IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-9, Sept. 2018 E-ISSN: 2347-2693

An Approach of LSB- Symmetric Cryptography to Secure Classified Text Content

[1*]R. Sharma, [2]A. Dwivedi, [3]V. Namdeo

[1]M.Tech. Scholar SRKU, Bhopal, India
[2]CSE Dept, SRKU, Bhopal, India
[3]HOD. CSE Dept, SRKU, Bhopal, India

[*]*Corresponding Author: rhlshrm@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 18/Sept/2018, Published: 30/Sept/2018

Abstract- The proposed idea provides information that obscures the idea with the combination of cryptography and steganography. Proposed ideas are important to support verification, confidentiality and fairness. To achieve these effects, the main idea is to use a symmetric cryptography system for privacy and validation security, mainly an incomplete reliability key supported by the steganography method. The proposed idea is primarily dependent on the security with the coding of the emission data is covered in the first phase and the data in the next phase encrypted discharge, so that it ensures a double security for a discharge date. Exhibited steganography idea, image or content as the information first (as a picture) coded and packaged by correlation with minimal image collective size after compressed data were shaken by symmetric cryptographic process using a private key of 128 bits of coded data, this private key splits via a private channel between the sender and the payee, and finally inserts encrypted data into the bitplanes of the title image using the smallest noteworthy piece (LSB) of the standard stereographic procedure. To achieve a high security strategy, the proposed steganography strategy has used random numbering (RAND) which selects an irregular LSB from the envelope. The results shown demonstrate the implementation and feasibility of the proposed proposal for inclusion of the peek flag on sedimentation rate (PSNR), compound and entropy.

Keywords - Decryption, Encryption, Internet, Steganography, Security etc.

I. INTRODUCTION

With the rise of the internet, communication through digital media has become more and more popular. All the personal and commercial interactions happen through internet, where digital media is the major source of communication. When confidential data of organizations and corporates are communicated, security of the information is a major concern. They have to protect their data from leakage. But because of the wide access of internet to the common man, digitally transferred data has a high risk of being attacked or destroyed. Thus the security in transmission of information is questioned.
understand the data. A third person, even if he is able to see the data, cannot read or understand the information. The message will be encrypted by the sender and it can be decrypted only by the receiver with the help of a previously agreed upon key.

Steganography is an art of secret communication of data. i.e., the data which is being transmitted is hidden from a third person. In cryptography, the secret message is kept in an unreadable form to a third person, whereas in steganography, the existence of the message is kept as a secret from the third person.

II. RELATED WORK

In [1] a multi secure and power of restorative picture based steganography conspire is proposed. This proposed strategy gives a productive and capacity security component for the insurance of computerized medicinal pictures.

In [2] is worried about executing Steganography for pictures, with a change in both security and picture quality. The one that is actualized here is a variety of plain LSB (Least Significant Bit) calculation. The stego-picture quality is enhanced by utilizing bit-reversal method.

In [3] exhibited system before installing the mystery data into a picture, the mystery data has been compacted utilizing the wavelet change procedure. The got bits after pressure are encoded utilizing quantum doors.

In [4] the proposed work shows a remarkable system for Image steganography in light of the Data Encryption Standard (DES) utilizing the quality of S-Box mapping and Secrete key.

In [5] I have investigated that creator proposes three indigenous strategies as a variation of Cipher Block Chaining (CBC) mode for picture encryption by considering three diverse crossing way.

III. PROPOSED WORK

In this section, consider a picture document as a cover picture to stow away discharge message. The execution of framework will just concentrate on Proposed Encryption Process as another method of symmetric cryptography and Least Significant Bit (LSB) as one of the steganography procedures as said in beneath (see figure 1). In cryptography proposed encryption and decoding process depend on symmetric cryptography idea. As we realize that symmetric cryptography are speedier as think about lopsided cryptography method. The minimum noteworthy piece (LSB) of a couple or the greater part of the bytes inside a picture is spoiled to a touch of the secret message. Advanced pictures are for the most part two sorts one is 8 bit pictures and second is 24 bit pictures. Three bits of data of every pixel can be included 24 bit pictures pixels, one in every one LSB area of the three 8 bit esteems. Rising or reducing the incentive by modifying the LSB does not adjust the presence of the picture; much so the resultant stego picture looks practically same as the cover picture. In 8 bit pictures, one piece of data can be covered up. In the event that the LSB of the pixel estimation of cover picture C(i,j) is equivalent to the message bit m of mystery back rub to be implanted, C(i,j) stay unaltered; if not, set the LSB of C(i, j) to m. The message installing method is given beneath

S(i,j) = C(i,j) - 1, if LSB(C(i,j)) = 1 and m = 0
S(i.j) = C(i,j), if LSB(C(i,j)) = m
S(i,j) = C(i,j) + 1, if LSB(C(i,j)) = 0 and m = 1where LSB(C(i, j)) remains for the LSB of cover picture C(i,j) and m is the following message bit to be embedded.S(i,j) is the stego picture. As it is at this point every pixel is finished up of 3 bytes comprising of either a 1or a 0. For instance, accept in the event that anyone can shroud a classified message in 3 pixels of a cover picture (24-bitcolors). Expect the first 3 pixels are:[16]
(100000110 10001110 11100011)
(01111110 11011110 11111000)
(10001001 11100101 11101001)
A steganography could shroud the character "K" which has an area 75 in ASCII set and have a twofold portrayal " 01001011", by adjusting the channel bits of pixels

.(11101010 11101001 11001010)
(01100110 11001011 11101000)
(11001001 00100100 11101001)

For this case, just a single bits should have been adjusted to include the character effectively. The resultant adjustments that are finished to the slightest noteworthy bits (LSB) are minor to be prestigious by the stripped human eye, so the private message is electively hide. The advantage of LSB strategy is straightforwardness amid implanting and numerous techniques utilize these strategies [10]. LSB inserting strategy additionally permits expansive perceptual straightforwardness.

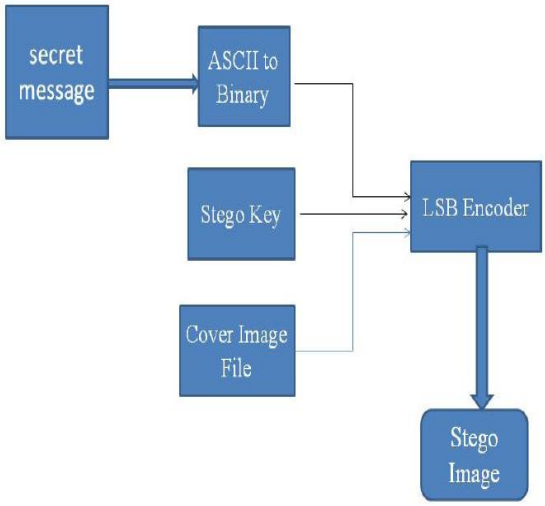


Figure 1: Steganography Technique

Introduced Idea: It depends on steganography and cryptography associatively, where at first it checks sort of mystery message if discharge message (SM) is content (T) at that point it pass encoding (E) prepare and if mystery message is picture (I) at that point it go to pressure (C) procedure to diminish the measure of the first picture to look after proficiency. This pressure procedure calls wavelet change since wavelet change gives lossless change (LT) where unique data can be returning in the wake of uncompressing. Once the examination done packed data passed go to encoding process. Encoding process call key (K) esteem to deliver figure (CP) esteem these figure esteem go to steganography procedure (ST). In the proposed idea steganography strategy utilizes slightest noteworthy bits (LSB) handle. Minimum noteworthy bits handle select LSB from cover picture (CI) by utilizing randomization (R) prepare and inserted figure an incentive in cover picture to created stego picture (STI).

Proposed Encryption Method: Figure 2 is demonstrating engineering of proposed encryption prepare. This design are indicating finished one round process. All the procedure is characterized well ordered in encryption calculation venture in next area.

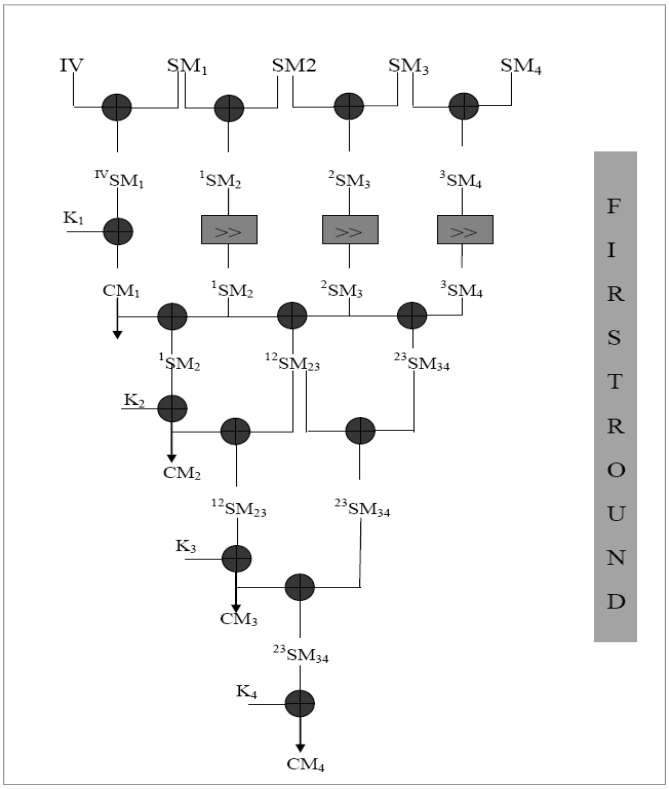


Figure 2: Proposed Encryption Architecture

Encryption_ Algorithm :
1. Input Secrete Message (SM) of 128 bits
2. Input Key (K) of 128 bits
3. Input Initialization Vector (IV) of 32 bits
4. Divide Secrete Message (SM) into four sub secrete message of equal size like (SM_1, SM_2, SM_3, SM_4)
5. Divide Key (K) into four sub key of equal size like (K_1, K_2, K_3, K_4)
6. Perform XOR in following way

$IV \text{ XOR } SM_1 = {}^{IV}SM_1$
$SM_1 \text{ XOR } SM_2 = {}^{1}SM_2$
$SM_2 \text{ XOR } SM_3 = {}^{2}SM_3$
$SM_3 \text{ XOR } SM_4 = {}^{3}SM_4$
${}^{IV}SM_1 \text{ XOR } K_1 = CM_1$

7. Perform 2 bits right circular shift in following way

$(>>2)\ {}^{1}SM_2 = {}^{1}SM_2$
$(>>2)\ {}^{2}SM_3 = {}^{2}SM_3$
$(>>2)\ {}^{3}SM_4 = {}^{3}SM_4$

8. Perform XOR in following way

$CM_1 \text{ XOR } {}^{1}SM_2 = {}^{1}SM_2$
${}^{1}SM_2 \text{ XOR } {}^{2}SM_3 = {}^{12}SM_{23}$
${}^{2}SM_3 \text{ XOR } {}^{3}SM_4 = {}^{23}SM_{34}$
$K_2 \text{ XOR } {}^{1}SM_2 = CM_2$
${}^{12}SM_{23} \text{ XOR } {}^{23}SM_{34} = {}^{23}SM_{34}$
$CM_2 \text{ XOR } {}^{12}SM_{23} = {}^{12}SM_{23}$
$K_3 \text{ XOR } {}^{12}SM_{23} = CM_3$
$CM_3 \text{ XOR } {}^{23}SM_{34} = {}^{23}SM_{34}$
$K_4 \text{ XOR } {}^{23}SM_{34} = CM_4$

9. Combine CM_1, CM_2, CM_3, and CM_4 to get Cipher Message (CM)
10. Repeat above step 10 times
11. Exit

Proposed Decryption Method: Figure 3 is showing architecture of proposed decryption process. In this architecture one round process is shown. All the process is defined step by step in decryption algorithm in next section.

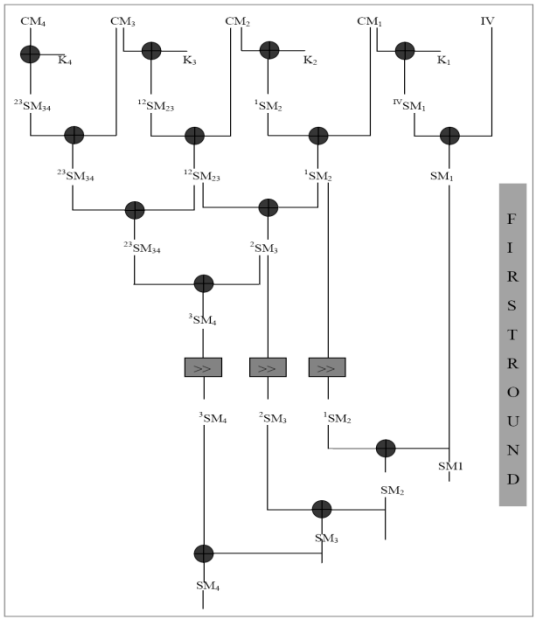


Figure 3: Proposed Decryption Architectur

Decryption_ Algorithm:
1. Input Cipher Message (CM) of 128 bits
2. Input Key (K) of 128 bits
3. Input Initialization Vector (IV) of 32 bits
4. Divide Cipher Message (CM) into four sub cipher message of equal size like (CM_1, CM_2, CM_3, CM_4)
5. Dive Key (K) into four sub key of equal size like (K_1, K_2, K_3, K_4)
6. Perform XOR in fowling way

$CM_4 \text{ XOR } K_4 = {}^{23}SM_{34}$
${}^{23}SM_{34} \text{ XOR } CM_3 = {}^{23}SM_{34}$
$CM_3 \text{ XOR } K_3 = {}^{12}SM_{23}$
${}^{12}SM_{23} \text{ XOR } CM_2 = {}^{12}SM_{23}$
$CM_2 \text{ XOR } K_2 = {}^{1}SM_2$
${}^{1}SM_2 \text{ XOR } CM_1 = {}^{1}SM_2$
$CM_1 \text{ XOR } K_1 = {}^{IV}SM_1$
${}^{IV}SM_1 \text{ XOR } IV = SM_1$
${}^{23}SM_{34} \text{ XOR } {}^{12}SM_{23} = {}^{23}SM_{34}$
${}^{12}SM_{23} \text{ XOR } {}^{1}SM_2 = {}^{2}SM_3$
${}^{23}SM_{34} \text{ XOR } {}^{2}SM_3 = {}^{3}SM_4$

7. Perform 2 bits right circular shift in reverse order in following way

Rev(>>2) $^3SM_4 = {}^3SM_4$
Rev(>>2) $^2SM_3 = {}^2SM_3$
Rev(>>2) $^1SM_2 = {}^1SM_2$

8. Perform XOR in following way
$^1SM_2$ XOR $SM_1 = SM_2$
$^2SM_3$ XOR $SM_2 = SM_3$
$^3SM_4$ XOR $SM_3 = SM_4$
9. Combine SM_1, SM_2, SM_3 and SM_4 to get SM
10. Repeat above step 10 time
11. Exit

Hiding Cipher Message Algorithm:

1. Input Cipher (CP) Message
2. Input Cover Image (CI)
3. Call Least Significant bits (LSB) process
4. Pass Cipher (CP) message and Cover Image (CI) to LSB
5. Call Randomization (LSB)
6. Produced Steog Image (SI)
7. Exit

Extraction of Cipher Message Algorithm:

1. Input Stego Image (SI)
2. Call Least Significant Bits (LSB) process
3. Call Randomization (LSB)
4. Extract Cover Image (CI) and Cipher Message (CM)
5. Exit

Wavelet Transform: Using wavelet transformation the data can be stored in less space, By doing so the memory space will be reduced and the data can be transferred easily [4].

Randomization Process: For randomization proposed concept used a technique known as MDSQR method. Step of this technique is as follow:

Start with an initial seed (e.g. a 2-digit integer and in our case it is again a random value).

Square the number.

Take the middle 2 digits.

MDSQR Method, example

$x_0 = 5497$

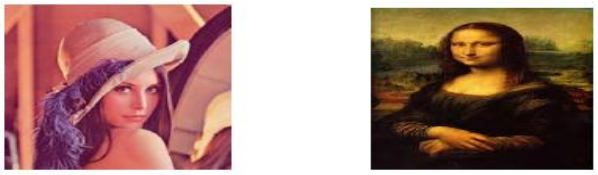
x_1: $5497^2 = 30217009$ ® $x_1 = 17$, $R_1 = 2170$

x_2: $2170^2 = 04708900$ ® $x_2 = 08$, $R_2 = 7089$

x_3: $7089^2 = 50253921$ ® $x_3 = 53$, $R_3 = 2539$

IV. RESULT ANALYSIS

Here results on two type of secret messages one is text based secrete message and second is image based secret message. Proposed system design and developed on MAT LAB. During results evaluation proposed system has selected various type of cover image like (lena.jpg, monalisa.jpg, see figure 4 (a) and (b)) which is highlighted as a "Input Cover Image" Similarly proposed system has various secret messages. For image there are five secrete images have used like (secret image 0.jpg, secret image 1.jpg, secret image 2.jpg, secret image 3.jpg, and secret image 4.jpg see figure (a), (b), (c), (d) and (e)) and for text secrete message there are four secrete (Text 1, Text 2, Text3 and Text 4 see Table 1) of various size have used all are define below.



.(a) Lena.jpg (b) Monalesa.jpg

Figure 4: Cover Image

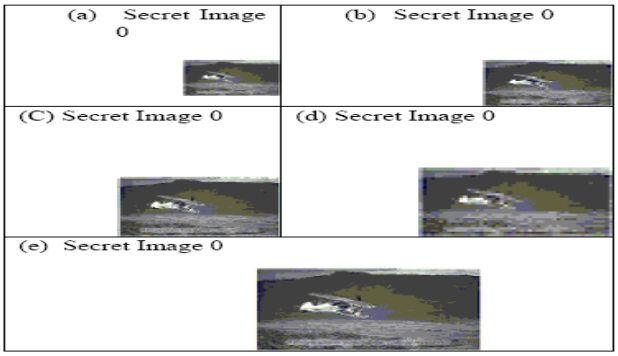


Figure 5: Secret Image

Table 1: Secret Text

Name	Secret Text Message
Text 1	Pls find details of my account is, username:ram, password:mohan.
Text 2	Pls find details of my account is, username:ram, password:mohan Pls find details of my account is, username:ram, password:mohan
Text 3	Pls find details of my account is, username:ram, password:mohan Pls find details of my account is, username:ram, password:mohan Pls find details of my account is, username:ram, password:mohan
Text 4	Pls find details of my account is, username:ram, password:mohan Pls find details of my account is, username:ram, password:mohan Pls find details of my account is, username:ram, password:mohan Pls find details of my account is, username:ram, password:mohan

For the experiment proposed system used three parameters which is following

- Peek Signal to Noise Ratio
- Correlation
- Entropy

Peek Signal to Noise Ratio (PSNR) Analysis: PSNR is defined as assume that N is the total number of pixels in the input or output image, MSE (Mean Squared Error) is calculated as [2,3 ,4]

$$PSNR = 10log_{10}\frac{(L-1)^2}{MSE}$$

Where L is the number of discrete gray levels
The value of PSNR should be greater for the better of the output image quality

Entropy Analysis: Entropy defined as follows [18]-[19].

$$H_e = -\sum_{k=0}^{G-1} P(k)\log_2(P(k))$$

Where:
He: entropy.
G: gray value of input image (0... 255).
P(k): is the probability of the occurrence of symbol *k*.
The Entropy is a used to measure the richness of the details in the output image.

Correlation Analysis: In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image/cipher image respectively. Firstly, we randomly select 2000 pairs of two adjacent pixels from an image. Then, we calculate their correlation coefficient using the following two formulas [30]:

Initially proposed system presenting results for image secret message where two cases has design and results are presented in table 2 to 4.

Test Case 1: When Cover image is Mahatmagandhi.Jpg and various Secret Image's.

Table 2: PSNR Analysis (Cover Image is Mahatmagandhi.Jpg)

Mahatmagandhi.Jpg	Input		PSNR	
	Input Data	Size	Existing Work	Propose Work
secret_Img0.bmp	Img1	2.5	43.837928	43.839592
secret_Img3.bmp	Img2	6.67	43.831132	43.836673
secret_Img4.bmp	Img3	9.03	43.817026	43.839397

Test case 2: Whene Cover image lena.Jpg and various Secrete Text.

Table 3: PSNR Analysis (Cover Image is Lena.jpg)

lena.jpg	Input		PSNR	
	Input Data	Size	Existing Work	Propose Work
secret_Img0.bmp	Img1	2.5	45.82392	45.824747
secret_Img3.bmp	Img2	6.67	45.818282	45.823471
secret_Img4.bmp	Img3	9.03	45.808756	45.828173

Table 4: Analysis of PSNR, Correlation and Entropy: (a)PSNR (b) Correlation (c) Entropy Analysis (Cover Image is cover.jpg)

Table 4(a)PSNR

Cover.Jpg	Input		PSNR	
	Input Data	Size	Existing Work	Propose Work
secret_image0.bmp	Img1	2.5	38.294831	38.29497
secret_Img1.bmp	Img2	3.55	38.292756	38.294973
secret_Img2.bmp	Img3	5.11	38.290274	38.294719

Key Space Analysis: Secret key space analysis mean key size or key length in byte that is used during proposed encryption and decryption. Hear proposed encryption and decryption have used 128 bits key size that mean any hacker will take to break this key in 2^{128} times by using brute force attack which is impossible. Another security feature in proposed steganography is randomization of LSB selection from cover image which is also providing security for proposed concept.

Table 4(b) Performance Correlation Analysis

Cover.Jpg	Input		Correlation	
	Input Data	Size	Base	Propose
secret_image0.bmp	Img1	2.5	0.429717	0.429758
secret_Img1.bmp	Img2	3.55	0.42962	0.430696
secret_Img2.bmp	Img3	5.11	0.428805	0.429971

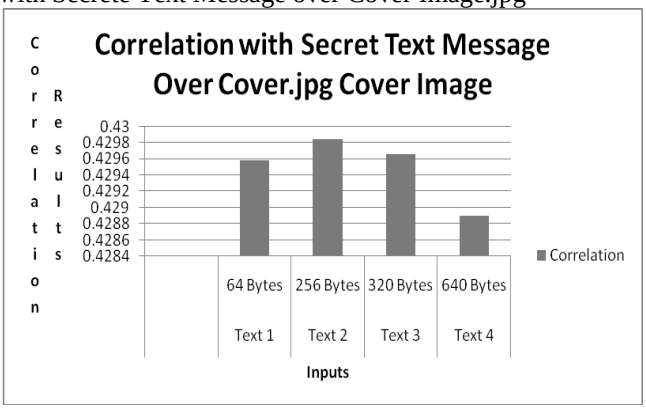
Table 4(c) Performance Entropy Analysis

Cover.Jpg	Input		Entropy	
	Input Data	Size	Base	Propose
secret_image0.bmp	Img1	2.5	7.768511	7.768668
secret_Img1.bmp	Img2	3.55	7.767985	7.768801
secret_Img2.bmp	Img3	5.11	7.767122	7.768805

Results Summary: For Image Secrete Message In Table 2 PSNR, Correlation and Entropy value are 35.638026, 0.749495 and 7.768702 by the proposed concept on the monaleesa.jpg as a cover image with secret image 0. Similarly In Table 3 PSNR, Correlation and Entropy value are 45.824747, 0.592466 and 7.768668 by the proposed

concept on the lena.jpg as a cover image with secret image 0. From the result it is observing that proposed concept are producing batter results in all aspect. And For Text Secret Message In Table 4 PSNR, and Correlation value are 35.637955, and 0.748887 by the proposed concept on the monaleesa.jpg as a cover image with secret text 1. Graph 1 to 5 is also showing the performance of the proposed concept with various secret text and image message over Cover.jpg and monaleesa.jpg cover image respectively. From the result it is observing that proposed concept are producing batter results in all aspect.

Grpah 1: Correlation Performance of Proposed Concept with Secrete Text Message over Cover Image.jpg



V. CONCLUSION & FUTURE SCOPE

Here in Steganography system has additionally utilized two methodologies one is the LSB Technique and second is the Pseudo-Random Encoding Technique on pictures to acquire secure stego-picture. Exhibited PSNR is demonstrating great picture nature of stego picture in LSB encoding. Our outcomes demonstrate that the LSB addition utilizing irregular key is superior to straightforward LSB insertion in the event of lossless pressure. The nature of the picture does not change excessively and is immaterial when implant the emit message into the cover picture and the discharge message is secured with the private key. In this way, it is difficult to hurt the emit message by unapproved character. The calculation is use for both 8 bit and 24 bit picture of the approx twofold size of cover as think about mystery picture, so it is anything but difficult to be actualizing in both grayscale and shading picture. This work concentrates on the approach like expanding the security of the message and expanding PSNR and diminishing the bending rate.

REFERENCES

[1] Nisha Kundu, Dr. Amadeep Kaur "Secure Approach to Audio Steganography"International Journal of Engineering Trends and Technology (IJETT) , 2017

[2] Sujarani Rajendran, Manivannan Doraipandian "Chaotic Map Based Random Image Steganography Using LSB Technique", International Journal of Network Security, 2017

[3] Reza tavoli, Maryam bakhshi, Fatemeh salehian, "A New Method for Text Hiding in the Image by Using LSB" (IJACSA) International Journal of Advanced Computer Science and Applications, 2016

[4] Rajalakshmi, Sowjanya.TP2, Hemanthkumar, "Image Steganography using H-LSB Technique for Hiding Image and Text Using Dual encryption method" SSRG International Journal of Electronics and Communication Engineering , 2015

[5] G Prabakaran, R. Bhavani, P.S. Rajeswari, "Multi secure and robustness for medical image based steganography scheme" International Conference on Circuits, Power and Computing Technologies (ICCPCT), 2013

[6] M.K Ramaiya. ; N.Hemrajani, ; , A.K Saxena. "Security improvisation in image steganography using DES" IEEE 3rd International on Advance Computing Conference (IACC), 2013

[7] N. Akhtar, ; P. Johri, ; S Khan, "Enhancing the Security and Quality of LSB Based Image Steganography" 5th International Conference on Computational Intelligence and Communication Networks (CICN), 2013

[8] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar "An Image Steganography Technique using X-Box Mapping" IEEE-International Conference On Advances In Engineering, Science And Management , 2012

[9] RigDas and Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding" IEEE, 2012

[10] Rengarajan Amirtharajan\ Anushiadevi .R2, Meena .y2, Kalpana. y2 and John Bosco Balaguru "Seeable Visual But Not Sure of It" IEEE-International Conference On Advances In Engineering, Science And Management, 2012

[11] G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan "Steganography Using Edge Adaptive Image" IEEE International Conference on Computing, Electronics and Electrical Technologies [ICCEET], 2012

[12] L.Jani Anbarasi and S.Kannan "Secured Secret Color Image Sharing With Steganography" IEEE, 2012

[13] Thomas Leontin Philjon. and Venkateshvara Rao. "Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT , 2011

[14] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana "A Competitive Study of Cryptography Techniques over Block Cipher" UKSim 13th IEEE International Conference on Modelling and Simulation, 2011

[15] Abhishek Gupta, Sandeep Mahapatra and, Karanveer Singh " Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm", 2011

[16] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application, (2011)

[17] Mohit Kulkarni, Maitreyee Phatak, Uma Rathod, Sudhir Prajapati, Mrs. Shivganga Mujgond "Efficient Data Hiding Scheme Using Audio Steganography", International Research Journal of Engineering and Technology (IRJET), 2016

[18] Manoj Kumar, Naveen Hemrajani and Anil Kishore Saxena "Security Improvisation in Image Steganography using DES" IEEE, 2012

[19] Sesha Pallavi Indrakanti , P.S.Avadhani, Permutation based Image Encryption Technique, International Journal of Computer Applications (0975 – 8887), 2011

[20] Qais H. Alsafasfeh , Aouda A. Arfoa, Image Encryption Based on the General Approach for Multiple Chaotic Systems Journal of Signal and Information Processing, 2011
[21] M.J.Thenmozhi, Dr.T.Menakadevi "A New Secure Image Steganography Using Lsb And Spiht Based Compression Method", International Journal of Engineering Research & Science (IJOER), 2016
[22] Amnesh Goel, Reji Mathews, Nidhi Chandra "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices" International Journal of Computer Applications (0975 – 8887) , 2011
[22] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, Image Encryption Using Affine Transform and XOR Operation ,International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011
[23] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption "2010 IEEE International Conference on Electronics and Information Engineering ICEIE, 2010
[24] ZHANG Yun-peng, ZHAI Zheng-jun, LIU Wei, NIE Xuan, CAO Shui-ping, DAI Wei-di "Digital Image Encryption Algorithm Based on Chaos and Improved DES" "Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA, 2009
[25] Obaida Mohammad Awad Al-Hazaimeh "Hiding Data in Images Using New Random Technique" IJCSI International Journal of Computer Science Issues, 2012
[26] Nada ElyaTawfiq "Hiding Text within Image Using LSB Replacement" IOSR Journal of Computer Engineering (IOSR-JCE), 2013
[27] Hyder Yahya Atown "Hide and Encryption Fingerprint Image by using LSB and Transposition Pixel by Spiral Method" International Journal of Computer Science and Mobile Computing, 2014
[28] Rajalakshmi, Sowjanya.TP, "Image Steganography using H-LSB Technique for Hiding Image and Text Using Dual encryption method" SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE), 2015
[29] Arun Karthick, Kavitha, Sivakumar, Surender, "A Hybrid Method For Covert Communication Using Steganography And Image Fusion", International Journal of Advances in Engineering & Technology, May, 2014.
[30] Manpreet Kaur, Vinod Kumar Sharma "Encryption based LSB Steganography Technique for Digital Images and Text Data", IJCSNS International Journal of Computer Science and Network Security, 2016

Authors Profile

Mr. R.Sharma pursed Bachelor of Engineering with Computer Science & Engineering branch from Rajeev Gandhi Technical University, Bhopal, MP and pursuing Master of Technology in Computer Science & Engineering specialization from Sarvepalli Radhakrishnan University, Bhopal, MP. His main research focuses in the field of computer security like: Cryptography, Network Security and Privacy.

Mr. A. Dwivedi Post Graduated in Master of Technology in Computer Science & Engineering specialization, *is working as an Assistant Professor in* Department of in Computer Science & Engineering Sarvepalli Radhakrishnan University, Bhopal, MP. His main research focuses in the field of Algorithm designing, computer security like: Cryptography, Network Security, Cloud Security and Privacy.

Dr. V. Namdeo is working Head of Department of in Computer Science & Engineering in Sarvepalli Radhakrishnan University, Bhopal, MP. Her main research focuses in the field of Algorithm designing, computer security like: Image processing,Network and Computer security,language Processing etc..

