Design and Development of Image Security Technique by Using Cryptography and Steganography: A Combine Approach

Article *in* International Journal of Image, Graphics and Signal Processing · April 2018

DOI: 10.5815/ijigsp.2018.04.02

CITATIONS
6

READS
691

3 authors:

Aumreesh Kumar Saxena
Sagar Institute of Research and Technology
16 PUBLICATIONS **36** CITATIONS
SEE PROFILE

Sitesh Kumar Sinha
Rntu, bhopal
16 PUBLICATIONS **37** CITATIONS
SEE PROFILE

Piyush Kumar Shukla
Rajiv Gandhi Proudyogiki Vishwavidyalaya
139 PUBLICATIONS **311** CITATIONS
SEE PROFILE

I.J. Image, Graphics and Signal Processing, 2018, 4, 13-21
Published Online April 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2018.04.02

Design and Development of Image Security Technique by Using Cryptography and Steganography: A Combine Approach

Aumreesh Kumar Saxena
Research Scholar CSE Dept, AISECT University Bhopal, MP, India
Email: aumreesh@gmail.com

Dr. Sitesh Sinha
Prof. CSE Dept. AISECT University Bhopal, MP, India
Email: siteshkumarsinha@gmail.com

Dr. Piyush Shukla
Prof. CSE Dept. UIT RGPV Bhopal, India
Email: pphdwss@gmail.com

Received: 12 January 2018; Accepted: 24 February 2018; Published: 08 April 2018

***Abstract*—This paper proposes security technique for the confidential data which is the combination of three techniques, first is image compression that is based on wavelet transformation which will compress confidential image and reduce the size of the image, second is cryptography that is based on symmetric key which will encrypt the confidential image, and third is steganography that is based on least significant bit (LSB) which will embedded encrypted information inside a cover image. Therefore the purpose of the proposed technique is the high security and quality of the reconstructed cover image.**

***Index Terms*—Security, Cryptography, Steganography, Symmetric Key, Encryption, Decryption, Wavelet Transform, Image Compression**

I. Introduction

Security of confidential data is the prime issue in today's digital world. Steganography is one of the solutions to provide security, basically it is an art of hiding confidential data inside another image called cover image [1]. Normal user cannot see to the confidential data directly, once it is hidden in cover image. Hidden data is invisible to unauthorized user and only authorize user can see confidential data by using proper process of steganography method. Beside steganography another security technique is also available called cryptography [2]. Cryptography convert secrete data into unreadable form, generally it is called encryption and through decryption unreadable form convert into readable form. Normally only one security approach is used at a time by the users either cryptography or steganography [2, 3]. As we know that cryptographic technique is most useful and powerful security technique, so the combination of steganography and cryptography can be playing a very important role in this field.

The equation (1) describing a very simple method of steganography:

$$\text{Cover Image} + \text{Secrete Data} + \text{Key} = \text{Stego Imag} \quad (1)$$

In eq.1, Secrete data will hide inside of the cover image through suitable and strong key concept like LSB or MSB to produced stego image. Secrete data can be encrypted through cryptography technique; it will depend on the concept used by the user [4]. The primary concern of the steganography method is to hide a secret data inside cover image so that secrete data will invisible to the unauthorized user [5, 6].

Prime focused of this paper is to design and develop secure and efficient symmetric cryptography method for encrypt secret data to implement steganography method. The proposed symmetric cryptography method plays an important role in the steganography method to indicate the user need for the security. The paper is organized as follows: Section 2 presents related work and comparative analysis of existing work. Section 3 presents some common issues. Section 4 presents the proposed work. Section 5 presents the performance analysis of proposed steganography method in terms of result. Finally Section 6 offers conclusions.

II. Related Work

In [7] presented steganography method that is based on block matching in DWT domain. By using naïve BM technique which improve the quality of the reproduced

secret image. In [8] presented steganography method by implement a random key generator as a method. Stream cipher (LFSR) is the basic idea behind random key generator. Another thing which is use known beta that will consequence on the selection of the cover image. In [9] presented steganography method which is the combination of image steganography and cryptography. For Encrypt secrete data they used content based encryption technique and raster scan method along with LSB is used for image steganography. In [10] presented steganography method which is the combination of cryptography and steganography. In cryptography they used RSA for encryption/decryption and least significant bit image steganography for hiding data. In [11] presented steganography method which is also the combination of cryptography and steganography. In steganography they used sequential technique and Symmetric XOR technique for Cryptography. In [12] presented another steganography method which is used RSA encryption technique to encrypt secrete data as a cipher block and these blocks are inserted into cover image by mapping using breadth first search (BFS).

In [13] presented steganography method which is used least significant bit (LSB) technique for cover image and most significant bit (MSB) is used for secret image. Along with this dynamic key cryptography mechanism is also used for encryption. In [14] presented steganography method which is providing two level securities. They are using 2D Arnold Cat Map technique to scramble secret data in a random order after that encrypted data is concealed behind a cover image using basic LSB method. Table 1 is showing comparative analysis of existing steganography method based on steganography, cryptography and transformation technique which they have used.

Table 1. Comparative analysis of existing techniques

S. No.	Author's and Title	Steganography	Cryptography	Transformation	Remarks
1	Jaeyoung Kim; Hanhoon Park; Jong-Il Park "Image steganography based on block matching in DWT domain" -2017	Least Significant Bits (LSB)	X	integer wavelet transform (IWT)	Security can be Enhanced
2	Ismael Abdul Sattar; Methaq Talib Gaata Image steganography technique based on adaptive random key generator with suitable cover selection" -2017	Self Design	Adaptive Random Key Generator	X	Length of the Key Generator can be Manageable
3	Shivani Chauhan; Jyotsna; Janmejai Kumar; Amit Doegar "Multiple Layer Text security Using variable block size cryptography and image steganography" -2017	Least Significant Bits (LSB)	Variable block size data encryption	X	Efficiency can be increased
4	Shubhi Mittal; Shivika Arora; Rachna Jain "PData security using RSA encryption combined with image steganography" -2016	Least Significant Bits (LSB)	RSA	X	It Can be suitable for Small amount of Data
5	M. Saritha; Vishwanath M. Khadabadi; M. Sushravya "Image and text steganography with cryptography using MATLAB" -2016	Not Known	Symmetric	X	Efficiency can be increased
6	Mamta Jain; Rishabh Charan Choudhary; Anil Kumar "Secure medical image steganography with RSA cryptography usingdecision tree" -2016	Least Significant Bits (LSB)	RSA	X	It Can be suitable for Small amount of Data
7	Nikhil Patel; Shweta Meena "LSB based Image steganography using Dynamic key cryptography" -2016	Least Significant Bits (LSB)	pseudo noise sequences	Inverse transform	Efficiency can be increased
8	Rupali Bhardwaj; Divya Khanna Enhanced the security of image steganography through image encryption" -2015	Least Significant Bits (LSB)	X	Arnold Transform	Security can be Enhanced

III. Issues

After analysis of existing steganography method, we have observed some common issues which are as follow:

- **Security:** Security of the secret data is primary issues if we send secret data from one end to another end through public transmission like internet. There are many existing techniques are using extra effort to protect secret data like asymmetric and symmetric cryptography technique to encrypt secret data before hiding in cover image but this is not efficient because flaws of these type of cryptography techniques.
- **Correlation:** Depending on the manner in which the secrete data is concealed; various type of manipulations may destroy the secret data.

- **Efficiency:** Another issue is the efficiency of the algorithm. Efficiency of any algorithm can by evaluated by execution time and memory space occupied by the algorithm. There are many existing method which is taking too much time in execution and lots of memory space required.
- **Reliability:** There are many steganography methods which leave a sign during hiding secret data which can be detectable. Such types of methods are not reliable.

IV. Proposed Work

Common view of proposed concept is shown in figure 1. Initially we select secrete image then apply image compression technique that is wavelet transform to reduce size of secret image. After that we read binary data from compressed image which is passed to the encryption technique to convert into cipher data by using proposed symmetric cryptography technique. At last encrypted data hide through proposed steganography technique which is using least significant bit (LSB) mechanism to produce final image which will treat as Cover Image. Basically proposed work is the combination of three different techniques which are following:

A. Wavelet Transform
B. Symmetric Cryptography
C. Steganography

A. Wavelet Transform

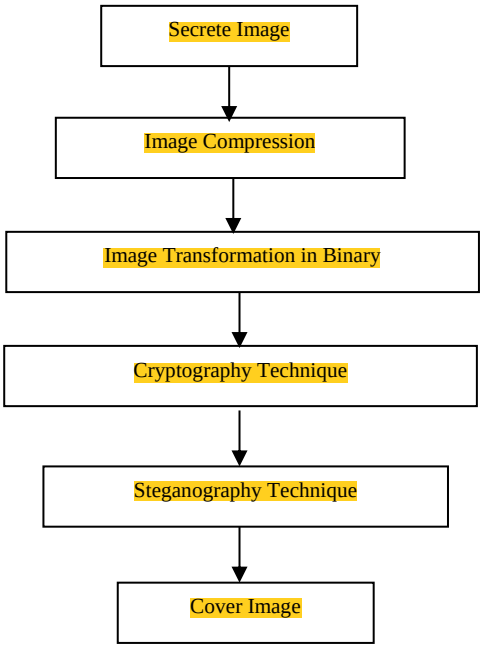


Fig.1. Common View of Proposed Concept

Lossy and Lossless compression is the type of wavelet compressions. The uses of these techniques are very common because it can be reduce the size of image without losses of information [15]. Original image can be reproduced from compressed image according lossless compression where lossy compression reproduced partially. Less space is required to store data by wavelet transformation which is very easy to compress image [15].

Wavelet Compression steps are as follow:

1. Upload the Selected Image,
2. Wavelet Decomposition of the Image
3. Image Compression through a Threshold Value.

B. Symmetric Cryptography

Symmetric cryptography technique has two processes one is encryption and second is decryption. In encryption process compressed image data will convert into unreadable data that is called cipher data and that cipher data decrypted in decryption process to convert into readable data.

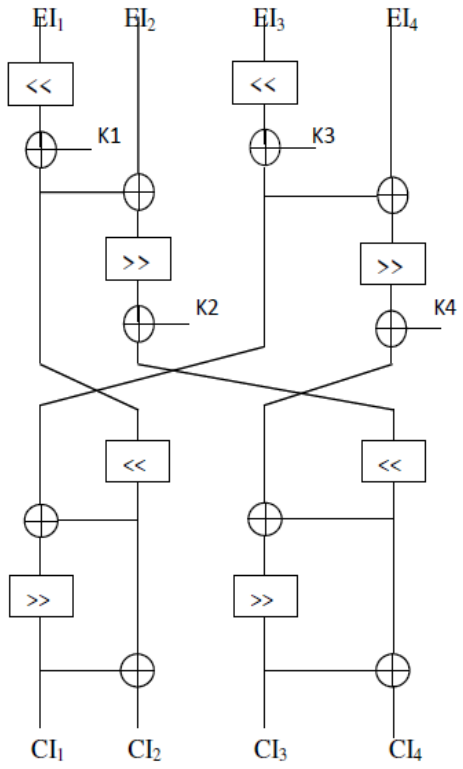


Fig.2. Proposed Encryption Architecture

1. **Encryption:** Proposed encryption architecture is shown in figure 2. Proposed encryption process is using two logical operations one is "XOR" and second is "circular shift" operation. In circular shift we used both type left and right circular shift operations. All these type of operations are working between binary value of compressed secret image and secret symmetric key respectively to produced cipher data. Initially read binary value of compressed secrete image (EI) and select 128 bits at a time for further processing with secrete key (K) which is also 128 bits in size. Here EI and K is divided in four equal sub part (EI_1, EI_2, EI_3, EI_4) and (K_1, K_2, K_3, K_4,) which is 32 bits

each respectively. After that we have applied 2 bits left circular shift and 2 bits right circular shift on sub parts of EI (for more information see figure 2) and performing XOR operation between sub parts of EI. Also the XOR operation is performing between sub parts of EI and K (for more information see figure 2). Finally perform all predefined step one by one to get cipher data. For more description see encryption algorithm.

Encryption Algorithm

1. Start
2. Looping: For N = 1 to 12 (N is the total number of round executed by proposed steps)
3. Selection: Initial 128 Binary Value of Confidential Image 'EI' Selected

$EI \rightarrow$ 128 bits (at once)

3. Selection: Now 128 bits Secrete Key 'K' Selected

$K \rightarrow$ 128 bits

4. Division: Divide 128 Binary Value of Confidential Image 'EI' and 128 bits Secrete Key 'K' into 4 equal sub parts like (EI_1, EI_2, EI_3, EI_4) and (K_1, K_2, K_3, K_4,) respectively

$EI = EI/4 \rightarrow (EI_1, EI_2, EI_3, EI_4)$

$K = K/4 \rightarrow (K_1, K_2, K_3, K_4)$

5. Left Circular Shift with 2 bits: Apply Left Circular Shift with 2 bits on first sub parts EI_1 to produced new EI_1 and third sub parts EI_3 to produced new EI_3 of Confidential Image 'EI'

$EI_1 = 2 \rightarrow (EI_1)$

$EI_3 = 2 \rightarrow (EI_3)$

6. XOR: Apply XORing between new EI_1 that is produced in step 5 & first sub parts of secret key K_1 to produced another new EI_1 and new EI_3 that is produced in step 5 & third sub parts of secret key K_3 to produced another new EI_3

$$EI_1 = EI_1 \bigoplus K_1$$

$$EI_3 = EI_3 \bigoplus K_3$$

7. XOR: Apply XOR between second sub parts EI_2 of Confidential Image 'EI' & new EI_1 that is produced in step 6 to produced new EI_2 and fourth sub parts EI_4 of Confidential Image 'EI' & new EI_3 that is produced in step 6 to produced new EI_4

$$EI_2 = EI_2 \bigoplus EI_1$$

$$EI_4 = EI_4 \bigoplus EI_3$$

8. Right Circular Shift with 2 bits: Apply right Circular Shift with 2 bits on new EI_2 and new EI_4 that is produced in step 7 to produced new EI_2 and EI_4 respectively

$EI_2 = 2 \rightarrow (EI_2)$

$EI_4 = 2 \rightarrow (EI_4)$

9. XOR: Apply XOR between new EI_2 that is produced in step 8 & second sub parts of secret key K_2 and new EI_4 that is produced in step 8 & fourth sub parts of secret key K_4 to produced another new EI_2 and EI_4 respectively

$$EI_2 = EI_2 \bigoplus K_2$$

$$EI_4 = EI_4 \bigoplus K_4$$

10. Interchange: Now interchanging the value of EI_1 into EI_2, EI_2 into EI_4, EI_3 into EI_1, and EI_4 into EI_3

$EI_1 \rightarrow EI_2$

$EI_2 \rightarrow EI_4$

$EI_3 \rightarrow EI_1$

$EI_4 \rightarrow EI_3$

12. Left Circular Shift with 2 bits: Apply Left Circular Shift with 2 bits on EI_2 and EI_4 that is produced in step 10 to produced EI_2 and EI_4 respectively

$EI_2 = 2 \rightarrow (EI_2)$

$EI_4 = 2 \rightarrow (EI_4)$

13. XOR: Apply XORing between EI_2 of step 12 & EI_1 of step 10 and EI_4 of step 12 & EI_3 of step 10 to produced EI_1 and EI_3 respectively

$$EI_1 = EI_2 \bigoplus EI_1$$

$$EI_3 = EI_4 \bigoplus EI_3$$

14. Right Circular Shift with 2 bits: Apply right Circular Shift with 2 bits on EI_1 and EI_3 of step 13 to produced cipher text CI_1 and CI_3 respectively.

$CI_1 = 2 \rightarrow (EI_1)$

$CI_3 = 2 \rightarrow (EI_3)$

15. XOR: Apply XORing between EI_2 of step 12 & EI_1 of step 13 and EI_4 of step 12 & EI_3 of step 13 to produced cipher text CI_2 and CI_4 respectively.

$$CI_2 = EI_2 \bigoplus EI_1$$

$$CI_4 = EI_4 \bigoplus EI_3$$

16. End Loop: Repeat Step-2 to step-15 for 12 round.
17. Exit

2. **Proposed Decryption:** Proposed decryption architecture is shown in figure 3. Proposed decryption is just reverse process of encryption where we get original data from cipher data. Initially we read binary value of encrypted image (CI) and select 128 bits at a time for further processing with secrete key (K) which is also 128 bits in size. Here encrypted image (CI) and Key K is divided in four equal sub part like (CI1, CI2, CI3, CI4) and (K1, K2, K3, K4,) which is 32 bits each respectively. Now once again we used same logical operation like "XOR" and Circular Shift" but in different way to get original data. Circular shift operation executed in reverse order in decryption process like that we have applied 2 bits left circular shift and right circular shift on sub part of CI (for more information see figure 3) in reverse and performing XOR operation between sub parts of CI. Also perform XOR operation between sub parts of CI and K (for more information see figure 3). For more description see decryption algorithm

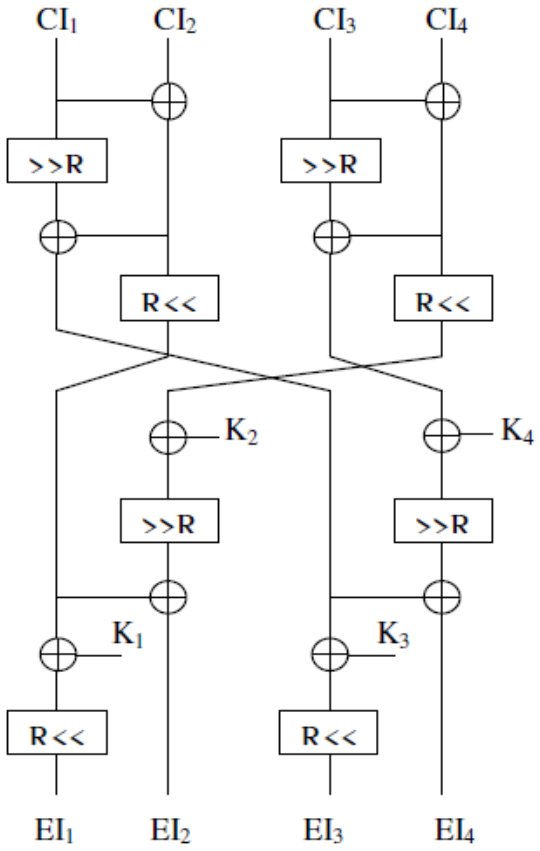


Fig.3. Proposed Decryption Architecture

Decryption Algorithm

1. Start
2. Looping: For N = 1 to 12 (N is the total number of round executed by proposed steps)
3. Selection: Initial 128 binary value of encrypted secrete image CI selected
   CI→ 128 bits (at once)
4. Selection: Now 128 bits secrete key 'K' selected
   K→ 128 bits
5. Division: Divide 128 Binary Value of encrypted secret image 'CI' and 128 bits Secrete Key 'K' into 4 equal sub parts likes (CI1, CI2, CI3, CI4) and (K1, K2, K3, K4,) respectively
   CI = CI/4→ (CI_1, CI_2, CI_3, CI_4)
   K = K/4→ (K_1, K_2, K_3, K_4)
6. XOR: Apply "XOR" between second sub part CI_2 & first sub parts CI_1 of encrypted secret key image 'CI' to produced new CI_2 and fourth sub part CI_4 & third sub parts CI_1 of encrypted secret key image 'CI' to produced new CI_4

$$CI_2 = CI_2 \oplus CI_1$$

$$CI_4 = CI_4 \oplus CI_3$$

7. Reverser Right Circular Shift with 2 bits: Apply 2 bits right circular shift in reverse on first sub part CI_1 and third sub part CI_3 of encrypted secret key image 'CI' to produced new CI_1 and CI_3
   $CI_1 = 2\rightarrow (CI_1)$
   $CI_3 = 2\rightarrow (CI_3)$
8. XOR: Apply "XOR" between new CI_1 of step 7 & new CI_2 of step 6 and new CI_3 of step 7 & new CI_4 of step 6 to produced new CI_1 and CI_3

$$CI_1 = CI_1 \oplus CI_2$$

$$CI_3 = CI_3 \oplus CI_4$$

9. Reverser Left Circular Shift with 2 bits: Apply 2 bits left circular shift in reverse on CI_2 and CI_4 of step 6 to produced another new CI_2 and CI_4
   $CI_2 = 2\rightarrow (CI_2)$
   $CI_4 = 2\rightarrow (CI_4)$
10. Interchange: Now interchanging the value of CI_1 into CI_3, CI_2 into CI_1, CI_3 into CI_4, and CI_4 into CI_2
    $CI_1 \rightarrow CI_3$
    $CI_2 \rightarrow CI_1$
    $CI_3 \rightarrow CI_4$
    $CI_4 \rightarrow CI_2$
11. XOR : Apply "XOR" between new CI_2 of step 9 & second sub part K_2 of secret key 'K' and new CI_4 of step 9 & fourth sub part K_4 of secret key 'K' to produced new CI_2 and CI_4

$$CI_2 = CI_2 \oplus K_2$$

$$CI_4 = CI_4 \oplus K_4$$

12. Reverse Right Circular Shift with 2 bits: Apply 2 bits right circular shift in reverse on new CI_2 and new CI_4 of step 11 to produced new CI_2 and CI_4
    $CI_2 = 2\rightarrow (CI_2)$
    $CI_4 = 2\rightarrow (CI_4)$
13. XOR: Apply "XOR" between new CI_1 of step 9 & new CI_2 of step 11 and new CI_3 of step 9 & new CI_4 of step 11 to produced new CI_2 and CI_4

$$CI_2 = CI_2 \oplus CI_1$$

$$CI_4 = CI_4 \oplus CI_3$$

14. XOR: Apply "XOR" between new CI_1 of step 9 & first sub part K_1 of secret key 'K' and new CI_3 of step 9 & third sub part K_3 of secret key 'K' to produced new CI_1 and CI_3

$$CI_1 = CI_1 \oplus K_1$$

$$CI_3 = CI_3 \oplus K_3$$

15. Reverse Left Circular Shift with 2 bits: Apply 2 bits left circular shift in reverse on CI_1 and CI_3 of step 14 to produced another new CI_1 and CI_3
    $CI_1 = 2\rightarrow (CI_1)$
    $CI_3 = 2\rightarrow (CI_3)$
16. End Loop: Repeat Step-2 to step-15 for 12 round.
17. Exit

C. Proposed Steganography

In steganography technique, large size of images is used as cover image to concealed secret images. Proposed steganography technique works on spatial domain and Least Significant Bits (LSB) technique is used to hide to secrete image. There are two proposed steganography algorithm which are "hiding secret image" and "extracting secret image". Hiding secret image algorithm is hiding encrypted secret image behind a cover image that is large in size. Extracting secrete image is reading

encrypted secret image information from cover image and reforming encrypted secret image.

Hiding Secret Image

1. Start
2. Select Cover Image Cov_Img
   Cov_Img = Image→Cov_Imge
3. Select Encrypted Secrete Image CI
   CI = Image→CI
4. Read binary value of encrypted secret image
   Bin_CI = Bin_CI→ (0, 1)
5. Read binary value of cover image
   Bin_Cov_Img = Bin_Cov_Img→ (0, 1)
6. Select least significant bits from cover image
   LSB_Cov_Img = LSB_Reader (Cov_Img)
7. Replace one by one least significant bits of cover image from binary value of encrypted secret image
   LSB_Cov_Img = Bin_CI
8. Exit

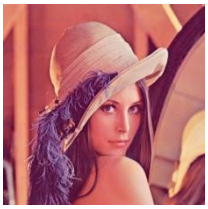
Extract Secret Image

1. Start
2. Select Steganography Image
   Stega_Img = Image→Stega_Img
3. Read binary value from steganography image
   Bin_Stega_Img = Binary_Stega_Image (0,1)
4. Read least significant bit from steganography image
   LSB_Binary_Stega_Image (0,1)
5. One by one insert all least significant bit of steganography to produced image as secret image
   CI = LSB_Binary_Stega_Image (0,1) →CI
6. Exit

V. Simulation

The testing conducted on two cover images and five secret images of various sizes; the secret image is entrenched into LSB of the cover image. The entropy, peak signal-to-noise ratio (PSNR) and correlation were examined. The entropy indicates the quality of the cover image. The lower the value of entropy is the better quality. PSNR indicate the resemblance between the cover image and stego image [16]. The better image quality is propositional to the higher value of PSNR. Correlation is simple operation which is applied horizontally, vertically or diagonally on image pixel to extract information [18, 19]. The proposed algorithm executed several time on various machine and each time different size of data was selected for execution. In this work we have selected two cover image named are monalesa.jpg and Lena.jpg shown in figure 4 (a) and (b). Size of secrete images are shown in table 1.

(a) Monalesa.jpg



(b) Lena.jpg

Fig.4. Cover Images

A. 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 by using equation (2) [16, 17].

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

and PSNR calculated by using equation (3)

$$PSNR = 10\log_{10} (L-1)^2 \quad (3)$$

PSNR of various secretes images with Leena and monaleesa cover images are shown in table 2 and 3. Figure 5 shown Pictorial representations for the same.

Table 2. Psnr analysis of proposed concept over leena.jpg

		PNSR
Secrete Image	**Size**	**Propose Work**
Im1	1.85 KB	43.4125
Im2	2.72 KB	43.4225
Im3	3.68 KB	43.4225
Im4	4.36 KB	43.5064
Im5	9.35 KB	43.5112

Table 3. Psnr analysis of proposed concept over monalesa.jpg

		PNSR
Secrete Image	**Size**	**Propose Technique**
Im1	1.85 KB	43.4125
Im2	2.72 KB	43.4225
Im3	3.68 KB	43.4225
Im4	4.36 KB	43.5064
Im5	9.35 KB	43.5112

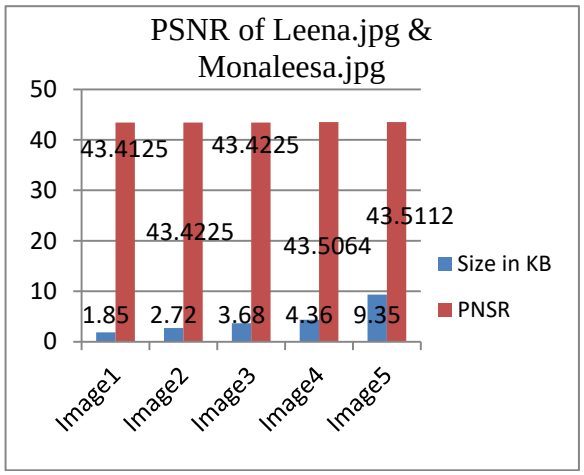


Fig.5. Pictorial Representation of PSNR

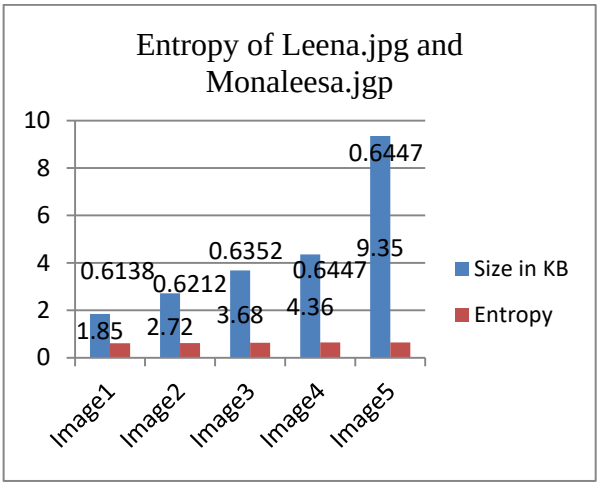


Fig.6. Pictorial Representation of Entropy

B. *Entropy Analysis*

Entropy calculated by using equation (4) [18].

$$H_e = -\sum_{k=0}^{G-1} p(k)\log_2\left(p(k)\right) \qquad (4)$$

Where

He: entropy.
G: gray value of input image (0…255).
P(k): probability of the occurrence of symbol K.

Entropy of various secretes images with Leena and monaleesa cover images are shown in table 4 and 5. Figure 6 shown Pictorial representations for the same.

Table 4. Entropy analysis of proposed concept over leena.jpg

		Correlation
Secrete Image	**Size**	**Propose Work**
Im1	1.85 KB	0.6138
Im2	2.72 KB	0.6212
Im3	3.68 KB	0.6352
Im4	4.36 KB	0.6447
Im5	9.35 KB	0.6447

Table 5. Entropy analysis of proposed concept over monalesa.jpg

Input		Correlation
Secrete Image	**Size**	**Propose Work**
Im1	1.85 KB	0.6138
Im2	2.72 KB	0.6212
Im3	3.68 KB	0.6352
Im4	4.36 KB	0.6447
Im5	9.35 KB	0.6447

C. *Correlation Analysis*

Correlation [19] of various secretes images with Leena and monaleesa cover images are shown in table 6 and 7. Figure 7 shown Pictorial representations for the same.

Table 6. Correlation analysis of proposed concept over leena.jpg

Input		Correlation
Secrete Image	**Size**	**Propose Work**
Im1	1.85 KB	0.5235
Im2	2.72 KB	0.5245
Im3	3.68 KB	0.5245
Im4	4.36 KB	0.5555
Im5	9.35 KB	0.5555

Table 7. Correlation analysis of proposed concept over monalesa.jpg

		Correlation
Secrete Image	**Size**	**Propose Work**
Im1	1.85 KB	0.5235
Im2	2.72 KB	0.5245
Im3	3.68 KB	0.5245
Im4	4.36 KB	0.5555
Im5	9.35 KB	0.5555

The proposed technique is providing higher security and quality as compare to existing techniques because the high occurrence components scarcely differ while the small occurrence components very much differ crosswise the images with dissimilar contrast. PSNR results are showing in table 2 and table 3 for leena.jpg and monaleesa.jpg respectively on various size of secret image, after conceal an image file of 1.87 KB, the PSNR value is 43.4125 produced for both type of cover image

respectively. Similarly for an image file of 2.72 KB, 3.68 KB, 4.36 KB and 9.35 KB, the PSNR values are 43.4225, 43.4225, 43.5064 and 43.5112 respectively for both type of cover image. From the results we have observed that PSNR value is directly proportional with increasing file size which shows better quality of stego image and form image we can visualized that there is no difference between main cover image and stego image. Similarly entropy and correlation results are showing in table 4-5 and table 6-7 for leena.jpg and monaleesa.jpg respectively on various size of secret image, after conceal an image file of 1.87 KB, 2.72 KB, 3.68 KB, 4.36 KB and 9.35 KB, the entropy values are 0.6138, 0.6212, 0.6352, 0.6447 and 0.6447 produced for both type of cover image respectively. Similarly the correlation values are 0.5235 0.5245, 0.5245, 0.5555 and 0.5555 produced for both type of cover image respectively on the same size of secrete image. Lower entropy and correlation value shows better quality for stego image which is proved by the results that is produced by the proposed algorithm. One more thing that correlation shows that image pixels are strongly adjusted in reconstructed cover image to maintain quality. Results (table 2-7) proved the quality and effectiveness of the stego image produced by proposed algorithm when the increasing size of secret image for a flat cover image. Another thing is also notified that PSNR, Entropy and Correlation is continually rising with the rising of size of secrete image. At last cryptography technique proved one level ahead security.

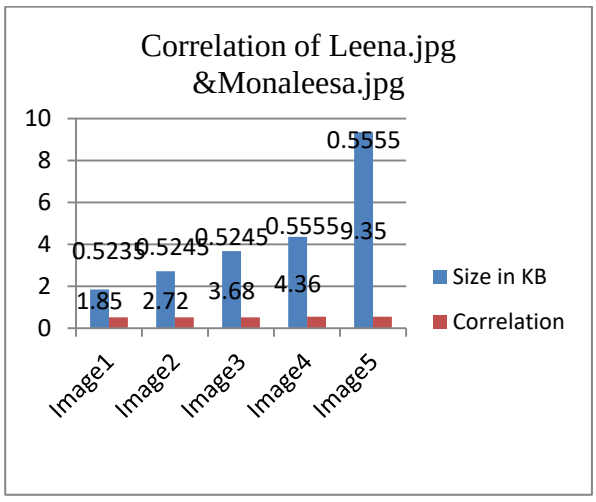


Fig.7. Pictorial Representation of Correlation

VI. Conclusion

In this paper, a novel image security technique is presented which is the combination of image compression that is based on wavelet transform, cryptography that is based on symmetric key and steganography that is based on LSB. Security of the confidential image is the primary concern and stego image quality is another concern of the proposed technique. Proposed technique proved that two layer securities are the sufficient at primary level and image quality not degrading after reconstruction cover image.

References

[1] 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), Page(s): 1188 – 1193, India 2013 ,

[2] 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), Page(s): 385 – 390 India 2013 ,

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

[4] 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 Pages(s):415-419 UK 2011

[5] 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) Pages(s): V1-141-V1-145, Japan 2010

[6] 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 Page(s): 474-479, USA - 2009

[7] Jaeyoung Kim; Hanhoon Park; Jong-Il Park "Image steganography based on block matching in DWT domain" IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Page(s):1 – 4, Italy-2017

[8] Ismael Abdul Sattar; Methaq Talib Gaata Image steganography technique based on adaptive random key generator with suitable cover selection" Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Page(s):208-212 Iraq- 2017

[9] Shivani Chauhan; Jyotsna; Janmejai Kumar; Amit Doegar "Multiple Layer Text security Using variable block size cryptography and image steganography" 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Page(s):1-7, India-2017

[10] Shubhi Mittal; Shivika Arora; Rachna Jain "PData security using RSA encryption combined with image steganography" 1st India International Conference on Information Processing (IICIP), Page(s):1-5, India-2016

[11] M. Saritha; Vishwanath M. Khadabadi; M. Sushravya "Image and text steganography with cryptography using MATLAB" International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) page(s): 584-587, India-2016.

[12] Mamta Jain; Rishabh Charan Choudhary; Anil Kumar "Secure medical image steganography with RSA cryptography usingdecision tree" 2nd International Conference on Contemporary Computing and Informatics (IC3I), Page(s):291-295, India- 2016

[13] Nikhil Patel; Shweta Meena "LSB based Image steganography using Dynamic key cryptography" 2016 International Conference on Emerging Trends in Communication Technologies (ETCT), Pages(s): 1-5,India-2016
[14] Rupali Bhardwaj; Divya Khanna Enhanced the security of image steganography through image encryption" Annual IEEE Conference (INDICON), Page(s):1-4, India-2015
[15] Kalpana Sanjay Shete, Mangal Patil and J. S. Chitode "Least Significant Bit and Discrete Wavelet Transform Algorithm Realization for Image Steganography Employing FPGA" MECS I.J. Image, Graphics and Signal Processing, Vol. 6, Pp-48-56, 2016
[16] T. Bhattacharya, N. Dey, and S.R.B. Chaudhuri, "A session based multiple image hiding technique using DWT and DCT," International Journal of Computer Application (IJCA), vol. 38, no. 5, pp. 398–409, 2012.
[17] G V Chaitanya, D Vamsee Krishna, L Anjaneyulu "A 3-Level Secure Histogram Based Image Steganography Technique" MECS I.J. Image, Graphics and Signal Processing, Vol. 4, Pp- 60-70, 2013
[18] M.K Ramaiya. ; N.Hemrajani, ; , A.K Saxena. "Security improvisation in image steganography using DES" IEEE 3rd International on Advance Computing Conference (IACC), Page(s): 1094 – 1099, India-2013
[19] S. Laskar, and K. Hemachandran, "High Capacity Data Hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol. 4, No. 6, pp. 57-68, December 2012.

Authors' Profiles

Mr. Aumreesh Kumar Saxena is a Research Scholar in the Department of Computer science and engineering, AISECT University, Bhopal. He has obtained his M.Tech degree from Department of Computer science and Engineering UIT, BU University, Bhopal. He is also a technical reviewer of IJCSIS. He can be reached at aumreesh@gmail.com.

Dr. Sitesh Kumar Sinha is working as a professor in department of computer science and engineering, AISECT University, Bhopal. He has obtained PhD degree from BRAB MIT, muzaffarpur, Bihar. He is completed government funding project during his PHD work related on computer Network. He is published more than 20 research paper in various international and national journals. He can reach at siteshkumarsinha@gmail.com.

Dr. Piyush Kumar Shukla is working as an Assistant professor in department of computer science and engineering, UIT RGPV University, Bhopal. He has obtained PhD degree from RGPV University, Bhopal. His area of interest is data communication, networking and network security. He is published more than 30 research paper in various international and national journals. He can reach at pphdwss@gmail.com.

How to cite this paper: Aumreesh Kumar Saxena, Sitesh Sinha, Piyush Shukla," Design and Development of Image Security Technique by Using Cryptography and Steganography: A Combine Approach", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.10, No.4, pp. 13-21, 2018.DOI: 10.5815/ijigsp.2018.04.02