International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 2, February 2021)

Securing Information via Image Steganography using Least Significant Bit Method and Multiple XOR Operations on MSB

Vardichand Parmar[1], Umesh Joshi[2]
[1]M.Tech Scholar, [2]Assistant Professor, [1,2]CSE, Oriental College of Technology, Bhopal, India

***Abstract*- The Least Significant Bit (LSB) strategy is an extremely well-known technique in steganographic images' spatial space. This technique is generally utilized and keeps on being created to date due to its points of interest in steganographic image quality. Be that as it may, the customary LSB strategy is exceptionally straightforward and unsurprising. It needs an approach that increases the security of concealed messages along these lines. This research work proposes a basic and secure approach to hide messages in the least Significant Bit methods. Multiple times the XOR activity is done to encode the message before it is installed on the LSB. Three Most Significant bits are utilized as keys in XOR operations to encourage the cycle of encryption and unscrambling of messages. The aftereffects of this research demonstrate that this technique gives security to a straightforward message activity. The impalpability nature of the stego image is likewise brilliant, with a Peak Signal to Noise Ratio (PSNR) esteem over 50 dB.**

***Keywords*— PSNR, Steganography, Least Significant Bit, Most Significant Bit, XOR**

I. INTRODUCTION

Innovation in the Internet era gives people numerous advantages, particularly in getting or trading data, picking up, working, etc. One of the issues on the Internet is security and information protection. Various methods have been useful in giving security; for instance, cryptography, Steganography, watermarking, and progressed marks [1] [2] [3]. Watermarking and Steganography are portions of the investigation of disguising data on other media like anything inside envelop [4]. What makes a difference is its ability, where Steganography is used to cover messages while watermarking is used to ensure copyright. Data stowing ceaselessly in the image is segregated into two regions, accurately spatial space and repeat space. In the repeated area, the message is concealed by first changing the cover picture. Changes that have been comprehensively used are DCT, DWT, and SVD [3] [5]. The mystery message is installed authentically in the spatial territory by changing the cover picture's pixel regard. LSB and MSB are the most standard strategies in a spatial region [6] [7].

Cryptography is a technique for changing a message's state, so it can not be scrutinized direct. The AES, DES, RSA, Vigenere, MD5 figurings are celebrated counts used in cryptography [2] [7] [8]. Vigenere is a robust and mind-boggling cryptographic estimation in message encryption, where XOR executives are used as one of the top parts [5]. XOR operation has also applied a huge steganographic assessment to improve message security [9] [10]. Given the development continues propelling, more investigation is making a crossbreed methodology of Steganography and cryptography to give layered security to messages [11]. This assessment joined steganographic methods with LSB and cryptography by changing the substance of messages with XOR overseers subject to the three most essential pieces.

II. RELATED WORK

Nowadays, everyone works on steganography systems to cover their belongings using pictures. I have explored various such algorithms and many techniques designed to hide important information behind a towering image while not making any kind of mark.

W. S. Sari et al. (1995) built up a mix of DCT-DWT Steganography with OTP cryptography in imaging media. Their test outcomes indicated better nature of permeability, contrasted with existing techniques. It is sealed by the tests performed on 20 dim pictures estimating 512x512 in execution tests utilizing MSE, PSNR, and N.C. Test outcomes affirm that DCT-DWT-OTP produces PNSR over 50 dB, while N.C. for all images is 1. The least PSNR is 50.9910 dB, and the most elevated is 51.3053 dB. Execution tests were additionally tried utilizing MSE and N.C. Given the relative consequences of the examinations [13], [14], and [24], the proposed strategy recommends that PSNR scores are higher than the past three investigations [1].

K. Joshi et al. (2015) created steganographic strategies for spaces utilizing XOR administrators. Message input is finished with the initial two XOR capacities set at one and eighth pieces and the second at 2, seventh piece. The exhibition result is then analyzed and utilized as a message input message.

The cover picture is a 512 * 512 dark picture with three message sizes, 1024 pieces, 2048 pieces, and 4096 pieces. The measure of PSNR got is roughly 69 dB with a message length of 4096 pieces [6].

K. Joshi and R. Yadav (2016) proposed steganographic systems and LSBs incorporated with XOR administrators. The message is stuck to three more modest pieces. There before the encryption of mystery, messages made XOR work. With the dim cover's picture size, 256 * 256 pixels can be inserted with a sizeable 196608-piece message. Simultaneously, the measure of PSNR found in high implanting is more than 37 dB [7].

A. U. Islam et al. (2016), proposing Steganography in photography utilizing a fracture cycle in pieces 5 and 6. In the event that there is a distinction in pieces 5 and 6 which is equivalent to the bits of secret data, at that point no change is conceivable. Meanwhile, if there is a distinction in worth, the worth changes to fifth piece with the goal that the estimation of the distinction relates to the base an incentive in the classified data. The cover picture utilized is a dark picture and shading picture with size 512 * 512. Along these lines, PSNR 51.17977 dB in Lena's grayscale picture and PSNR 52.3438 in Lena's shading picture, with a stacked heap of 262144 pieces [9].

R. D. Ardy et al. (2017) proposed arrangement in which they consolidate three calculations: RSA, Vigenere Cipher and Message Digest 5 (MD 5). The mix of TheMD5 and Vigenere improves result than simply hash work. The mix of this capacity is done in the picture and the picture document name: vigenere and RSA and coded. The closeness of MD5, Vigenere and RSA is a cryptographic calculation, so the calculation has been effectively coordinated. This calculation can shield you from picture control or different picture changes. Despite the fact that the pixels have changed marginally, as proven by the PSNR estimation of up to 86.7532 dB, the calculation effectively distinguishes pixel picture advances and document name changes to the computerized signature picture. Along these lines, if the cycle of picture move happens a twisting that is harming or deluding the picture, this calculation can make security more secure. The proposed strategy is likewise tried with different assaults to gauge the dependability of computerized marks, different assaults utilizing obscuring, salt, and pepper, Gaussian channels. As far as hostile outcomes, the littlest change that has happened in an obscuring assault than the best PSNR is 86.7532 dB. The test outcome demonstrates a slight change in the picture, and the record name can influence the approval result [10].

A. Winarno et al. (2017) This paper proposes the utilization of Discrete Cosine Transform (DCT) in light of 8x8 squares to change the first picture from an area over to a typical space. The impact of the DCT change will deliver A.C. what's more, D.C. coefficients Next, DC coefficients are gathered in the framework to be changed over through DWT. The DWT change impact produces four subbands. The L.L. subband is then chosen to embed copyright as a double picture with a specific measure of watermark power. The last advance in changing over DWT-DCT transformation is to create a picture with a watermark. In view of the aftereffects of this examination, elevated levels of obscurity were affirmed by PSNR and MSE [11].

G. Ardiansyah et al. (2017) Social organizations, for example, the Internet are advancing, quicker, and less expensive, to utilize data trade. This can build the odds of secret data being taken and misused by unapproved people. This investigation proposed a blend of two Steganography areas combined with Cryptography which expected to make private data safer and difficult to reach to unapproved people. Messages are scrambled utilizing the 3-DES strategy [12].

A. Setyono et al. (2017) In this investigation, the StegoCrypt cycle is proposed utilizing a blend of Discrete Wavelet Transform (DWT) and One-Time Pad (OTP). The cover picture in size 512 * 512 is changed over by Wavelet transformation of four levels. In the first to third level, subband L.L. is chosen to procure LL3 subband. In the fourth stage, LL3 is then changed over to HH4 subband with the assistance of wave transformation [13].

E. J. Kusuma, et. Al (2017) additionally proposes message inserting in the region at the edge of the picture. In his exploration he joined steganography methods utilizing LSB procedures and cryptographic strategies utilizing DES. Before the image message is entered, the message is encoded utilizing the DES technique. The cover picture utilized is a shading picture with a size of 1024 * 1024, and this message is additionally a shading picture with a size of 64 * 64. As per the consequences of this investigation, the normal estimation of PSNR 72.21584 dB, found in five sorts of pictures [15].

C. Irawan, et.al. (2017) proposed a blend of steganographic and cryptographic strategies, with messages scrambled utilizing the OTP strategy preceding LSB arrangement. Improving the intangibility and secure installing of messages is done at the edge of the picture. The area of the edge of the picture is done as Canny.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 2, February 2021)

The pre-owned cover picture composed JPEG with a size of 11035 bytes, and the message passed on by 1024 bytes got PSNR 69.1106 dB. Furthermore, the nature of stego picture is additionally estimated with histogram, where the cover picture of the histogram and the picture of stego are the equivalent [16].

YaniParti Astutiet.al. (2018) proposed a picture security arrangement utilizing Least Significant Bit (LSB). Notwithstanding, the customary LSB technique is extremely straightforward and unsurprising. It requires an approach to improve the security of concealed messages thusly. This investigation recommends a basic and safe approach to conceal messages in LSB procedures. Multiple times the XOR activity is performed to scramble the message prior to installing it to LSB. To improve the encryption cycle and eliminate text informing, three MSB sections are utilized as keys for XOR usefulness. The consequences of this investigation demonstrate that this technique gives security of messages a lot simpler activity. Stego picture perceivability quality is likewise incredible with a PSNR esteem more than 50 dB [17].

Touhid Bhuiyan et.al. (2019) Author Suggested a definite investigation of the proposed LSB substitution calculation incorporates a study directed by PSNR-and MSE. The test outcomes show an awesome commotion level reach (PSNR) (55.90 dB of 65,536 pieces of message inside the cover picture of 256x256 pixels) and mean a square worth (MSE) indicating less ill-advised and extra wellbeing. The aftereffects of the examination demonstrate that the proposed system gives greater security in the sharing of secret data, contrasted with other related strategies [18].

J. R. Jayapandiyan et.al. (2020) Auhtor proposed a technique chips away at a nearby area and makes a private message that incorporates two classes. The outcomes are contrasted and the LSB calculation and contrasted with Peak Signal with Noise Ratio (PSNR), Mean Square Error (MSE) and Root Mean Square Error (RMSE) qualities to demonstrate that the proposed calculation works better in the scrambled content picture on the cover picture [19].

Table 2.1:
Comparison of literature Survey

S.No	Year	Author	Paper Title	Method	PSNR Results
1.	2020	J.R.Jayapandiyan[19]	Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization	Enhanced LSB	55.0dB
2.	2019	Touhid Bhuiyan[18]	An Image Steganography Algorithm using LSB Replacement through XOR Substitution	LSB eith XOR operation	55.90dB
3.	2018	YaniParti[17]	Simple and secure image steganography using LSB and triple XOR operation on MSB	LSB with three times XORoperation	50dB
4.	2017	A.winarno[11]	Image Watermarking using Low Wavelet Subband based on 8×8 Sub-block DCT	DWT-DCT	42dB
5.	2016	A.U.Islam[9]	An Improved Image Steganography Technique based on MSB using Bit Differencing	LSB with XOR operator	52.34
6.	2015	K.Joshi[7]	New Approach Toward Data Hiding using XOR for Image Steganography	XOR Operator	69dB
7.	1995	W.S.Sari[1]	A Good Performance OTP Encryption Image based on DCT-DWT Steganography	DCT -DWT-OTP	51.30dB

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 2, February 2021)

III. PROPOSED WORK

This work presents information concealing procedures by joining encryption and Steganography to accomplish high quality secret images.

- Proposed algorithm is a comprise proposed Encryption / decryption Algorithm and proposed Steganography Algorithm.
- Proposed encryption algorithm is designed in a way that it can encrypt both text file as well as image file.
- Proposed algorithm works on bit manipulation.
- It is block cipher symmetric key algorithm.

3.1 Steps of Steganography algorithm

Step 1. Convert the plaintext into binary format and make it multiple of 3.

Step 2. Make it multiple of 3 by padding '0' at the end of plaintext.

Step 3. Now, divide the cover image into eight categories based on 3 MSB and initialize eight counters of each category by zero,

Category 1 having MSB 000, counter C000 = 0
Category 2 having MSB 001, counter C001 = 0
Category 3 having MSB 010, counter C010 = 0
Category 4 having MSB 011, counter C011 = 0
Category 5 having MSB 100, counter C100 = 0
Category 6 having MSB 101, counter C101 = 0
Category 7 having MSB 110, counter C110 = 0
Category 8 having MSB 111, counter C111 = 0

Step 4. Now, from the fifth pixel of cover image compare whether the message bit is equal to pixel LSB if not increment the counter of that category in which that pixel lie.

Step 5. if the percentage of change pixel is more than 50 % in any category then all the message bits in that category are replaced by LSB of Pixel after inverting the bits and if the change pixel is not more than 50% then just replace the message bit with the LSB bit of pixel without inverting.

Step 6. Repeat step 4 and 5 for all message bits.

Example:

Let's the binary plain text is 10110… and the cover image pixel be 10110000, 10100100, 10000000, 1011000, 10101101,….

Now, apply LSB method by replacing least significant bit of pixels by plaintext bits.

New pixel will be:

1011000**1**, 10100100, 1000000**1**, 101100**1**, 1010110**0**,….

Now, if we group all pixels on the basis of first 3 MSB of pixels

So, as shown in example there are 4 pixels belong to 101 group and out of them 3 pixels are changed.

Now, as the changing percentage is more than 50% therefore, we invert all LSB of this group.

Hence, the new pixel will be:

1011000**0**, 10100101, 1000000**1**, 101100**0**, 1010110**1**,.

Now on comparing original pixels with the embedded pixels out of four only one pixel is changed.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 2, February 2021)

3.2 Proposed Flowchart

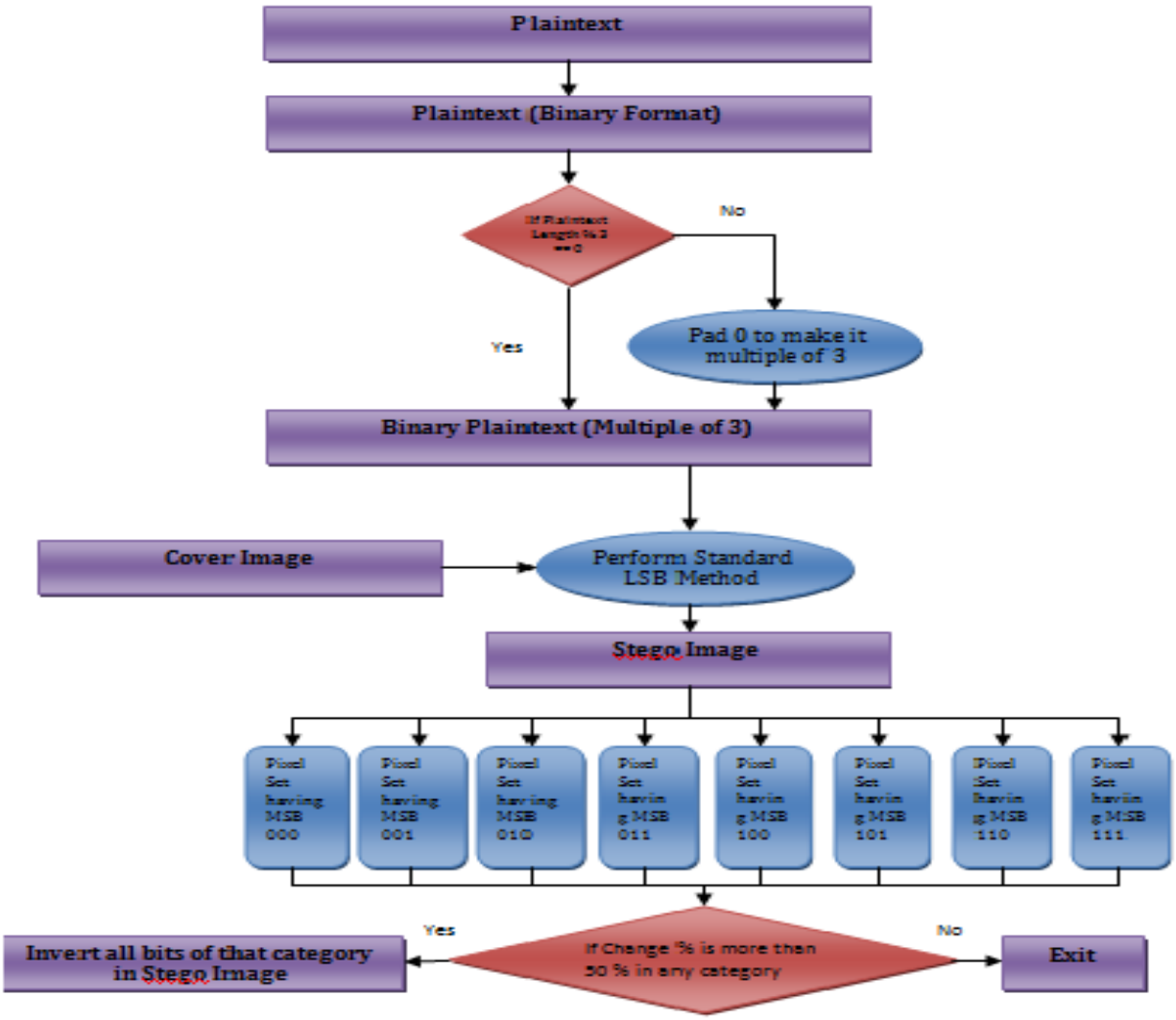

Figure.3.1: Block diagram of Proposed Steganography algorithm

IV. Results And Discussion

The experiments performed in this study used six gray images as a cover image and a Secret text message I love my India!!; see Figure 4.1 as cover images and Figure 4.2 as the text message. Photo cover is of size, 256 * 256. Here is the cover image used in this study:

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 2, February 2021)

(i)

(ii)

(iii)

(iv)

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 2, February 2021)

(v) **(vi)**

Figure 4.1: Cover image used {(a) cameraman.bmp(b)F16.bmp (c) Peppers.bmp (d) Barbara.bmp (e)Pentagon.bmp (f) Lena.bmp }

I love my India!!

Figure 4.2: Secret Text message

An experiment of embedding the message using the method proposed above. Here is the stego Image generated, shown in Figure 4.3.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 2, February 2021)

(i)

(ii)

(iii)

(iv)

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 2, February 2021)

(v) **(vi)**

Figure 4.3: Stego image Results {(a) cameraman.bmp(b)F16.bmp (c) Peppers.bmp (d) Barbara.bmp (e)Pentagon.bmp (f) Lena.bmp }

People cannot tell the difference between a stego image (Figure 4.3) and a cover image (Figure 4.1). After all, does this mean that stego's image is correct? So that required a stego image quality tool above. In this study, PSNR, MSE, and image histogram were used to measure stego image quality. The rating is made by comparing the cover image with the image of the stego. Calculating the MSE used for Formula 1 and calculating the PSNR used for Formula 2.

$$MSE = \sum_{x=1}^{X-1} \sum_{y=1}^{Y=1} \| A_i(x,y) - S_i(x,y) \| \qquad (1)$$

$$PSNR = 10log_{10} \left(\frac{256-1}{MSE} \right) \qquad (2)$$

Where x,y is the image size,A_i is the cover image,S_i is the stego image

Result:

Table 4.1 : Comparison of PSNR Value

Algorithm	PSNR Value
Standard Algorithm (LSB Method)	66.83
Base Paper(2018)	66.18
Proposed Algorithm	67.12

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 2, February 2021)

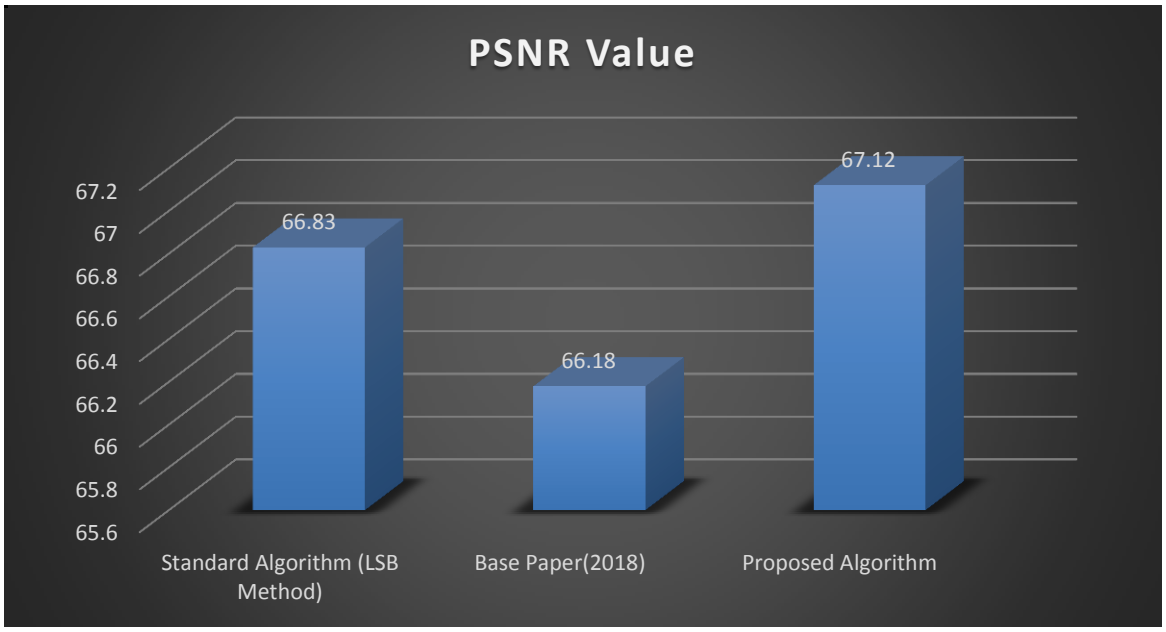

Figure 4.4: Comparison between PSNR value of Standard LSB algorithm, Base paper algorithm, and the proposed algorithm

Cover File Size: Cover File size is constant for all three algorithms; that is, It should be greater or equal to ((8/3) * PlainText size in Bytes

The proposed Steganography algorithm guarantees that its PSNR value is always higher than the Standard LSB Method in the best or average case and equal in the worst case. Its PSNR value cannot be less than the Standard Algorithm.

The below table shows the PSNR and MSE results of the stego images.

Table 4.2 :
Comparison of Various images PSNR and MSE values

Image	PSNR	MSE
Cameraman	90.049	6.430
F16	80.969	0.001
Peppers	81.495	0.0004
Barbara	81.557	0.0004
Pentagon	81.941	0.0004
Lena	82.341	0.0003

It knows the effectiveness of the release of the results. Return the message image from the stego image also measured using the coefficient of integration (CoCr). A CoCr value equal to 1 indicates that the extraction process is well performed. If the CoCr value is between 0 to 1, then there are message fragments that can be omitted, making a CoCr using a formula.

$$\mathbf{CoCr} = \frac{\sum_x \sum_y (\boldsymbol{M_0} - \overline{\boldsymbol{M_0}})(\boldsymbol{M_r} - \overline{\boldsymbol{M_r}})}{\sqrt{\sum_x \sum_y (\boldsymbol{M_0} - \overline{\boldsymbol{M_0}}) \sum_h \sum_g (\boldsymbol{M_r} - \overline{\boldsymbol{M_r}})}} \quad (3)$$

Where $\sum_x \sum_y$ is the sum of bits of text message
M_0:Original message image
M_r: Recover message image

Based on the scale using the formula (3), we get all stego images. It means that the extraction process works well.

V. Conclusion

With projectiles such as the growth of technology in computers and the Internet, data security is essential in modern life. This work studied many cryptographic algorithms, developed an advanced algorithm, and analyzed it with a base paper algorithm [13]. Steganography has been known and practiced for centuries. In the past, people used methods designed to hide data where data was stored within a particular Host file or object. But with the advent of digital Steganography, the whole process of hiding data has changed. Digital Steganography has surpassed traditional methods in the modern world of computers and the Internet. With the advent of new ways, attackers have developed new code-breaking techniques. This, in turn, leads to the development of more secure, more complex mechanisms. This paper aims to create an algorithm that provides additional security for encryption by encrypting it using a new fast encryption algorithm and hiding it in other full-size image files on the Internet. Our proposed Steganography ensures that its PSNR value remains higher than the standard LSB method in the best or most moderate condition and is highly proportional. Its PSNR value cannot be below the Standard Algorithm.

VI. Application

The proposed algorithm can be used anywhere in the world where the text is transferred from one end to another via public networks.

VII. Future enhancement

Progress in this work is possible in the future in many ways:

- First, this security system encrypts and encrypts a secret text message. Now, if this last message is encrypted and sent as a private message, the attacker will not receive the original message.
- Second, this method can also be upgraded to compress the original encrypted message file and encrypt more than one compressed, encrypted files and upload them randomly.

REFERENCES

[1] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi and h. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," TELKOMNIKA (Telecommunication Computing Electronics and Control) , vol. 15, no. 4, pp. 1987-1995,

[2] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia, "Application of LSB Based Steganographic Technique for 8-bit Color Images," World Academy of Science, Engineering and Technology, 2009.

[3] Yu Qiudong, X.-W. L., "A New LSB Matching Steganographic Method Based on Steganographic Information Table," Second International Conference on Intelligent Networks and Intelligent Systems, China, 2009, pp. 362 - 365.

[4] S. S. Divya, M. Ram Mohan Reddy, "Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography," International Journal of Scientific & Technology, research Volume I, Issue 6, July 2012 ISSN 2277-8616 68 ijstr©20 12 www.ijstr.org.

[5] Bing Song and Zhi-hong Zhang, "One improved LSB steganography algorithm," Proc. SPIE 8784, Fifth International Conference on Machine Vision (ICMV 2012): Algorithms, Pattern Recognition, and Basic Technologies, 87840V (March 13, 2013).

[6] K. Joshi, P. Dhankhar and R. Yadav, "A New Image Steganography Method in Spatial Domain Using XOR," in Annual IEEE India Conference (INDICON), New Delhi, 2015.

[7] K. Joshi and R. Yadav, "New Approach Toward Data Hiding using XOR for Image Steganography," in International Conference on Contemporary Computing (IC3), Noida, 2016

[8] P. S. Sapra and H. Mittal, "Secured LSB Modification using Dual Randomness," in International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, 2016.

[9] A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali and M. Naeem, "An Improved Image Steganography Technique based on MSB using Bit Differencing," in International Conference on Innovative Computing Technology (INTECH), Dublin, 2016.

[10] R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto, "Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)," in International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICONSONICS), Yogyakarta, 2017.

[11] A. Winarno, D. R. I. M. Setiadi, A. A. Arrasyid, C. A. Sari and E. H. Rachmawanto, "Image Watermarking using Low Wavelet Subband based on 8×8 Sub-block DCT," in International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, 2017.

[12] G. Ardiansyah, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto, "Hybrid Method using 3-DES, DWT and LSB for Secure Image Steganography Algorithm," in International Conference on Information Technology, Information System, and Electrical Engineering (ICITISEE), Yogyakarta, 2017.

[13] A. Setyono, D. R. I. M. Setiadi and Muljono, "StegoCrypt Method using Wavelet Transform and One-Time Pad for Secret Image Delivery," in International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2017.

[14] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi and C. A. Sari, "A Performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size," in International Seminar on Application for Technology of Information and Communication (ISemantic), Semarang, 2017.

[15] E. J. Kusuma, O. R. Indriani, C. A. Sari, E. H. Rachmawanto and D. R. I. M. Setiadi, "An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption," in International Conference on Innovative and Creative (ICITech), Salatiga, 2017.

[16] C. Irawan, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption," in International Conference on Informatics and Computational Sciences (ICICoS), Semarang, 2017.

[17] Y. P. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB," 2018 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, 2018, pp. 191-195, doi: 10.1109/ICOIACT.2018.8350661.

[18] T. Bhuiyan, A. H. Sarower, R. Karim and M. Hassan, "An Image Steganography Algorithm using LSB Replacement through XOR Substitution," 2019 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, 2019, pp. 44-49, doi: 10.1109/ICOIACT46704.2019.8938486.

[19] J. R. Jayapandiyan, C. Kavitha and K. Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization," in IEEE Access, vol. 8, pp. 136537-136545, 2020.

[20] https://searchsecurity.techtarget.com/definition/cryptography.