International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 10, October 2014 **ISSN 2319 - 4847**

EMSEMBLE APPROACH FOR HIDDING DATA IN STEGANOGRAPHY

[1]Ruchi Jain, Piyush Singh[2]

[1]Department of Information Technology, RKDF
RGPV University, INDIA

[2]Assistant Professor, Department of Information Technology, RKDF
RGPV University, INDIA

ABSTRACT

In today's era the one of the main communication method is internet. Beside of having so many advantages it has some disadvantages too. Because of so many hackers, our data is not secure and safe. There are so many methods by which we can secure our data. Cryptography is one of it. But the main problem is that by using Cryptography, the cipher text is visible to the unwanted user. In this paper the concept of stegnography is used. Stegnography is the method to hide data so that any information will not be received by third party by remains unaware about the presence of secret message. The work is based on Encryption using stegnography that proposes an encryption algorithm based on cipher text. Further the secret text will be embedded with cover image that generates a stereo image of its same size of cover image. After that decryption process is used to produce cipher secret information and finally wavelet transform is used to uncompressed secret information.

Keywords:-.Terms-Information hiding, Steganography, Logical OperationsRandom number generator, Transformation technique.

1. INTRODUCTION

Present days all data the knowledge the data is keep within the kind of digital media. By victimization the web as a medium several info is transferred from one person to a different person. Each system can give completely different security mechanisms for outgoing packets. The sender and receiver assurances that the is information is firmly transferred. however the data is transferred over covered (insecure) channel, if anyone will get the encrypted info and by applying cryptography the reason, the entrant will get the initial message the oppose will even alter the data and pass to the receiver. Two kinds of mechanisms square measure there to produce security for the information, they're cryptography and steganography. Cryptography means that changing the text from readable format to unclear format.[1, 2, 3, 4]

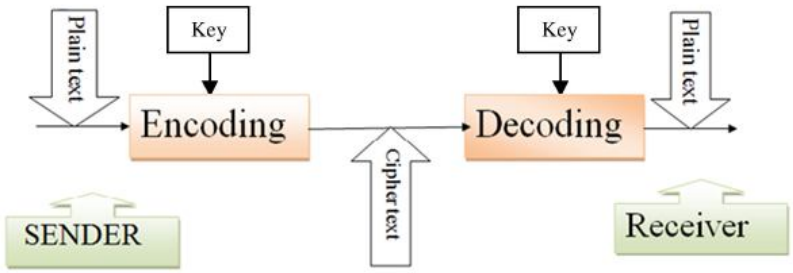

Figure 1.1: Block Diagram of Cryptography

But the encrypted text is visible to any or all, by applying cryptanalysis on cipher text, the unwelcome person will get the first message, otherwise he will alter the cipher text. Steganography is used for concealing the knowledge in a picture [1, 3, 5].The information is not visible. the essential steganographic mode is shown below.

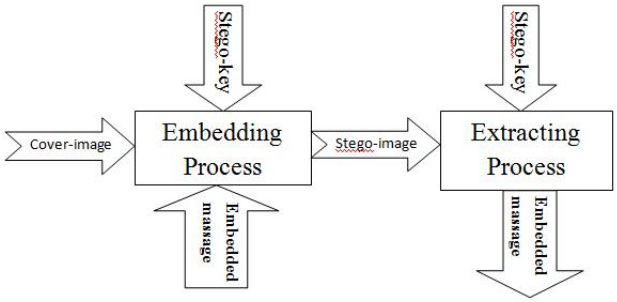

Figure 1.2: Block Diagram of Stegnographic

There are 3 differing types of steganographic techniques are obtainable for concealing the knowledge in a picture, that is Least vital Bit Insertion, Masking, and Transformation techniques. The higher than 3 techniques having their own characteristics. Least vital bit insertion is that the best technique for embedding the key info in a picture with less noise, however it's applicable just for a little quantity of data. Transformation techniques are helpful for embedding the large amount of knowledge in a picture the biggest disadvantage in transformation technique is it produces a lot of noise within the stego Image. By using transformation techniques we can embed large amount of data while LSB insertion techniques limited to small amount of data

2. LITERATURE SURVEY

Potdar et al. [6] used a spacial domain technique in manufacturing a fingerprinted secret sharing steganography for strength against image cropping attacks. Their paper self-addressed the difficulty of image cropping effects instead of proposing associate embedding technique. They divide the duvet image into sub- pictures and compress and code the key information. Shirali-Shahreza and Shirali-Shahreza [7] exploited Arabic and Persian alphabet punctuations to cover messages. whereas their technique is not associated with the LSB approach, it falls into the special domain if the text is treated as a picture. Jung associated Yoo [8] down-sampled an input image to half its size and so used a changed interpolation technique, termed the neighbor mean interpolation (NMI), to up-sample the result back to its original dimensions prepared for embedding. Piyu Tsai et al. [9] divided the image into blocks of 5x5, wherever the residual image is calculated mistreatment linear prediction. Then the key information is embedded into the residual values, followed by block reconstruction. Li and Wang [10] conferred a steganographic technique that modifies the quantization table of JPEG pictures and inserts the hidden bits within the middle frequency coefficients. information is inserted into separate circular function remodel (DCT) coefficients ' insignificant bits '. Rubata et al [11] projected a completely unique hash-based approach for colour image steganography for cryptography text information in any sort of colour pictures like bmp, jpeg, and fuss pictures. The hash formula indiscriminately generates a hashkey that later on utilized by the formula to get a pattern of pixels, wherever the information are keep. Xing Li et al [12] introduced a completely unique blind steganalyzer for additive noise steganography in JPEG decompressed pictures Based on the principles of LSB Replacement Steganography formula, Yongzhen Zheng, et al [13] projected associate approach to spot steganography computer code by Core directions temple Matching. Yasser M. Behbahani et al [14] projected a brand new JPEG-based steganography technique, mistreatment eigenvalues properties of matrices of measure DCT coefficients. Eigen value Steganography technique hides confidential information using the eigenvalues of measure DCT matrices and manipulating them. Kazem Ghazanfari et al [15] propose a brand new technique for image steganography, known as LSB++, that improves over the LSB+ image steganography by decreasing the number of changes created to the sensory activity and applied mathematics attributes of the duvet image the essential plan of the LSB+ technique is to alter the unused pixels during a unit so as to revive the frequency of bin

3.PROPOSED APPROACH

The proposed method is made up for providing the security through steganography. It has following main parts: (i) Compress the input image, (ii) secret message encryption, (iii) selection of a cover image and (iv) message embedding tothe chosen cover image. Figure 3.1 describes the block structure of the proposed encryption method. This proposed encryption method block diagram isat sender side and Figure 3.2 tells it's reverse. It means this figure shows the decryption process and this decryption process is at receiving end.

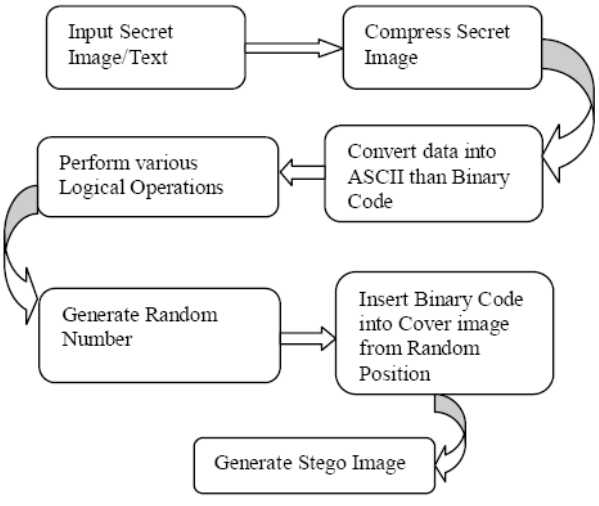

Figure 3.1: Block Diagram of Proposed Steganography at Sender end

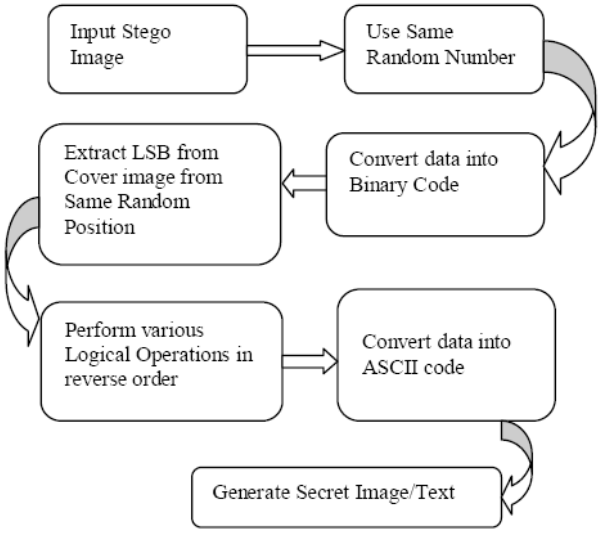

Figure 3.2: Block Diagram of Proposed Steganography at Recieving end

3. EXPERIMENTS

The proposed steganography technique is implemented in MATLAB 7.7. The cover images considered are cover1.jpg with dimensions 477x720 and the secret images / secret areconsidered more than one with following dimensions. All the images under consideration are grey scale.

TABLE 4.1: Size of Secret Text and Image

S. No.	Secret Text Size	Secret Image Size
1	64 bytes	4 KB
2	192 Bytes	5.96KB
3	384 Bytes	13.9KB
4	768 Bytes	16.2KB

Fig 4.1: Comparison between cover and stego-image for secret Text

Fig 4.2: Cover Images after decryption process

4. RESULT ANALYSIS

SNR, MSE, Correlation, Regression are some of the comparison parameters. They compare the quality of images between Stego-image and cover image. Table 5.1 & 5.2 shows the performance based comparison of the Proposed work with Base work. while taking data as given reference in table 4.1..

TABLE 5.1: PSNR for Secret Texts

S. No.	Previous Work	Proposed Work
1	39.716514	39.716761
2	39.716457	39.716713
3	39.716281	39.716679
4	39.716281	39.716586

TABLE 5.2: PSNR for Secret Images

S. No.	Previous Work	Proposed Work
1	39.71665	39.71667
2	39.716694	39.716803
3	39.716721	39.716826
4	39.716658	39.716735

The result of tables show that there is less changes in cover image after embedding secret text/image into cover image though our method as compare to previous method. Other way around researchers can say the quality of stego-images is much better as compare to the stego-image produce by base paper method.

5. CONCLUSIONS

In this paper a secure image steganography technique is proposed to hide images, which also tells how to hide data bits. An improved efficient computer-based steganographic method has been proposed for embedding secret messages into images

without producing noticeable changes. The proposed model explores the possible of providing higher hiding capacity with lower distortion in the wavelet domain. The method utilizes the characteristic of the human vision's sensitivity to grayvalue variations. Experimental results showed the high invisibility of the proposed model.It provides an easy way to produce a more imperceptible result than those yielded by simple least-significant-bit replacement methods. The method not only provides a better way for embedding large amounts of data into cover images with imperceptions, but also offers an easy way to accomplish secrecy. The experimental results show that the technique produces good quality stego images with good PSNR values.

REFERENCES

[1] N. Provos and P. Honeyman, "Hide and seek: An introduetion to steganography", IEEE Seeurity and Privaey1(3) pp. 32-44,2003.
[2] S. Song, J. Zhang, X. Liao, J. Du and Q. Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Elsevier Ine, Advanced in Control Engineering and Information Seienee, Vol. 15, pp. 2767 - 2772,2011
[3] P. Marwaha and P. Marwaha, "Visual Cryptographic Steganography in Images", in Proe. ICCCNT, 2010.
[4] S. Song, J. Zhang, X. Liao, J. Du and Q. Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Elsevier Ine, Advaneed in Control Engineering and Information Seienee, Vol. 15, pp. 2767 - 2772,2011.
[5] Changder. S, Ghosh. D, and Debnath. N.C, "LCS based text steganography through Indian Languages", in Proc.ICCSIT 2010, pp. 53-57.
[6] V.M. Potdar, S. Han, E. Chang, Fingerprinted secret sharing steganography for robustness against image cropping attacks, in: Proceedings of IEEE Third International Conference on Industrial Informatics (TNDIN), Perth, Australia, 10-12 August 2005, pp.717-724.
[7] M.H. Shirali-Shahreza, M. Shirali-Shahreza, A new approach to Persian/Arabic text steganography, in: Proceedings of Fifth IEEE/ACIS International Conference on Computer and Information Science (ICIS-COMSAR 2006), 10-12 July 2006,pp. 310-315.
[8] K.H. Jung, K.Y. Yoo, Data hiding method using image interpolation, Computer Standards and Interfaces 31 (2) (2009) 465-470.
[9] P. Tsai, Y.C. Hu, H.L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, Signal Processing 89 (6) (2009) 1129-1143.
[10] Li, J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm, Information Sciences 177 (15) (2007) 3099-3109l.
[11] Riasat, R.; Bajwa, I.S.; Ali, M.Z , "A Hash-Based Approach for Colour Image Steganography", International Conference on Computer Networks and Information Technology (ICCNIT),2011. Pp 303 - 307.
[12] Xing Li Tao Zhang Kaida Li Xijian Ping, "Blind Detection Method for Additive Noise Steganography in lPEG Decompressed Images", Third International Conference on Multimedia Information Networking and Security (2011). Pp489 -493
[13] Yongzhen Zheng, Fenlin Liu et al," A Identification of steganography software Based on Core Instructions Template Matching", Third International Conference on Multimedia Information Networking and Security (2011), pp 494 -498.
[14] Yasser M. Behbahani, Parham Ghayour, Amir Hossein Farzaneh, "Eigenvalue Steganography Based on Eigen Characteristics of Quantized DCT Matrices", Proceedings of the 5th International Conference on IT & Multimedia at UNITEN (ICIMU 2011) Malaysia.
[15] Kazem Ghazanfari, Shahrokh Ghaemmaghami, Saeed R. Khosravi, "LSB++: An Improvement to LSB+ Steganography", TENCON 2011 - 2011 IEEE Region 10 Conference, pp.364-368