the best results as shown in Table 2. By analysis of various images like Lena, Baboon, Triffy and Peppers with their stego images, the proposed method gives better imperceptibility. The histogram analysis of original and stego images also indicates that there is not much difference between the original and stego images. Clubbing together the cryptographic and the Steganography approaches enhance the security level, as the hybrid proposed approach uses the benefit of both the techniques of security i.e. Cryptography and Steganography. In the future, we will try to club it with frequency domain and neural network which may yield better results.

REFERENCES

[1] Waziri, V. O., Ochoche, A.: Steganography and Its Applications in Information Dissimilation on the Web Using Images as Security Embedment: A Wavelet Approach. International Journal of Computer and Information Technology,**1**(2) 194–202(2012)

[2] Yadav, R., Saini, R.: Biometric Template Security Using Invisible Watermarking With Minimum Degradation in Quality of Template. International Journal on Computer Science and Engineering **3**(1), 3656–3668(2011)

[3] Pascal, V.: Code Based Cryptography and Steganography. Multimedia Tools Applications **7**(8), 9–46(2013)

[4] Lee, Y. K., Chen, C.: High capacity image steganographic model. IEEE Proceedings - Vision, Image, Signal Process **147**(3), 288-296(2000)

[5] Rajyaguru, M. H.: Cryptography-Combination of Cryptography and Steganography with Rapidly Changing Keys. International Journal of Emerging Technology and Advanced Engineering **2**(10),329–332(2012)

[6] Anand, H.,Narwal, K., Mudgal, K.: Implementation of 16 * 16 Quantization Table Steganography on Gray Scale Images. International Journal of Science and Research **2**(7),2–5(2013)

[7] Kaur, K., Singh, E. N.: Image steganography using cryptography. International Journal of Advanced Research in computer science **3**(6),402-405(2013)

[8] Johnson, N.,Jajodia, S: Exploring steganography: seeing the unseen. IEEE Computer **5**(1), 26–34(1998)

[9] Wu, D.C.,Tsai, W.H.: Steganographic method for images by pixel value differencing. Pattern Recognition Letters **24**(1),1613–1626(2003)

[10] Bilal, M., Imtiaz, S., Abdul W., Ghouzali S., Asif S.: Chaos based Zero-steganography algorithm. Multimedia Tools and Applications **72**(2), 1073–1092(2014)

[11] Hajizadeh, H., Ayatollahi, A., Mirzakuchaki, S.: A new high capacity and EMD-based image steganography scheme in spatial domain. 21st Conference of Electrical Enggineering(ICEE) **2**(5), 23–34(2013)

[12] Abdelfatah, A., Ayman, M., Omaima, A.: Hiding an Image inside another Image using Variable-Rate Steganography. International Journal of Advanced Computer Science and Applications **4**(10), 18–21(2013)

[13] Fangjun, H., Jiwu, H.: Calibration based universal JPEG steganalysis. International Journal of Computer Science and its Technology (IJCST) **52**(2), 260-268(2009)

[14] Luo, W., Huang, F., Huang J.: Edge Adaptive Image Steganography Based on LSB Matching Revisited. Informative Forensics Security Journal **5**(2), 201-214(2010)

[15] https://in.mathworks.com/help/vision/ref/psnr.html

[16] Malathi P., Manoaj, M., Raghavan R., Vinodhini R.E.: Highly Improved DNA Based Steganography. Journal of Computer Science **115**(1), 651–659(2017)

[17] Mukherjee S., Roy S., Sanyal G.: Image Steganography Using Mid Position Value Technique. Journal of Computer Science **132**(1), 461-468(2008)

[18] Younus Z. S., Hussain M. K.: Image steganography using exploiting modification direction for compressed encrypted data. Journal of King Saudi University - Computer and Information Sciences **8**(1) 1–11(2019)

[19] Joshi, K., Dhankhar, P., Yadav, R.: A new image steganography method in spatial domain using XOR. Proceedings of Annual IEEE India Conference (INDICON), IEEE :1–6(2015)

[20] Joshi, K., Yadav, R.:A New approach towards data hiding using XOR for image steganography.Proceedings of Ninth International Conference on Contemporary Computing (IC3), IEEE,1–6(2016)

[21] Joshi, K., Yadav, R., Allwadhi, S.: PSNR and MSE based investigation of LSB.Proceedings of International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), IEEE : 280- 285(2018)

[22] Joshi, K., Yadav, R.: A new LSB-S image steganography method blend with Cryptography for secret communication.Proceedings of Third International Conference on Image Information Processing (ICIIP), 86–90(2015)

[23] Allwadhi, S., Joshi, K., Yadav, A.K.: Pixel Interpolation Based Watermarking Scheme in Spatial Domain and its Analysis on Different Parameters. Journal of Advanced Research in Dynamical and Control Systems,**11**(5), 2087–2092(2019)

[24] Joshi, K., Gill, S.,Yadav, R.: A New Method of Image Steganography using 7th bit of a Pixel as Indicator by Introducing the Temporary Pixel in the Gray Scale Image. Journal of Computer Networks and Communications **6**(4): 1-10(2018)

[25] Rajendiran, P., Sekar, K.R., Ramesh, C., Manikandan, R.: A Novel Steganography Methodology Applied in Transposition Cipher for Hiding Text message. International Journal on Emerging Technologies **10**(2), 156-158(2019)

[26] Sarmah, D.K., Kulkarni,A.J.: Improved Cohort Intelligence A High Capacity, Swift and Secure Approach on JPEG Image Steganography.Journal of Information Security and Applications (Elsevier)**45**(5),90–106(2019)

[27] Liu, H.H.,Lee,C.M.:High-Capacity Reversible Image Steganography Based on Pixel Value Ordering. EURASIP Journal on Image and Video Processing (Springer)**11**(5),209-221(2019)

[28] Kaw,J.A., Loan,N.A, Parah,K.A, Muhammad,K.A, Sheikh,J.A.,Bhat,G.A.:A Reversible and Secure Patient Information Hiding System for IoT Driven e- Health. International Journal of Information Management (Elsevier)**45**(5), 262–275, (2019)

[29] Zhang, J., Lu,W.,Yin, X.,Liu, W.,Yeung, Y.:Binary Image Steganography based on Joint Distortion Measurement. Journal of Visual Communication and Image Recognization (Elsevier)**58**(4), 600–605(2019)

[30] Li, M., Mu,K.,Zhong, P.,Wen, J.,Xue,Y.:Generating Steganography Image Description by Dynamic Synonym Substitution. Signal Processing (Elsevier)**164**(3), 193–201(2019)

[31] Maniriho, P.,Ahmad, T.:Information Hiding Scheme for Digital Images Using Difference Expansion and Modulus Function.Journal of King University Computer and Information Sciences (Elsevier) **31**(6)335–347(2019)