Security Improvisation in Image Stegenography using DES

Miss Laxmi Randa
Computer Science &Engineering
Name of Organization Samrat Ashok Technological Institute
Vidisha,(M.P.),india

Prof. Payal Saxena
Computer Science &Engineering
Name of Organization Samrat Ashok Technological Institute
Vidisha,(M.P.),india

Dr. Y.K.Jain
HOD of Computer Science &Engineering
Name of Organization Samrat Ashok Technological Institute
Vidisha,(M.P.),india

Abstract: ***The quick development of information transfer through network made it easier to send the information faster and accurate to the destination side. There are lots of transmission media to move the data to destination side like e-mails and chatting; at the similar time it is may be easier to changes and abuse the valuable data through hacking or cracking. So, in order to transfer the information securely to the destination side without any modifications or changes, there are lots of approaches like cryptography and steganography. This paper deals with the image cryptography as well as image steganography technique with the various security issues and performance parameter, general overview of cryptography, steganography approaches and about the various steganography techniques like Least Significant Bit (LSB) algorithm. It also is showing proposed technique performance in terms of peek signal to noise ratio (PSNR), entropy, and correlation. This paper proposing new image security algorithm which is grouping of two various techniques one is cryptography and second is steganography that build use of Least Significant Bit (LSB) for embedding the data into the bit map image (.bmp) by using random number generation technique and its implemented through the MAT LAB software.***

Key Word: - Steganography, Security, Encryption, Decryption, Internet

1. INTRODUCTION

In this research work, use a method of encoding the images files in an image file in order to check the efficiency and accuracy of encryption. This technique helps to send the secrete information to the authorized user without any prospective risk. The proposed technique will help to sheltered the content with in the cover up image and encoded of images file with in the cipher image will help to build the document too much sheltered because even though if the un-authorized or un-

authenticated user succeeds in being capable to hack the secrete image, the user will not capable to read and see the confidential message as well as gain the secrete information in the image file. In this proposed research work, proposed system will evaluate two steganography techniques in order to compare the beating efficiency and capacity of beating the confidential message with in a cover image. Whenever the image is encrypted using cryptography and followed by steganography algorithms within cover image, neither secrete image nor should the cover image it is embedded in mislay its originality. Hence, here comparison the between existing and proposed algorithms used for cryptograph and steganography for the various imagers and formats and analyze the results obtained.

The proposed technique consists of

- Supporting two layer of security for the secrete image to be transmitted through public network by using steganography.
- Proposing a technique for hiding the secrete images within a cover image using cryptography followed by steganography technique which provides higher security and better accuracy of stego image.
- Using cryptography techniques.
- Using Least Significant Bits (LSB) technique in Steganography

- Using Random Number Generation technique in Steganography.
- Implementing existing and proposed steganography technique
- Comparing both steganography techniques in means of Peek Signal to Noise Ration (PSNR), Correlation and entropy of stego Image.

The MAT LAB software is used to extensively analyze the functions of the proposed steganography technique. Only Image file formats are encoded and embedded into a cover up image file which is then transferred to the other end (destination). Generally accessing of the confidential messages with un-authorized way is called hacking. Cryptanalysis and Steganalysis is the technique of a crypto-analyzer and stegano-analyzer to cracks the cover and get confidential message. So, that security is the prim concerned during the design and development of the new research. Drawbacks of the existing techniques are that the uses of ordinary approach and functionality during conceal secrets inside cover image. All existing technique has various strong and weak points related with various parameters; furthermore they all have a small number of basic requirements. The main requirement is that the existing techniques have to be imperceptible. From the study of the existing technique it's conclude various parameters from [1, 2, 4, 5,]. These are as follows:

Peak Signal-to-Noise Ratio (PSNR) is the ratio between the original image and the encrypted image. The higher the PSNR, the closer the encrypted image is to the original. PSNR reflects the encryption quality and PSNR of existing technique can be improved

Entropy: Entropy is one of the significant measures for evaluating any encryption system. Information entropy represent the degree of randomness and uncertainties in systems like cryptography, network security, and data compression [2]. Entropy of existing technique can be improved.

Correlation: Correlation is a issue that determines how much two variables are similar to each other. This is commonly used to measure the encryption quality of any cryptography scheme [2]. The strength and usefulness of any encryption technique is measured by its ability to conceal all attributes of the original data and to produce an encrypted data which is totally random and uncorrelated with the original one [11]. In image processing, usually, the correlation among adjacent pixels of original image is very high (i.e., equal to 1).

Secrecy – The secrecy of existing algorithm is the first and foremost requirement, since the strength of existing algorithm lies in its ability to be unnoticed by the human eye. The moment that one can see that information has been tampered with, the algorithm is compromised.

Robustness–Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the mode where the data is embedded, these manipulations may obliterate the concealed data. It is preferable for steganography to be robust beside either unintentional or malicious changes to the image.

Security: Security is the prim concerned in the field of encryption. It known that information over public network should be highly secured otherwise any eavesdropper can be easily access information. Encryption Key is play an important role in the field of encryption and security of the algorithm is depending upon key length. Higher key length will be causes higher security.

2. .PROPOSED WORK

Proposed Work: Reason behind choosing this model is the security, efficiency with good picture quality of stego image. Most interesting thing in this technique is the combination of two different techniques. This proposed technique is a approach of security that combines two or more security technique and usually a combination of symmetric and steganography to take benefit of the strengths of each type of encryption. Symmetric encryption has the performance benefit and therefore is the general solution for encrypting and decrypting confidential data, such as an online data stream. On the other hand, steganography provides better security in that the cryptographic key required for decrypting data does not have to be shared with other parties. The proposed concept are using three approach on secret image which is following

1. Encoding/Decoding
2. Steganography
3. Random Number Generation Technique

Detailed description of each process is shown in figure 1. It is providing general architecture of proposed concept. In this concept initially a secret image will select as an input and pass to proposed encoding method. Proposed encoding method are converting original secrete image into cipher image by using 128 bits secrete key value. This private key value will known only for sender and receiver. After producing cipher image proposed concept called steganography method where a cover image will pass as an input then this steganography technique read least significant bits from cover image by using random number generation technique which is play as key value role for steganography technique and replace from cipher bits value. This process will continue till last pixel of cipher image. At last an image will produced called stega image.

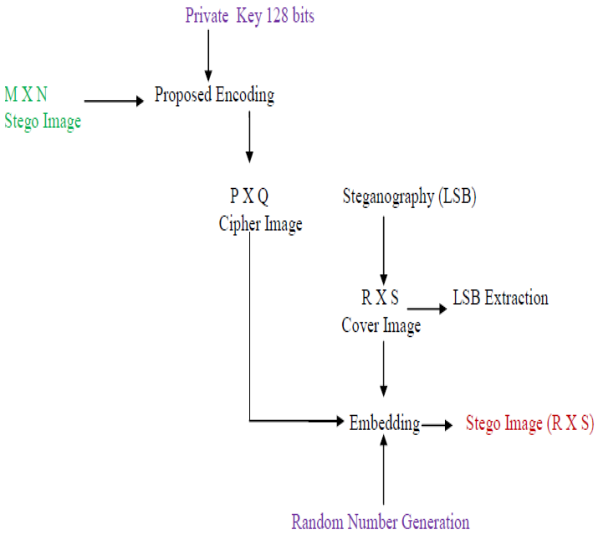


Figure 1: Architecture of Proposed Concept at First End

Figure 2 is showing the general architecture of proposed concept at receiver end. In this concept a stego image will select and pass to steganography technique where this technique worked in reverse order. Initial it will read least significant bit by using LSB method with the help of random number generation technique. This process will continue till last LSB from stego image whenever all LSB extracted then stego image will become cover image and all LSB extract pixel become cipher image. Then this cipher images pass to decoding method for decoded cipher value into original value. This decoding method is work with 128 bits secrete value and produced original secrete image.

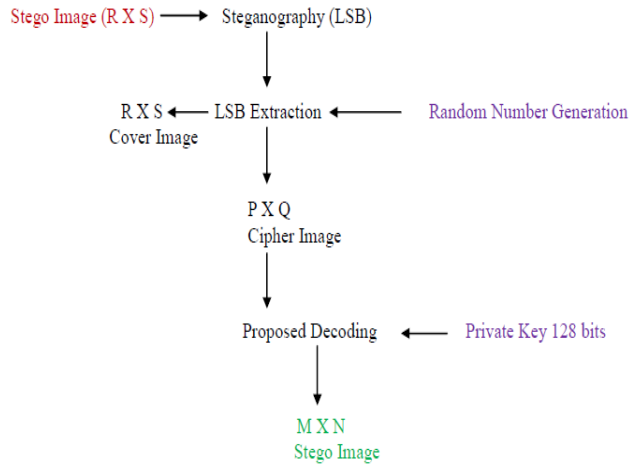


Figure 2 Architecture of Proposed Concept at Second End

Here number of steps of proposed technique and both (Sender and Receiver) end are as follow:

Steps of Proposed Technique at Sender Side

1. Input MXN Secrete Image
2. Input PXQ Cover Image
3. Input Key
4. Call Encoding Algorithm
5. Pass Secrete Image and Key
6. Produced Cipher Image
7. Call Steganography (LSB)
8. Pass Cover Image and Cipher Image
9. Call Random Number Generation Technique
10. Embedded Cipher Image into Cover Image
11. Produced Stego Image

Steps of Proposed Technique at Receiver Side

1. Input MXN Stego Image
2. Input Key
3. Call Steganography (LSB)
4. Pass Stego Image
5. Call Random Number Generation Technique
6. Extract Cipher Image and Cover Image
7. Call Decoding Algorithm
8. Pass Cipher Image and Key
9. Produced Secret Image

Encryption and Decryption Architecture: Figure 3 is showing the architecture of proposed encoded method. Proposed encryption and decryption architecture is a block cipher based architecture where secret values are encoding in a block of bit. Here 128 bits in a block are encoding at a time. Proposed encryption architecture is 10 round processes where output of first round passes as an input to the next round. Convert secrete image pixel into binary value.

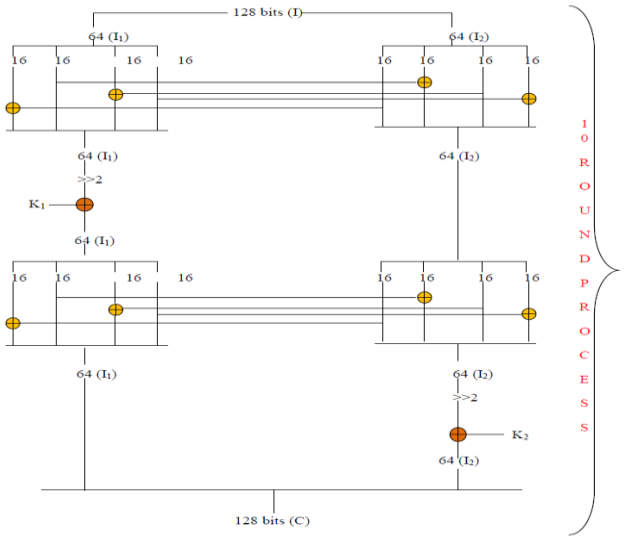


Figure 3: Architecture of Proposed Encryption

Initially pickup 128 bits binary value of secrete image and divide into two sub parts (sub part-1 and sub part-2) equally. Once again these sub parts (Sub part-1 and sub part-2) are again divide into four sub parts equally. These sub parts are perform very strong logical operation known as XOR which is provide approximately "4 to 5" round capabilities within single "XORing" and produced results. After completing this logical operation process proposed encoding perform another strong logical operation known of circular shift (left, right), here left circular shift operation are used and provide approximately "2 to 4" round capabilities within single "Circular Shifting". But these operation are applicable only one sub parts at a time (see figure 3). after that resultant value perform once again XORing operation through a secret key (K) value which is also divided into two sub parts(K_1 and K_2) used. First time key K_1 is used, then repeat some process and then use key K_2. At last final results combine and ready for the next round as an input, this process will continue till all binary value of secret image does not read. It's very important that XORing done between two equal bits so that the length of the key value is also 128 bits which is sufficiently secured.

Proposed Encryption Algorithm

1. Input secret Image I_s
   a. $I_s \leftarrow$ Secret Image
2. Input Key K of 128 bits
3. Divide K in to two sub parts K_1 and K_2 of equal size
   a. $K/2 = (K_1, K_2)$
4. Loop R = 1 to 10 { R= Round
5. Loop I_s = 1 to N block { 1 Block = 128 bits
6. Read Binary of I_s
   a. $BI_s \leftarrow$ Binary (I_s)
7. Divide BI_s into two equal sub parts
   a. $BI_s/2 \rightarrow ({}^1BI_s, {}^2BI_s)$
8. Again divide $({}^1BI_s, {}^2BI_s)$ into four equal sub parts
   a. ${}^1BI_s \rightarrow ({}^{11}BI_s, {}^{12}BI_s, {}^{13}BI_s, {}^{14}BI_s)$
   b. ${}^2BI_s \rightarrow ({}^{21}BI_s, {}^{22}BI_s, {}^{23}BI_s, {}^{24}BI_s)$
9. XOR_{ing}
   a. ${}^{11}BI_s \leftarrow {}^{11}BI_s \oplus {}^{21}BI_s$
   b. ${}^{22}BI_s \leftarrow {}^{12}BI_s \oplus {}^{22}BI_s$
   c. ${}^{13}BI_s \leftarrow {}^{13}BI_s \oplus {}^{23}BI_s$
   d. ${}^{24}BI_s \leftarrow {}^{14}BI_s \oplus {}^{24}BI_s$
10. Combine these sub parts
   a. ${}^1BI_s \leftarrow ({}^{11}BI_s, {}^{12}BI_s, {}^{13}BI_s, {}^{14}BI_s)$
   b. ${}^2BI_s \leftarrow ({}^{21}BI_s, {}^{22}BI_s, {}^{23}BI_s, {}^{24}BI_s)$
11. 2-bits left circular shift on ${}^1BI_s$
   a. ${}^1BI_s \leftarrow$ Left_Cir((${}^1BI_s$)>>2)
12. **XOR_{ing}**
   a. ${}^1BI_s = {}^1BI_s \oplus K_1$
13. Repeat 7 -9
14. 2-bits left circular shift on ${}^2BI_s$
   a. ${}^2BI_s \leftarrow$ Left_Cir((${}^2BI_s$)>>2)
15. **XOR_{ing}**
   a. ${}^2BI_s = {}^2BI_s \oplus K_2$
16. End Loop
17. Combine $({}^1BI_s, {}^2BI_s)$ to make CI_s
18. $CI_s \leftarrow {}^1BI_s \otimes {}^2BI_s$
19. End Loop
20. Exit

Figure 4 is showing the architecture of proposed decryption process. Proposed encryption architecture is 10 round processes where output of first round passes as an input to the next round. Convert cipher image pixel into binary value. Initially picked up 128 bits binary value from ciphered image and divide into two sub parts (sub part-1 and sub part-2) equally, Then perform XORing operation through a secret key (K) value which is also divided into two sub parts(K_1 and K_2) used. First time key K_2 is used, on the second sub parts. And then using reverse circular shift operation on the same sub parts. Once again these sub parts (Sub part-1 and sub part-2) are divide into four sub parts equally, and then performing XORing operation between each other. Repeats some process (See figure 4) and use key K_1. At last final results combine and ready for the next round as an input, this process will continue till all binary value of ciphered image does not read.

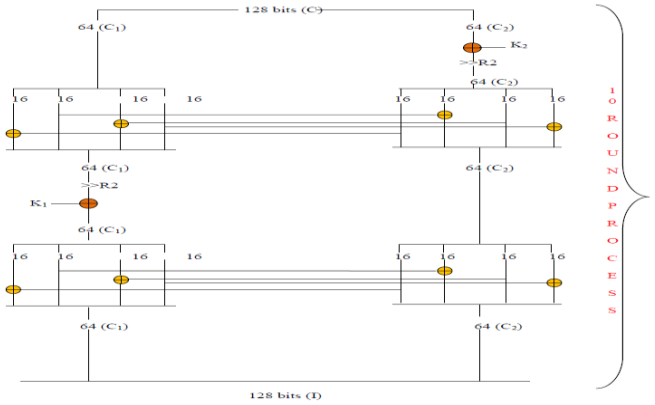


Figure 4: Architecture of Proposed Decryption

Proposed Decryption Algorithm

1. Input Cipher Image CI_s
   a. CI_s ← Cipher Image
2. Input Key K of 128 bits
3. Divide K in to two sub parts K_1 and K_2 of equal size
   b. $K/2 = (K_1, K_2)$
4. Loop R = 1 to 10 } R= Round
5. Loop I_s = 1 to N block } 1 Block = 128 bits
6. Read Binary of CI_s
   a. BCI_s ← Binary (I_s)
7. Divide BCI_s into two equal sub parts
   a. $BCI_s/2$ → ($^1BCI_s$, $^2BCI_s$)
8. **XOR_{ing}**
   a. $^2BCI_s = {}^2BCI_s \oplus K_2$
9. 2-bits reverse left circular shift on ^2BI_s
   a. $^2BCI_s$ ← Rev_Left_Cir(($^2BCI_s$)>>2)
10. divide ($^1BCI_s$, $^2BCI_s$) into four equal sub parts
    a. $^1BCI_s$ → ($^{11}BCI_s$, $^{12}BCI_s$, $^{13}BCI_s$, $^{14}BCI_s$)
    b. $^2BCI_s$ → ($^{21}BCI_s$, $^{22}BCI_s$, $^{23}BCI_s$, $^{24}BCI_s$)
11. XOR_{ing}
    a. $^{11}BCI_s$← $^{11}BCI_s \oplus {}^{21}BCI_s$
    b. $^{22}BCI_s$← $^{12}BCI_s \oplus {}^{22}BCI_s$
    c. $^{13}BCI_s$← $^{13}BCI_s \oplus {}^{23}BCI_s$
    d. $^{24}BCI_s$← $^{14}BCI_s \oplus {}^{24}BCI_s$
12. Combine these sub parts
    a. ^1BI_s ← ($^{11}BI_s$, $^{12}BI_s$, $^{13}BI_s$, $^{14}BI_s$)
    b. ^2BI_s ← ($^{21}BI_s$, $^{22}BI_s$, $^{23}BI_s$, $^{24}BI_s$)
13. Repeat 10-12
14. 2-bits reverse left circular shift on $^1BCI_s$
    a. $^1BCI_s$ ← Rev_Left_Cir(($^1BCI_s$)>>2)
15. **XOR_{ing}**
    a. $^1BCI_s = {}^1BCI_s \oplus K_1$
16. End Loop
17. Combine ($^1BCI_s$, $^2BCI_s$) to make I_s
18. I_s ← $^1BCI_s \otimes {}^2BCI_s$
19. End Loop
20. Exit

Block Diagram of Proposed Steganography: In the propped concept steganography technique is used after cryptography technique. This is another security technique which is providing additional security layer in the proposed concept.

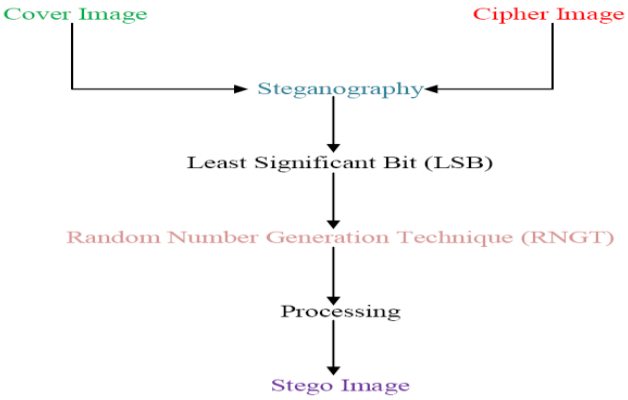


Figure 5: Architecture of Proposed Steganography at Sender End

The beauty of the steganography is increasing by using random number generation technique during least significant bit selection from cover image in least significant bits (LSB) technique. Figure 4 is showing the general architecture of proposed steganography technique and sender end. In this cover image and cipher image passed as an input. After that LSB technique select cover image and apply random number technique to find the least significant bit randomly and then replace these LSB from cipher bits value. The important thing is that size of the cover image should be grater then cipher image approximately double because smoothly embedding of cipher value in cover image and picture quality of the cover image does not major reflect. This process will continue till last pixel of cipher image. And at last an image produced called stego image.

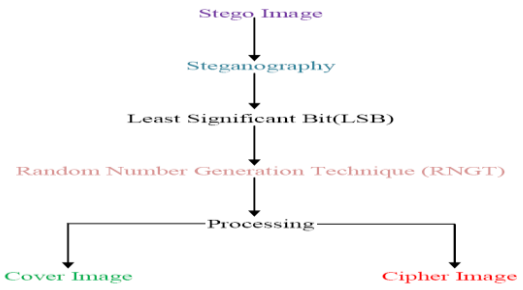


Figure 6: Architecture of Proposed Steganography at Receiver End

Similarly figure 6 general architecture of proposed steganography technique at receiver end. Hear a steg image is passing as an input then apply LSB technique to read least significant bits by using random number generation technique. Through this technique read all LSB pixel and produced cover image and cipher image separately.

Random Number Generation Technique: Blum Blum Shub generator is the pseudo random number generator. By using this random numbers are generated. The formula has shown below [3, 6],

Mi+1=(M/mod k
Where, Mi is the seed, and K be the range.
The pseudo random bit generator is used for generating random numbers in cryptography. Seed, two large prime numbers, and the range is the inputs for the pseudo random bit generators [3]. The mathematical formulae has shown below,
Mi+1= (LMi+O) mod k
Where L,O are two large prime numbers, Mi is the seed. k be the range

3. RESULTS

Performance Analysis: Here presents the Evaluated results through proposed technique by using some selected performance parameters. Selected performance parameters are Peek Signal to Noise Ratio (PSNR), Correlation and Entropy of the image which is described below.

- **Peek Signal to Noise Ratio (PSNR):** 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]

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

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

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

- **Correlation:** DIC is predicated on the maximization of a correlation coefficient that is determined by examining pixel intensity array subsets on two or more corresponding images and extracting the deformation mapping function that relates the images. An iterative approach is used to minimize the 2D correlation coefficient by using nonlinear optimization techniques. The cross correlation coefficient r_{ij} is defined as [18, 17, 19]

$$r = \frac{n\sum(xy) - \sum x \sum y}{\sqrt{\left[n\sum(x^2) - (\sum x)^2\right]\left[n\sum(y^2) - (\sum y)^2\right]}}$$

Where
r: correlation value
n: the number of pairs of data
$\sum xy$: sum of the products of paired data
$\sum x$: sum of x data
$\sum y$: sum of y data
$\sum x^2$: sum of squared x data
$\sum y^2$: sum of squared y data

- **Entropy:** For a given PDF *P,* Entropy Ent[P] is computed as [3, 4,6,7]-

$$\text{Ent[P]} = -\sum_{k=0}^{L-1} P(k) log_2 P(k)$$

The Entropy is a used to measure the richness of the details in the output image.

Table 1 is showing the PSNR, Entropy and Correlation value which is produced. During results of proposed technique, design and developed system on MAT lab which use various size of input image and one cover image which is mentioned below.

Cover Image 

Figure 7: Cover Imagee.jpg of 720 X 447

And input images

Proposed work used some input (secret image of various size which is following

Figure 8: Secrete Imagee 00.bmp of 48 X 31

Figure 9: Secrete Imagee 11.bmp of 64 X 40

Figure 10: Secrete Imagee 22.bmp of 80 X 52

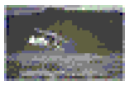
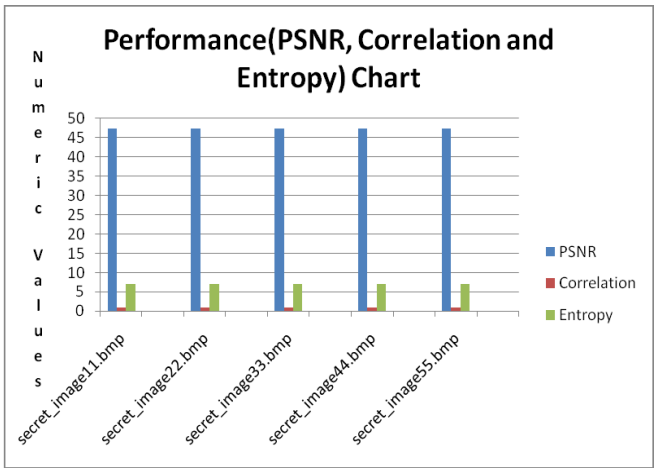


Figure 11: Secrete Imagee 33.bmp of 96 X 60

Figure 5.7: Secrete Imagee 44.bmp of 112 X 73

Table 1: PSNR, Correlation and Entropy of Proposed Technique

Images		**PSNR**	**Correlation**	Entropy
	Size	**Proposed Work(Approx Results)**		
secret_image 11.bmp	5.11 KB	47.098851	0.770967	7.011432
secret_image 22.bmp	6.67 KB	47.095403	0.772405	7.030251
secret_image 33.bmp	9.14 KB	47.097695	0.771635	7.013449
secret_image 44.bmp	11.5 KB	47.084006	0.770649	7.016246
secret_image 55.bmp	14.4 KB	47.08965	0.772169	7.030094



Graph 1: Graphically Respresentation of Perfromace Parameters

Results Summary: From the outcome study it has been experiential the performance of proposed concept in all facets has batter. By the LSB steganography, embedding hug amount of confidential information is not easy. Concept of the proposed work is to embed hug amount of confidential information i.e. image using LSB steganography. LSB Steganography technique is one of the best techniques when compared to transformation techniques, because it reduces lots of noise distortion. After LSB technique produced stego image quality shown in table 1 for image where five inputs confidential images with one cover image is noted. In this for image of 5.11 KB is producing 47.098851PSNR through proposed concept which is producing good results. Correlation of stego image had shown in table 1 for image. In this for image of 5.11 KB producing 0.770967, correlation through proposed concept respectively over image secrete information which producing good results. Similarly Entropy of stego image had shown in table 1 for image. In this for image of 5.11KB producing 7.011432, entropy through proposed respectively over image secretes which producing good results. Graph 1 is also showing the graphical analysis of proposed concept on selected parameters (PSNR, Correlation, Entropy) on various size of secrete Image.

4. CONCLUSION

Computer organization and their user are more conscious about security as normal organization and their user. Protection or security from superfluous type sources has become a component of the proposed research work. Proposed research works is not projected to changes or substitute the cryptography technique but it is providing additional benefit for it. If information is encoded and concealed with a steganography technique it provides an additional layer of shield and it is reduces the possibility of the secreted information being detected. The proposed research work is a small piece of the large steganography talent

with the combination of image encoded. Encoded technique goes well away from simply encoded an image by well distinct proposed encoding technique and steganography goes well away from simply hiding encoded image in a cover up image. The presented experimental results have also approved to our conclusion.

REFERENCES

[1] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena "Security Improvisation in Image Steganography using
DES" IEEE 3rd International Advance Computing Conference (IACC), 22-23 Feb. 2013 PP 1094 - 1099
[2] RigDas and Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding" IEEE 2012
[3] 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
[4 G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan "Steganography Using Edge Adaptive Image" IEEE International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012
[5] L.Jani Anbarasi and S.Kannan "Secured Secret Color Image Sharing With Steganography" IEEE 2012
[6] 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
[7] 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
[8] 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
[9] Abhishek Gupta, Sandeep Mahapatra and, Karanveer Singh " Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm" 2011 IEEE
[10] Guy-Armand Yandji, Lui Lian Hao, Amir-Eddine Youssouf and Jules Ehoussou research on a normal file encryption and decryption" IEEE 2011
[11] Akhil Kaushik, AnantKumar and Manoj Bamela " Block Encryption Standard for Transfer of Data " IEEE International Conference on Networking and Information Technology 2010
[12] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) 102-108
[13] danah boyd and Alice Marwick "Social Steganography: Privacy in Networked Publics" ICA 2011

