Enhance Steganography Techniques: A Solution for Image Security

Priyanka Thakur
M.Tech. Scholar,
SIST Bhopal (M.P)

Santosh Kushwaha
SIST Bhopal (M.P)

Yogesh Rai
SIST Bhopal (M.P)

ABSTRACT
Steganography word is making from two words: one is Steganos that means "covered or secret" and second is the graphic that means "writing". Similarly Cryptography word is also making from two words: one is Crypto that means "Alter original word Meaning" and second is the graphic that means "writing". In this work, Enhance Steganography technique with cryptograph technique is proposed, developed and analyzed. The proposed technique encrypts the confidential image by the proposed encryption technique initially and then hides the cipher image by Steganography technique which is using randomization techniques during selection of LSB. The results of the proposed technique are discussed and analyzed based on the peek signal to noise ratio (PSNR) and Correlation. The proposed technique is simple, fast secure and efficient, it strong to attack and better the image quality.

Keywords
Image Steganography, Secrete Image, Cover Image, Stego Image, Steganalysis, Cryptography, LSB(Least Significant Bit), Security.

1. INTRODUCTION
Presently all type of information is preserve in digital media. Internet is the medium where information is moving from one user to another user. Every system can give various security schemes for outgoing packets. The sender user and receiver user suppose that information is securely transferred. But the information is transferred over insecure medium, if somebody can get the ciphered information and through applying cryptanalysis on it, the intruder or attacker can get the original significance; the enemy can even change the information and pass to the receiver user. Two types of scheme are there to give security for the confidential information, they are scheme of cryptography and scheme of steganography. Cryptography that means [1, 6, 8] changing the text from understandable format to not unreadable format. Figure 1 is showing the concept of cryptography.

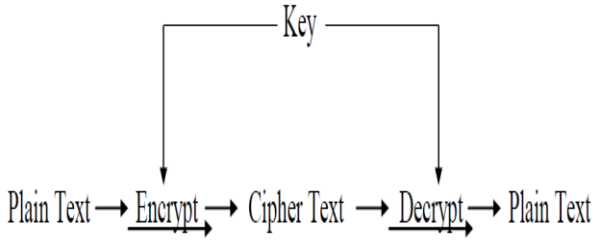


Figure 1: Cryptography Concept

But the ciphered text is able to be seen to everyone, through applying cryptanalysis on this cipher text, the attacker or intruder can get the original significance, otherwise he can change the cipher text. Scheme of Steganography is used for hiding the information in an image [2, 4, 7]. The information is not able to be seen. The Steganography concept is shown below.

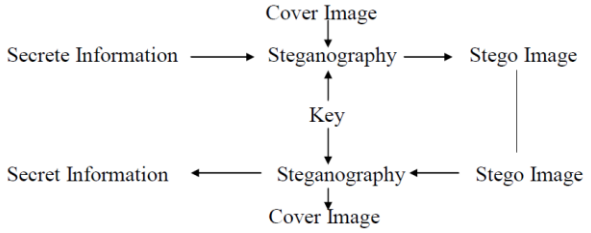


Figure 2: Steganography Concept

There are three types of scheme of Steganography techniques are accessible for hiding the information in a cover image, that is

- Least Significant Bit Insertion,
- Masking,
- Transformation techniques.

Each technique having their own attribute. Least significant bit insertion is the preeminent scheme for embedding the confidential information in a cover image with less noise, but it is applicable only for a few amount of information. Transformation techniques are helpful for embedding the big amount of information in a cover image, the main disadvantage of transformation scheme is, and it generates more noise in the stego image. The likeness between Steganography scheme and cryptography scheme is that, both are used to secure information. But the difference is that the scheme of Steganography does not disclose any doubtful about the hidden information to the user. Therefore the attackers or intruder will not try to get the original information. But it is already known that cryptography it self a strong security technique. Due to this reason proposed work is combine effort of the scheme of Steganography and scheme of cryptography.

2. PROPOSED WORK
Presented work with the secret messages that can be image which is transformed into its subsequent ASCII value, further the ACSII is transformed into its binary value. With the help of proposed encryption algorithm, proposed technique is encrypting the binary value. Now these encrypted bits are prepared to implant into a cover image through LSB image steganography technique. The encrypted data is ready to be entrenched in the cover image. Before implant the data, the cover image is now rehabilitated into its subsequent pixel values. These values are set in particular order, generally used M X N matrix order where M as a row and N as a columns represented respectively. The bit of the secret information has to be embedded in the random positions in the cover image.

To identify the random positions, Random number generators play a vital role. Random numbers act like another key value in this technique. B1umlblumlshub generator and Pseudo random number generator are used to se1ect the random rows and columns respectively. Random numbers are generated by the generator, using the key (seed). Randomness will be varying from generator to generator. The randomness is achieved by padding the bits in the sequence. After selecting the random positions in the image (pixel values) now the secret message is embedded in the corresponding bits using the LSB insertion technique.

Proposed Key Selection Technique: Figure 3 is viewing the architecture of proposed key selection. In this size (Sz) of secret image (SI) is checked in terms of bytes that it is even or odd. If the secret image is even then add all the even position pixel of secret image (SI) otherwise add all the odd position pixels of secret image (SI). Once we get summation of even or odd pixels then apply circular shift (left and right) of sub key K_1 and K_2 to get to new sub keys K_1 and K_2. These sub keys are producing by main key (K) (See figure 3).

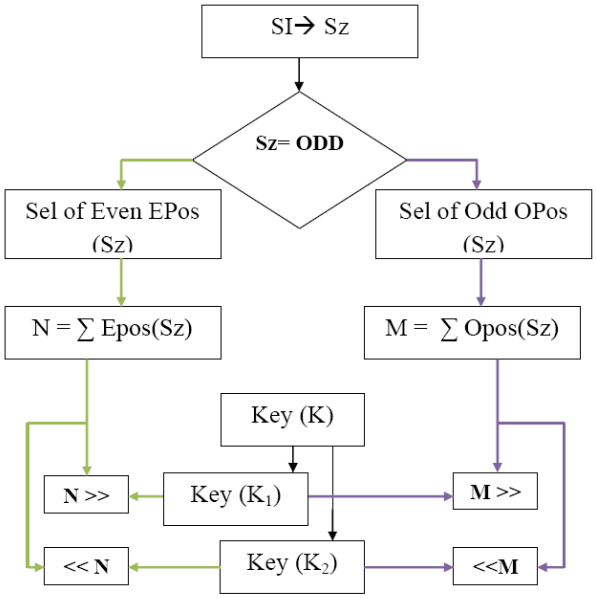


Figure 3: Architecture of Proposed Key Selection Steps of Key Selection Process.

1. Input Key K of 128 bit or 16 characters
2. Input Size (Sz) of Secret Image
3. Check If (Sz = = Even No)

   Then
4. Select Even Position (Epos) Number of Sz

   N = ∑ EPos
5. Else
6. Select Odd Position (OPos) Number of Sz

   N = ∑ OPos
7. Divide Key into two equal sub keys K_1 and K_2
8. Perform Left and Right circular shift if following way

   If (Sz = = Even)

   Than

   K_1→ N>> Nth Time Right Circular Shift

   K_2→ N << Nth Time Left Circular Shift
9. Else

   K_1→ M >> Nth Time Right Circular Shift

   K_2→ M << Nth Time Left Circular Shift
10. Now Combine K_1 and K_2 to get Final Key of 128 bits.
11. Exit

Proposed Encryption Architecture: Figure 4 is viewing the architecture of proposed encryption technique. Proposed encryption technique is based on symmetric key concept where it is using block cipher co1`ncept where confidential image are converting in cipher image block wise that means 128 bits block of secret image are encrypting at a time till all blocks of secret image. Now 128 bits form secret image and 128 bits key are performing XOR and shifting operation with each other (See figure 4). And at last S-Box concept are using hear to improve the complexity of secret image.

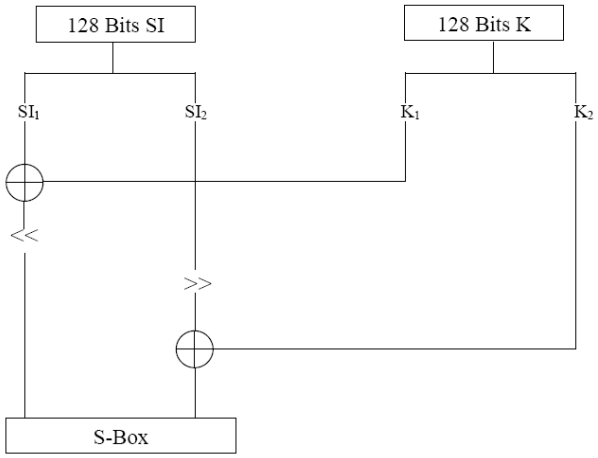


Figure 4: Architecture of proposed Encryption technique Steps of Proposed Encryption.

1. Input 128 bits of Secret Image (SI)
2. Input 128 bits Key K
3. Divide SI and K into two sub parts of equal bits (SI_1, SI_2) and (K_1, K_2) respectively.
4. Perform XOR between SI_1 and K_1. Resultant SI_1.
5. Perform 2 bits Right Circular Shift on SI_2.
6. Perform 2 bits Left Circular Shift of SI_1.
7. Perform XOR between SI_2 and K_2. Resultant SI_2
8. Pass SI_1 and SI_2 in S-Box
9. Exit.

Working principle of S-Box [4]: In this S-Box is a concept which is similar with [4] but it's a step in the proposed technique and it is improving the complexity of encryption and decryption process.

Step 1: Consider the first part of 128-bit block the Secret Information

SI_1=10110011010100011011000000011010101100110101000110110000000011011

Step 2: Take every bit of 8 or it's multiple place from the left end, which is as follows according to considered example (highlighted in red color):

11001101

Step 3: Input 1100-1101

The first 4 bits (first row) are inserted into the S-box S0 to generate a 4 bit resultant and the outstanding 4 bits (second row) are inserted into S1 to generate another 4 bit resultant. These boxes are defined as follows:

S0-Box

11 \ 00				
	8	9	10	11
	12	13	14	15
	10	11	8	9
	14	15	13	12

S1-Box

11 \ 01				
	11	10	9	8
	15	14	13	12
	9	8	10	11
	13	12	15	14

Step 4: S- box operation : The first two bits of input are treated like 2-bit number which state a row of the S-box, and the very last two input bits state column of S- box

For example if (b0,0 b0,1) = (11) and (b0,2 b0,3) = (00), then the output is from Row 1st , Column 2nd of S0, which is 14 , or (1110) in binary. Similarly (b1,0 b1,1) = (11) and (b1,2 b1,3)=(01) are used to index into S1 to produce additional 4–bit. The 8 bits produced by S0 and S1.

According to considered example, it is 14=1110 & 12=1100

Step 5: SI_{18}=1, SI_{116}=1 AND SI_{124}=1 , SI_{132}=0, SI_{140}=1, SI_{148}=1 AND SI_{156}=0 , SI_{164}=0

So consider input string of bits is look like as follows:

SI_1=10110011010100011011000100011010101100110101000110110000000011010

Random Number Generation: Blum Blum Shub (B.B.S.) is technique of pseudorandom number generator which takes the form [3]

$$x_{n+1} = x_n^2 \bmod M, \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(i)}$$

where

(i) M = ab is the product of two big primes a and b.

(ii) Consequent x_{n+1} is calculated as shown in eq (i).

First time x_n is called x_0 and it should be an integer number that is co-prime to M (where a and b are not factors of x_0) and not 1 or 0.

3. RESULTS ANALYSIS

Performance Analysis: In this performance analysis is evaluated by the proposed technique on selected parameters. These are Correlation, Key Space and Peek Signal to Noise Ratio (PSNR) Analysis. Proposed technique is implemented in MAT LAB. Results are evaluated on one cover image and four confidential image are shown below.

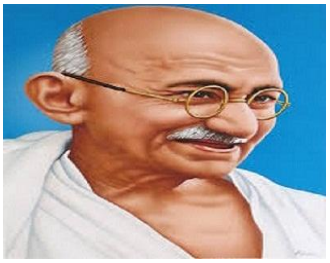


Figure 5: Mahatma Gandhi.jpg (Cover Image)

(A) Setg1.jpg

(B) Setg 2. jpg

(C) Setg 3.jpg

(D) Setg 4.jpg

Figure 6: Confidential Images (A-D) of Various Size

Peek Signal to Noise Ratio (PSNR): PSNR can be calculated as suppose that T is the entire number of pixels values in the given image or resultant image, Then MSE (Mean Squared Error) is assess as [2,3 ,4].

$$MSE = \sum_m \sum_n \frac{|R(m,n)-P(m,n)|^2}{T}$$

And PSNR is asses as

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

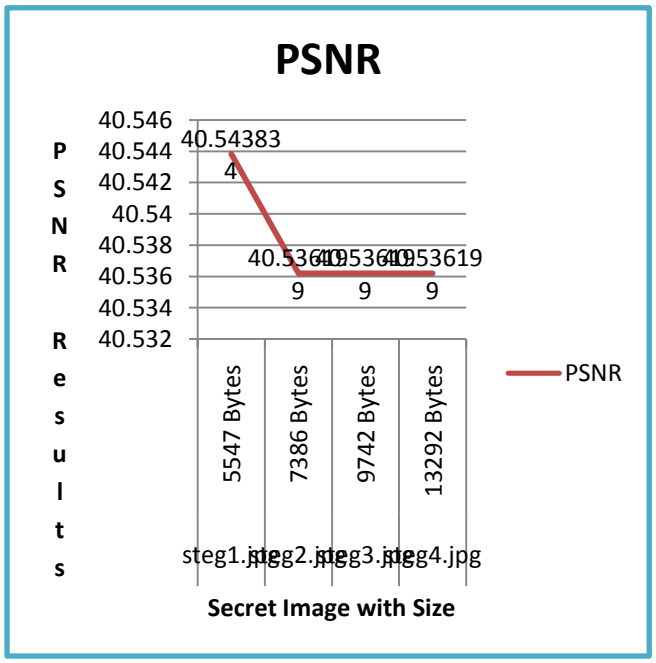
Where is the L discrete gray levels number.

And higher PSNR results be the higher stego image picture quality

Table 1 and Graph 1 is viewing the PSNR results performances of proposed technique over various secrete image.

Table 1: PSNR Results by Proposed Technique

Secret Images	Size	PSNR
steg1.jpg	5547 Bytes	40.543834
steg2.jpg	7386 Bytes	40.536199
steg3.jpg	9742 Bytes	40.536199
steg4.jpg	13292 Bytes	40.536199



Graph 1: PSNR Analysis by Proposed Technique

Correlation Analysis: In addition to the analysis of histogram, we have also analysis the correlation among two adjacent pixels, in secrete image and cipher image respectively. Firstly, we arbitrarily select n pairs of two neighboring pixels from the respective secret and cipher images. Then, we compute their correlation coefficient through the following formulas [15]:

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

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

In mathematical computations, the following discrete formulas were used [15, 16]:

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

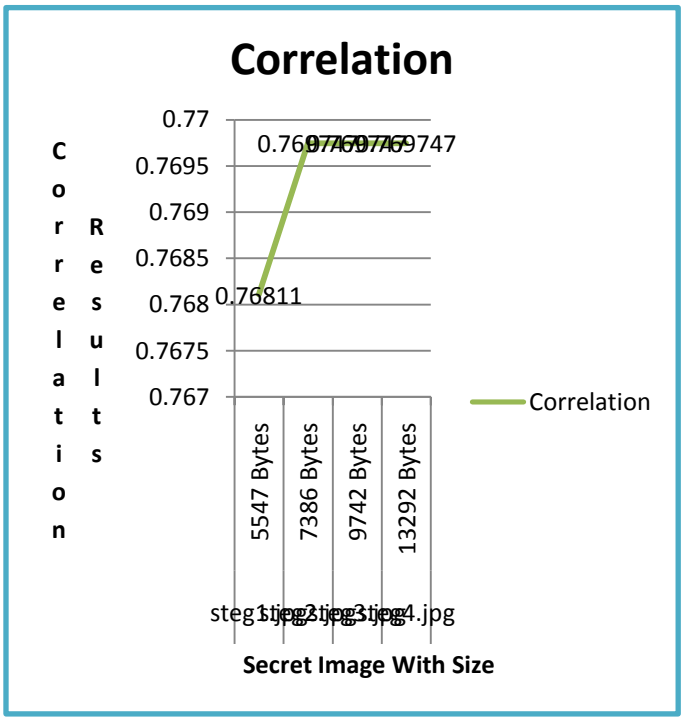
$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2,$$

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

Table 2 and Graph 2 is viewing the Correlation results performances of proposed technique over various secrete image.

Table 2: Correlation Results by Proposed Technique

Secret Images	Size	Correlation
steg1.jpg	5547 Bytes	0.76811
steg2.jpg	7386 Bytes	0.769747
steg3.jpg	9742 Bytes	0.769747
steg4.jpg	13292 Bytes	0.769747



Graph 2: Analysis of Correlation by Proposed Technique

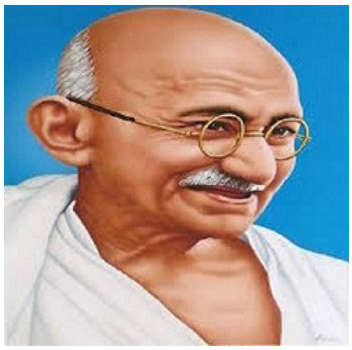


Figure 7: Stego Image

Proposed Techniques Highlighted Point:

- Capacity High: Highest size of confidential message can be embedding into image.
- Perceptual clearness: After hiding images into a cover image, eminence of perceptual will be tainted into stego image as contrast to main cover image.

- Robustness: After embedding, data should remain on essential if stego image goes into a number of transformations like filtering, addition of scaling and noise cropping.
- Temper Resistance: It should be very hard to modify the confidential message once it has been hided into stego image.
- Complexity of Computation: How much expensive it is computationally for hiding and extracting a concealed message.

Table-3 presents the best Proposed Technique measures.

Table 3: Proposed Techniques Measures

Measures	Remarks
High Capacity	Good
Perceptual Transparency	High
Robustness	Good
Temper Resistance	High
Computation Complexity	Low

Results Summary: Calculated results are shown in tables 1 to 2 and Graphs 1 to 2 for PSNR, and Correlation parameters on confidential image as an inputs and mahatmagandihi.jpg as a cover image. this analysis of confidential image with mahatma gandhi.jpg cover image it is observed that confidential images of various size 5547 Bytes, 7386 Bytes, 9742 Bytes and 13292 Bytes are producing 40.5438, 40.5361, 40.5361, 40.5361 PSNR results by "Proposed work". Likewise For correlation analysis of confidential image with leena.jpg cover image it is observed that confidential images of various size 5547 Bytes, 7386 Bytes, 9742 Bytes and 13292 Bytes are producing 0.7681, 0.7697, 0.7697 and 0.7697 Correlation results by "Proposed work" Security analysis is also proving enhanced security due to its key size (128 bits) which is impracticable to crack by brute force attacks. Finally proposed technique is proving two layers of security, first is cryptography technique and second is Steganography technique with this reason its support higher security.

4. CONCLUSION

This paper proposed a novel security technique for image as a steganography technique for unseen image files in cover images. Here we have also used a concept of cryptography technique and random number generation during steganography. So form this concept overall security of proposed technique is improving. In this proposed technique, initially cryptography technique applied on secret image and followed by steganography technique with random number generation technique. During results, we have selected some secret images (See figure 6) with cover image (see figure 5) to be concealed and accomplished that the resultant stego images do not have any perceptible changes (see figure 7). Also we founded good picture quality of the stego images in terms of (PSNR). Proposed technique works highly efficiently. Hence this novel steganography technique is robust and easy to understand.

Future Scope: Steganography Technique will carry on increasing in attractiveness over Technique of cryptography. At the time though but it will require more and more effort. Many of the steganography tools can find out the files concealed in any image. Some of the areas for further enhancement as possible compression size reduce further. There also seems very few in terms of technique and tools for beating messages in videos. There are some for audio, but this is at rest an area, which lags at the back image steganography technique. The future can see audio and video streams that could perhaps be decoded on the fly to form their exact messages.

5. REFERENCES

[1] Kumar, R.P. ; Hemanth, V. ; Shareef, M. "Securing Information Using Sterganoraphy" Published in IEEE International Conference on Circuits, Power and Computing Technologies (ICCPCT), 20-21 March 2013 Page(s):1197 - 1200 Print ISBN:978-1-4673-4921-5 INSPEC Accession Number:13583743

[2] Prabakaran, G., Bhavani, R. Rajeswari P.S. "Multi secure and robustness for medical image based steganography scheme" Published in IEEE International Conference on Circuits, Power and Computing Technologies (ICCPCT), 20-21 March 2013 Page(s): 1188 - 1193 Print ISBN:978-1-4673-4921-5 INSPEC Accession Number:13583718

[3] Ramaiya MK, Hemrajan N.i, Saxena A.K. "Security Improvisation in Image Steganography using DES" Published in IEEE 3rd International Advance Computing Conference (IACC), 22-23 Feb. 2013 Page(s): 1094 - 1099 Print ISBN:978-1-4673-4527-9 INSPEC Accession Number: 13498964

[4] Akhtar, N. ; Johri, P. ; Khan, S. "Enhancing the Security and Quality of LSB Based Image Steganography" Published in 5th IEEE International Conference on Computational Intelligence and Communication Networks (CICN), 27-29 Sept. 2013 Page(s):385 - 390 INSPEC Accession Number: 13896095

[5] Mehdi Hussain and Mureed Hussain "A Survey of Image Steganography Techniques" published in International Journal of Advanced Science and Technology Vol. 54 May , 2013 PP 113-124.Avilable at http://www.sersc.org/journals/IJAST/vol54/11.pdf

[6] Selvi, G.K. ; Mariadhasan, L. ; Shunmuganathan, K.L. "Steganography Using Edge Adaptive Image" Published in IEEE International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 21-22 March 2012 Page(s):1023 - 1027 Print ISBN: 978-1-4673-0211-1 INSPEC Accession Number: 12761978

[7] Nag A., Ghosh S., Biswas S., Sarkar D., Sarkar P.P. "An Image Steganography Technique using X-Box Mapping" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM - 2012) March 30, 31, 2012

[8] Amirtharajan, R. ; Anushiadevi, R. ; Meena, V. ; Kalpana, V. "Seeable Visual But Not Sure of It" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) 30-31 March 2012 Page(s):388 - 393 Print ISBN:978-1-4673-0213-5 INSPEC Accession Number: 12818719

[9] Das, R. ; Tuithung, T."A Novel Steganography Method for Image Based on Huffman Encoding" Published in 3rd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS), 30-31 March 2012 Page(s):14 - 18 Print ISBN: 978-1-4577-0749-0 INSPEC Accession Number:12772541

[10] Siva Janakiraman, Anitha Mary.A, Jagannathan Chakravarthy " Pixel Bit Manipulation for Encoded Hiding-An Inherent stego" Published in International Conference on Computer Communication and Informatics (ICCCI -2012), PP no 1-6 Jan. 10 – 12, 2012, Coimbatore, INDIA.

[11] Al-Abiachi, A.M. ; Inf. Technol. Dept., Univ. Utara Malaysia, Sintok, Malaysia ; Ahmad, F. ; Ruhana, K. "A Competitive Study of Cryptography Techniques over Block Cipher" Published in 13th IEEE International Conference on Modelling and Simulation March 30 2011-April 1 2011 Page(s):415 - 419 E-ISBN :978-0-7695-4376-5 Print ISBN:978-1-61284-705-4 INSPEC Accession Number:11963172

[12] Philjon, J.T.L. ; Rao, N.V. "Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption" Published in IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 3-5 June 2011 Page(s):217 - 222 Print ISBN:978-1-4577-0588-5 INSPEC Accession Number:12145614.