Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Enhanced Steganography Technique for Hiding Text and Image Type Secret Messages

[1]Hemendra Singh Yadav, [2]Prof. Niresh Sharma

[1]M.Tech. Scholar RKDF, Bhopal, India

[2]Prof. CSE Dept, RKDF, Bhopal, India

Abstract: ***The proposed concept presents data hiding concept with the combination of cryptography and steganography technique. Proposed concepts are supporting authentication, confidentiality and partially integrity security principal. To achieve these securities principal proposed concept apply symmetric cryptography technique to support confidentiality and authentication security principal and partially integrity security principal supported through steganography technique. Proposed concept is based on security principal where encryption of the secrete information at first stage and encrypted secrete information hide in next stage so it is double security protection on single secrete information. Presented Steganography concept uses, image or text as the input data, initially it encrypted and compressed (if Image) through comparison to compact total size image after that this compressed information encrypted through symmetric cryptography technique with the help of 128 bits private key to produced encrypted information, this private key will share through private channel between sender and receiver and at last it embed encrypted information in the bit-planes of the cover image by using least significant bit (LSB) of standard steganography technique. To achieve high security proposed steganography technique used a random number generation (RAND) technique which will select random LSB from cover image. Presented results are showing the performance and effectiveness of the presented proposed work on the basis on Peek signal to noise ratio (PSNR), correlation and entropy.***

Keyword: Steganography, Security, Encryption, Decryption, Internet

I. INTRODUCTION

An information hiding system has been developed for confidentiality. However, in this paper, study an image file as a cover image to hide secrete message. The implementation of system will only focus on Proposed Encryption Process as a new technique of symmetric cryptography and Least Significant Bit (LSB) as one of the steganography techniques as mentioned in below (see figure 1). In cryptography proposed encryption and decryption process are based on symmetric cryptography concept. As we know that symmetric cryptography are faster as compare asymmetric cryptography technique. The least significant bit (LSB) of a few or all of the bytes within an image is tainted to a bit of the confidential message. Digital images are generally two types one is 8 bit images and second is 24 bit images. Three bits of information of each pixel can be added in 24 bit images pixels, one in each one LSB location of the three 8 bit values. Rising or lessening the value by altering the LSB does not alter the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden. If the LSB of the pixel value of cover image C(i,j) is equal to the message bit m of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to m. The message embedding procedure is given below-

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)) stands for the LSB of cover image C(i,j) and m is the next message bit to be embedded.S(i,j) is the stego image

As it is by now each pixel is complete up of 3 bytes consisting of either a 1or a 0.

For example, assume if anybody can hide a confidential message in 3 pixels of a cover image (24-bitcolors). Assume the original 3 pixels are: [1]

(100000110 10001110 11100011)

(01111110 11011110 11111000)

(10001001 11100101 11101001)

A steganography could hide the character ”K” which has a location 75 in ASCII set and have a binary representation ” 01001011”, by altering the channel bits of pixels.

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

For this case, only one bits needed to be altered to add the character successfully. The resultant alterations that are complete to the least significant bits (LSB) are tiny to be renowned by the naked human eye, so the confidential message is electively conceal. The benefit of LSB technique is simplicity during embedding and many methods use these methods [10]. LSB embedding technique also allows large perceptual transparency. The following figure 1, shows the mechanism of LSB technique

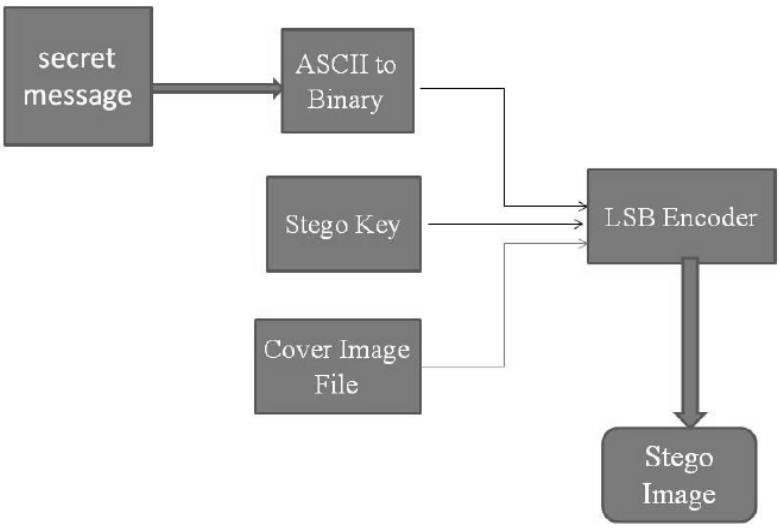


Figure 1: LSB Steganography Technique

II. PROPOSED CONCEPT

Proposed concept is based on the combination of steganography and cryptography. Figure 2 is showing the architecture of proposed concept. Initially it check type of secret message if secrete message (SM) is text (T) then it pass encoding (E) process and if secret message is image (I) then it pass to compression (C) process to reduce the size of the original image to maintain efficiency. This compression process calls wavelet transformation because wavelet transformation provides lossless transformation (LT) where original information can be reverting after uncompressing. Once the comparison done compressed information passed pass to encoding process. Encoding process call key (K) value to produce cipher (CP) value these cipher value pass to steganography technique (ST). In the proposed concept steganography technique uses least significant bits (LSB) process. Least significant bits process select LSB from cover image (CI) by using randomization (R) process and embedded cipher value in cover image to produced stego image (STI).

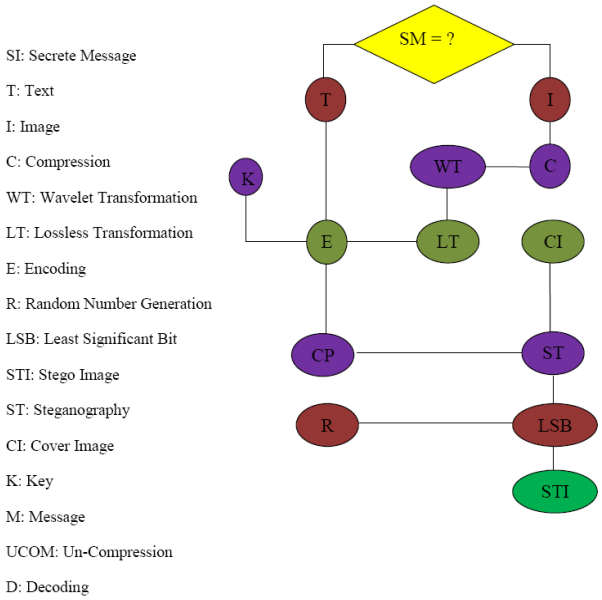


Figure 2: Block Diagram of Proposed Steganography at Encryption Side

Figure 3 is showing the architecture of proposed concept at extraction of original information from stego image. Here stego image (STI) pass to steganography technique (ST) where is use using least significant bits (LSB) technique to extract Cover image (CI) and Cipher (CP) value with the help of randomization (R) process. Once cipher value gated then it passed to decoding (D) process to get original secrete message if message is image then it pass to un-comparison (UCOM) process to get original size of the image without loss any information.

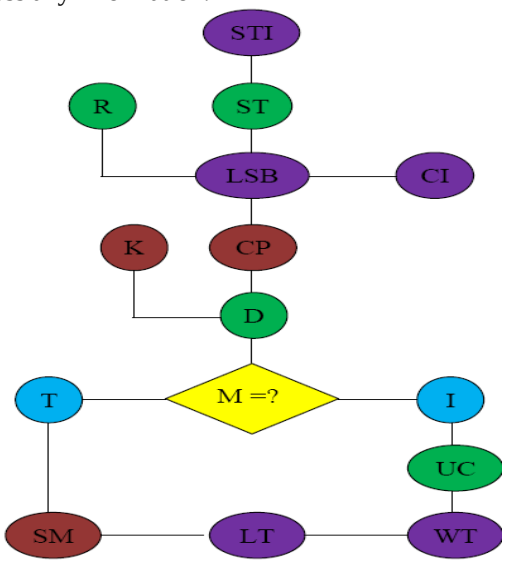


Figure 3: Block Diagram of Proposed Steganography at Decryption Side

III. Proposed Encryption Approach

Proposed encryption approach is based on symmetric cryptography technique. In this it is using block cipher concept with chaining block cipher mode where output of one step passes as an input to the next step. Proposed encryption process are using two logical operation one is XOR and another is right circular shift and as we know that one shift operation and one XOR operation work like six iteration with minimum time duration. Whole encryption process is 10 round processes. Figure 4 is showing architecture of proposed encryption process. This architecture are showing complete one round process. All the process is defined step by step in encryption algorithm step in next section

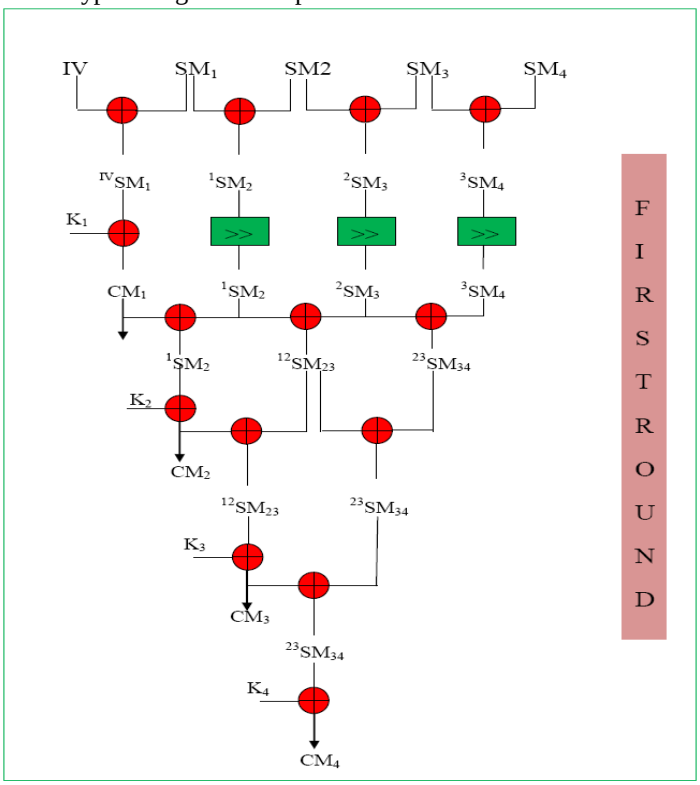


Figure 4: Architecture of Proposed Encryption

Encryption Algorithm Step:

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

IV. PROPOSED DECRYPTION APPROACH

Figure 5 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.

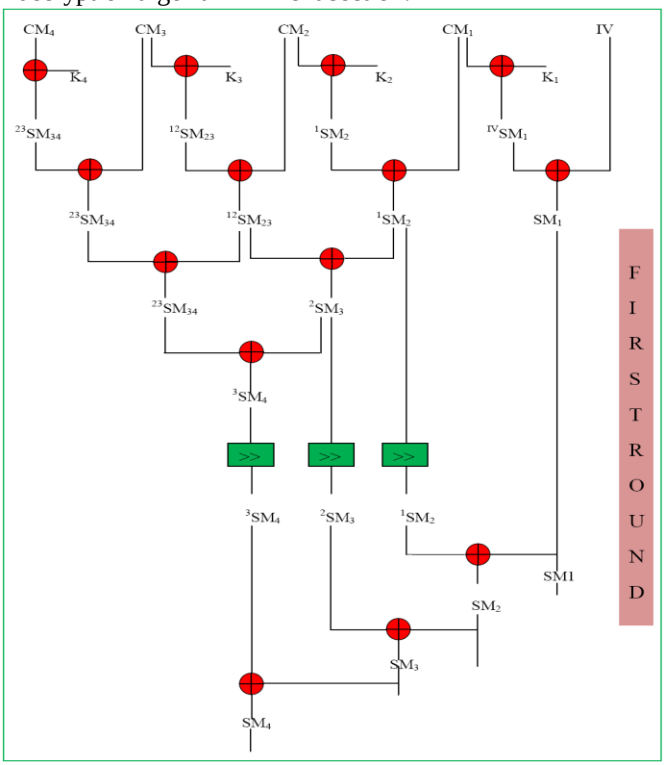


Figure 5: Architecture of Proposed Decryption

Decryption Algorithm Step:

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 XOR K_4 = $^{23}SM_{34}$
   $^{23}SM_{34}$ XOR CM_3 = $^{23}SM_{34}$
   CM_3 XOR K_3 = $^{12}SM_{23}$
   $^{12}SM_{23}$ XOR CM_2 = $^{12}SM_{23}$
   CM_2 XOR K_2 = $^{1}SM_{2}$
   $^{1}SM_{2}$ XOR CM_1 = $^{1}SM_{2}$
   CM_1 XOR K_1 = $^{IV}SM_{1}$
   $^{IV}SM_{1}$ XOR IV = SM_1
   $^{23}SM_{34}$ XOR $^{12}SM_{23}$ = $^{23}SM_{34}$
   $^{12}SM_{23}$ XOR $^{1}SM_{2}$ = $^{2}SM_{3}$
   $^{23}SM_{34}$ XOR $^{2}SM_{3}$ = $^{3}SM_{4}$
7. Perform 2 bits right circular shift in reverse order in following way
   Rev(>>2) $^{3}SM_{4}$ = $^{3}SM_{4}$
   Rev(>>2) $^{2}SM_{3}$ = $^{2}SM_{3}$
   Rev(>>2) $^{1}SM_{2}$ = $^{1}SM_{2}$
8. Perform XOR in following way
   $^{1}SM_{2}$ XOR SM_1 = SM_2
   $^{2}SM_{3}$ XOR SM_2 = SM_3
   $^{3}SM_{4}$ 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 Step:

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 Step:

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: Wavelet compressions are two types lossless or lossy. In lossless compression, the original data can be reconstructed from the compressed data, but in lossy compression the partial data can be reconstructed. 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]. Steps in wavelet compression: Load the image, perform wavelet decomposition of the image, and compress using fixed Threshold [3].

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

1. Start with an initial seed (e.g. a 2-digit integer and in our case it is again a random value).
2. Square the number.
3. Take the middle 2 digits.

Midsquare Method (Random Number Generation) 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: $7089^2 = 50253921$ ® $x_3 = 53$, $R_3 = 2539$

V. RESULTS

Performance Analysis: This section presents results on two type of secret message 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 6 (a) and (b)) which is highlighted as a "I**nput 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.

Input Cover Images

(a) Lena.jpg b) Monalesa.jpg

Figure 6: Cover Image

Input Secrete Images

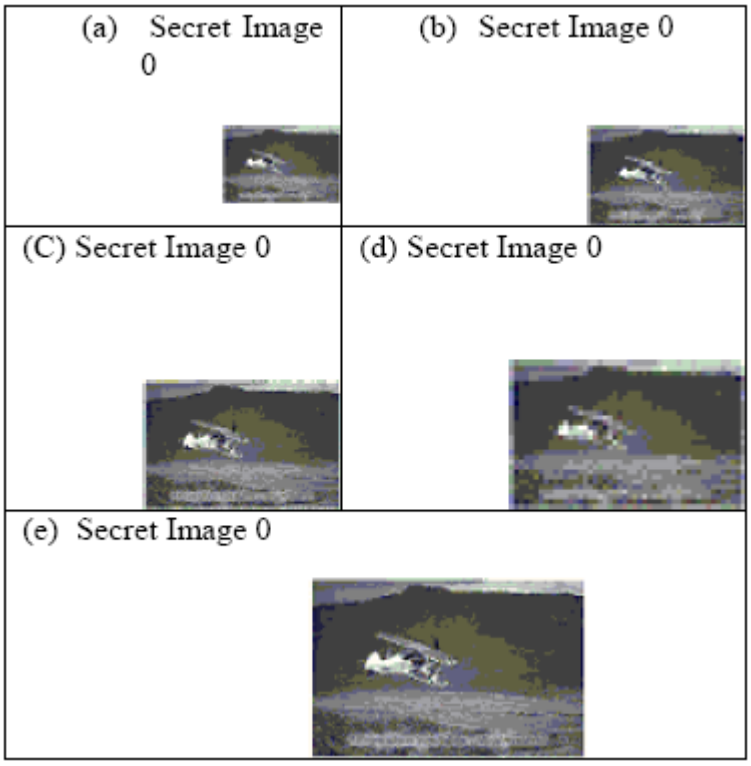


Figure 7: Secret Image

Input Secret Text Message

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

All three parameter are evaluated for image type of secret message and for text only PSNR and correlation evaluated. Each parameter is described below in detail.

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]

$$MSE = \frac{\sum_i \sum_j |x(i,j) - y(i,j)|^2}{N}$$

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

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 [5].

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

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: We have 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 [15]:

$$cov(x, y) = E(x - E(x))(y - E(y)),$$

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

Where and are the values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used [15]:

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

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

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

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 Monalisa.jepg and various Secret Image's.

Table 2: PSNR, Correlation and Entropy Performance of Proposed Concept over Image Secret Information (Cover Image is Monalisa.jpg)

	Input		PSNR	Correlation	Entropy
monalisa.jpg	Input Data	Size in KB	Propose Work	Propose	Propose
secret_image0.bmp	Image1	2.5	35.638026	0.749495	7.768702
secret_image1.bmp	Image2	3.55	35.638026	0.749495	7.768702
secret_image2.bmp	Image3	5.11	35.637947	0.749067	7.768647
secret_image3.bmp	Image4	6.67	35.638026	0.749495	7.768702
secret_image4.bmp	Image5	9.03	35.637989	0.747746	7.768686

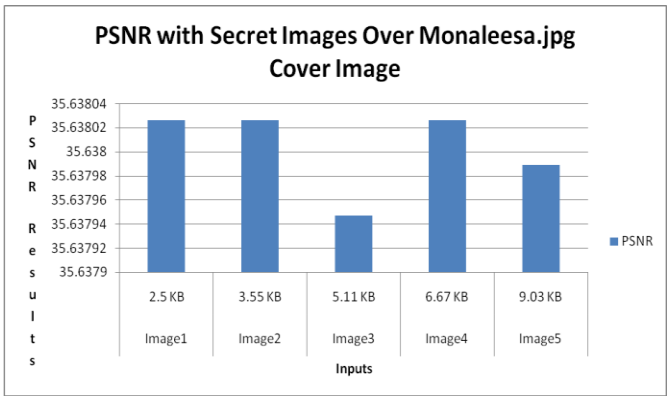
Table 3: PSNR, Correlation and Entropy Performance of Proposed Concept over Image Secret Information (Cover Image is Lena.jpg)

	Input		PSNR	Correlation	Entropy
monalisa.jpg	Input Data	Size	Propose Work	Propose	Propose
secret_image0.bmp	Image1	2.5	45.824747	0.592466	7.768668
secret_image3.bmp	Image4	6.67	45.823471	0.59069	7.768801
secret_image4.bmp	Image5	9.03	45.828173	0.591621	7.768805

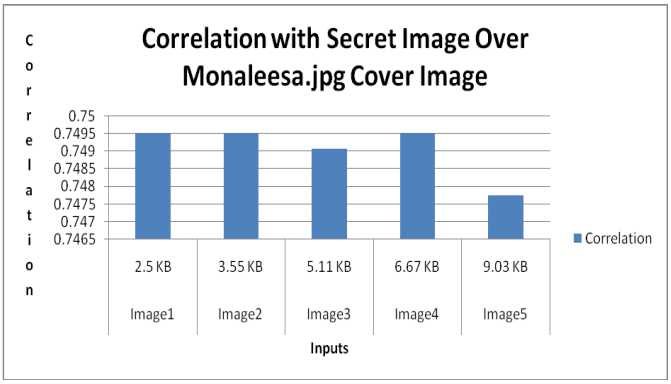
Test case 2: Whene Cover image is Monaleesa.jepg and various Secrete Text.

Table 4: PSNR and Correlation Performance of Proposed Concept over Text Secret Information with Monaleesa.jpg

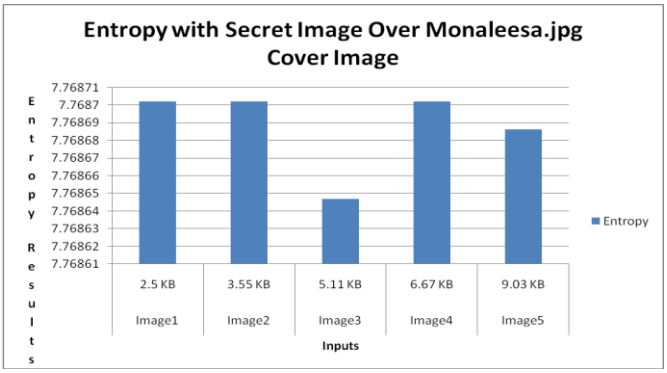
Input		PSNR		Correlation
Name	Size	Proposed		Proposed
Text 1	64 Bytes	35.637955		0.748887
Text 2	256 Bytes	35.637848		0.749297
Text 3	320 Bytes	35.637873		0.749388
Text 4	640 Bytes	35.637896		0.749183



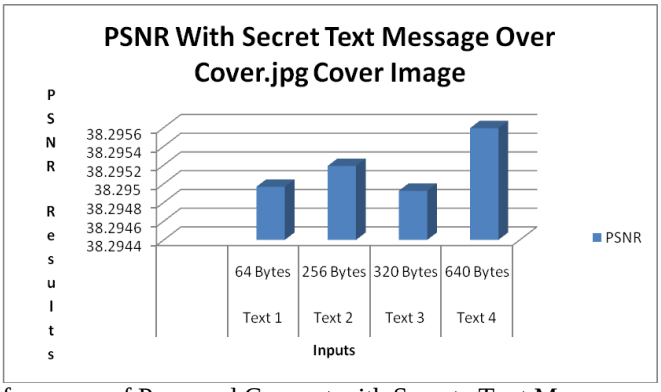
Grpah 1: PSNR Performance of Proposed Concept with Secrete ImageMessage over Monaleesa.jpg



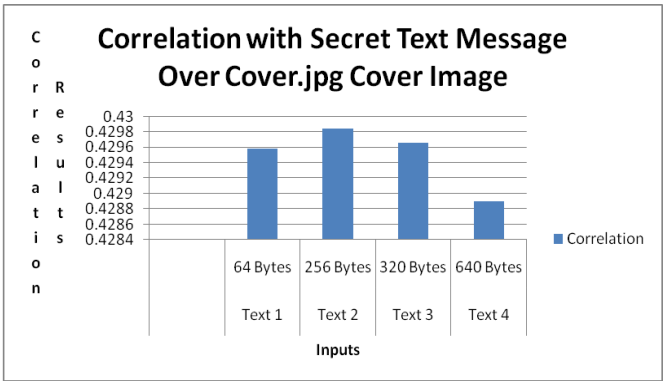
Grpah 2: Correlation Performance of Proposed Concept with Secrete ImageMessage over Monaleesa.jpg



Grpah 3: Entropy Performance of Proposed Concept with Secrete ImageMessage over Monaleesa.jpg



Grpah 4: PSNR Performance of Proposed Concept with Secrete Text Message over Cover Image.jpg



Grpah 5: Correlation Performance of Proposed Concept with Secrete Text Message over Cover Image.jpg

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.

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.

VI. CONCLUSION

Steganography is an effective way to hide sensitive information. In this research work two approaches have used one is encryption/decryption and another is steganography. In Steganography technique has also used two approaches one is the LSB Technique and second is the Pseudo-Random Encoding Technique on images to obtain secure stego-image. Presented PSNR is showing good picture quality of stego image in LSB encoding. Our results indicate that the LSB insertion using random key is better than simple LSB insertion in case of lossless compression. The image resolution doesn't change much and is negligible when embed the message into the image and the image is protected with the personal key. So, it is not possible to damage the data by unauthorized personnel. The algorithm is usage for both 8 bit and 24 bit image of the approx double size of cover as compare secret image, so it is easy to be implementing in both grayscale and color image. This research work focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate [5].

REFERENCES

[1] R.P Kumar, V. Hemanth, M "Securing Information Using Sterganoraphy" International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013 , Page(s): 1197 - 1200

[2] 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), Publication Year: 2013 , Page(s): 1188 – 1193

[3] M.K Ramaiya. ; N.Hemrajani, ; , A.K Saxena. "Security improvisation in image steganography using DES" IEEE 3rd International on Advance Computing Conference (IACC), Publication Year: 2013 , Page(s): 1094 - 1099

[4] 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), Publication Year: 2013 , Page(s): 385 – 390

[5] 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 (ICAESM -2012) March 30, 31, 2012

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

[7] 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 (ICAESM - 2012) March 30, 31, 2012

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

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

[10] 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

[11] 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

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

[13] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) 102-108

[14] danah boyd and Alice Marwick "Social Steganography: Privacy in Networked Publics" ICA 2011

[15] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) 102-108

