ISSN:0975-9646

Encryption Based Steganography- Modern Approach for Information Security

Mohammad Sajid Khan[1], Sarvesh Singh Rai[2]

[1]*Department of Computer Science & Engineering, IMEC*
RGPV University, INDIA
[2]*Assistant Professor, Department of Computer Science & Engineering, IMEC*
RGPV University, INDIA

Abstract— **Steganography is the technique of hiding information so that any intermediate third party is unaware about the presence of secret message. Digital steganography uses some digital media as the cover for the secret message, like in our case, we have used digital images as the cover media. Essence of steganography is that the third party should never be able to detect the presence of secret message in the cover image. Once the third party detects the secret message, it is assumed that the steganography technique has failed to serve its purpose. The proposed model presents a novel approach of develop a secure data hiding technique of Steganography using wavelet transform, Some logical operations, binary convertor, along with random number generation method.**

Keywords— **D**igital image, information hiding, ***steganography, PSNR value, LSB.***

I. INTRODUCTION

Cryptography is the field of technology for hiding information. It hides and encrypt the information in such a way that a third party who has access to the hidden and encrypted data cannot reconstruct. Unfortunately it is not enough in today's world. It is now also become necessary to keep the existence of the message secret from outside world. Basically it deals with embedding information to be hidden in a given media (cover media) without making any visible changes to that cover media. The message-embedded image is known as stego image [2]. A secret key Steganography system (Fig.1) is similar to a symmetric cipher, where the sender chooses a cover and embeds the secret message into the cover using a secret key. If the secret key used in the embedding process is known to the receiver, using the reverse process the secret message can be extracted[3].

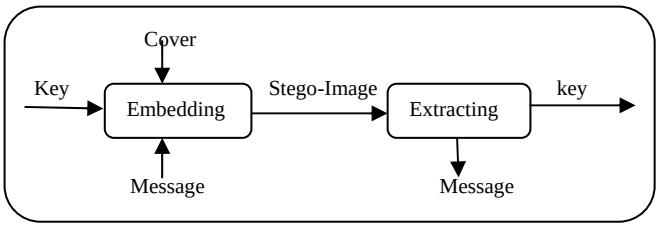

Fig.1 Secret key steganography

Image based secret key steganography uses images as the cover media. Several methods have been proposed for image based steganography, LSB being the simplest one. Steganography, derived from Greek, literally means "covered writing." It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum [4].

The advantages of Least-Significant-Bit (LSB) steganographic data embedding are that it is simple to understand, easy to implement, and it produces stego-image that is almost similar to cover image and its visual infidelity cannot be judged by naked eyes. Several steganography methods based on LSB have been proposed and implemented [5][6][7].

A good technique of image steganography aims at three aspects. First one is capacity (the maximum data that can be stored inside cover image). Second one is the imperceptibility (the visual quality of stego-image after data hiding) and the last is robustness [8]. The LSB based technique is good at imperceptibility but hidden data capacity is low because only one bit per pixel is used for data hiding. Simple LSB technique is also not robust because secret message can be retrieved very easily once it is detected that the image has some hidden secret data by retrieving the LSBs.

In this paper, we present a LSB based steganography method which is more secure and robust than plain LSB method. Rather than storing the message bits sequentially, they are stored in a encrypted form generated by proposed algorithm which uses a stagokey shared by both sender and receiver. After that staganalysis is performed on the stago-image to analyze the bit patterns of second and third LSBs that co-occur with LSB. Based on this analysis, LSB of those bytes may be inverted which co-occurs with a specific bit pattern, which improves the PSNR of stagoimage and also makes the task of staganalysis difficult.

Next section describes related work in section II which is followed by the method proposed in section III. Section IV describes the experiments and results. In section V, conclusion is discussed.

II. LITERATURE SURVEY

Steganography is the science of hiding secret information in an unsuspicious cover object. The goal of Steganography was defined by Johnson and Jajodia as "the goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated." [9].

Discovering the communication is the first attack to steganography since it is against the main goal of steganography. But it is possible to use steganography together with cryptography by encrypting the message before embedding it into a cover object. Using steganography and cryptography together to provide better information security is a hot topic [10, 11, 12, 13, 14].

Steganography techniques can be categorized as 'fragile' and 'robust' according to the strength of the stego-object against the steganalysis attacks [15, 16]. The stego-object, which does not lose its hidden message and its cover object is still recognizable after being exposed to multiple image processing techniques such as warping, cropping, rotating and blurring is defined as robust [9]. The others are fragile. Their hidden messages are lost under JPEG compression or they are completely destroyed after applying image processing techniques.

A. Steganography in Text Files

Hiding messages in text files is the easiest and oldest but a fragile way of secret communication. Today, it is applied by changing the layout of a document, adding extra spaces and using hidden characters in text. The disadvantage of text steganography is its weakness against attacks. The extra spaces, lines and characters added could easily be detected by opening the text in a word processor. The hidden message will be lost if the document is reformatted [17]. Additional techniques for hiding messages in text files are given in [18].

B. Steganography in Image Files

Images are the most common cover objects used in steganography. Image steganograms can be fragile or robust according to the method applied on the image file [19]. Image steganography methods can be categorized as 'Image domain methods' and 'Transform domain methods'. Image domain methods are easy to apply, but it is possible to create more robust stego-images with transform domain techniques. Some of the popular image domain tools are 'Hide and Seek', 'Mandelsteg', 'Steganos', 'StegoDos', 'S-TOOLS', and 'White Noise Storm'. Some of the transform domain tools are 'Jpeg-Jsteg', 'JPHide', 'Outguess', 'PictureMarc' and 'SysCop' [17].

Some of the techniques were briefly explained as follows:

1) Least Significant Bit Algorithm: This is the simplest method applied on image files. First, the message to be hidden is broken into pieces of 1 bit then the least significant bit of each pixel of the cover object is used to store the bits of the secret message. The change in cover object is invisible to naked eyes up to 4th LSB of the image. This technique is unsuccessful and visible to naked eyes, when the bits of the hidden message have more space to be placed than the cover image [16]. The LSB method is not a robust algorithm since it is easily corrupted when it is exposed to image processing techniques.

2) Patchwork Algorithm: It is a more complex method compared to LSB algorithm. First, two random pixels are selected from the image. Then, the brighter of the two is made brighter and the darker one is darker. The contrast change between these two pixels corresponds to a part of the bits of the hidden message [20, 21]. The image remains undetectable under filtering attacks, even in the case of a few hundred changes in pixels [20].

3) Transform Domain Algorithms: Robust methods use transformation algorithms such as DCT (Discrete Cosine Transformation) or Wavelet Transformation. The message is hidden in significant areas of the cover image using the algorithms which make the stego-object more robust to image processing attacks than the LSB method [19]. A more detailed research on transform domain techniques can be found in [22].

III. PROPOSED APPROACH

Proposed work is group of two techniques. Mainly called (i) cryptography and (ii) steganography. Our proposed work contains mainly three parts –message encryption, selection of a cover image, message embedding to the chosen cover image. Figure 3.1 showing the block diagram of the proposed encryption technique which is at sender side and Figure 3.2 showing the block diagram of the proposed decryption technique which is at receiver side.

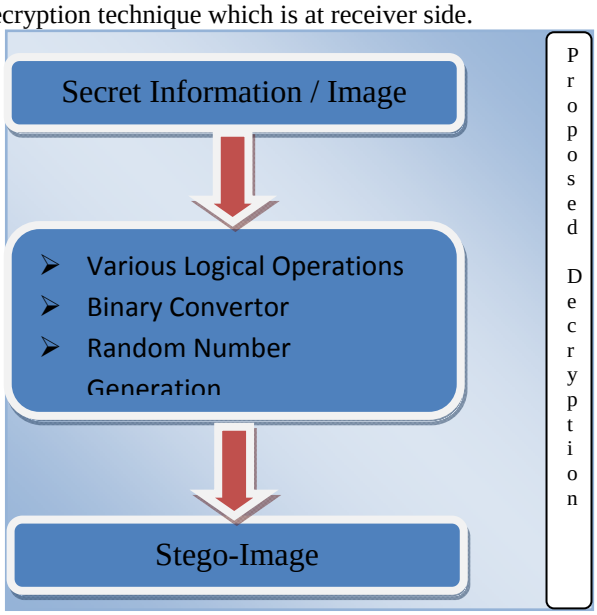

Figure 3.1: Block Diagram of Proposed Steganography at Encryption Side

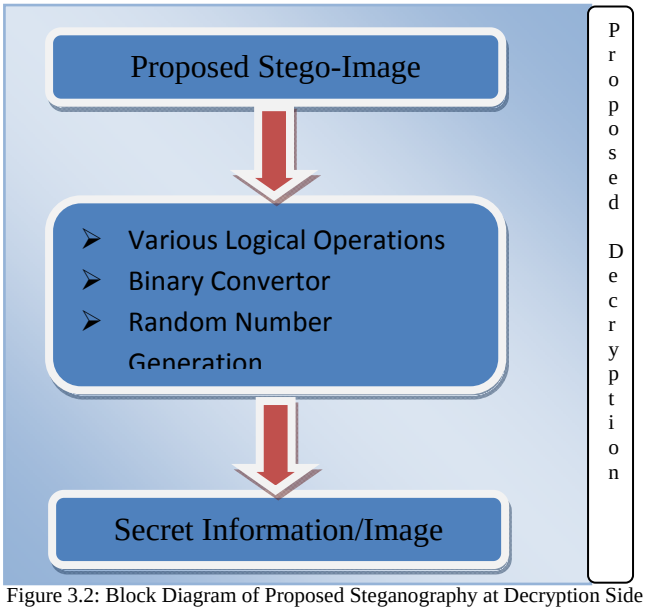

Figure 3.2: Block Diagram of Proposed Steganography at Decryption Side

IV. EXPERIMENTS

The proposed steganography technique is implemented in MATLAB 7.7. The cover images considered are nature.jpg with dimensions 680x556 and the secret images / secret are considered more than one with following dimensions. All the images under consideration are grey scale.

TABLE I Size of Secret Text and Image

S. No.	Secret Text Size	Secret Image Size
1	66 Bytes	844 Bytes
2	130 Bytes	1.75 KB
3	386 Bytes	2.35 KB
4	1.12 KB	3.8 KB
5	3.37 KB	4.4 KB

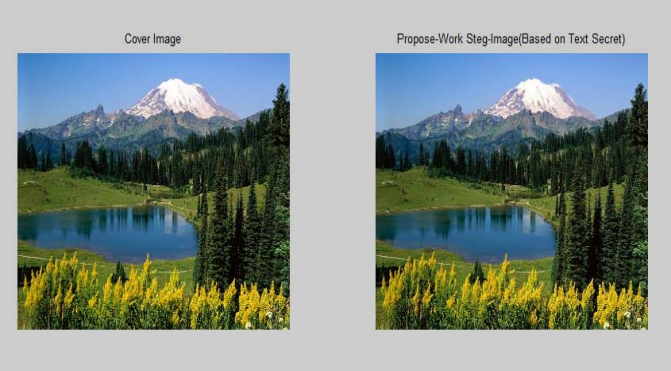

Fig 4.1: Comparison between cover and stego-image for secret Text

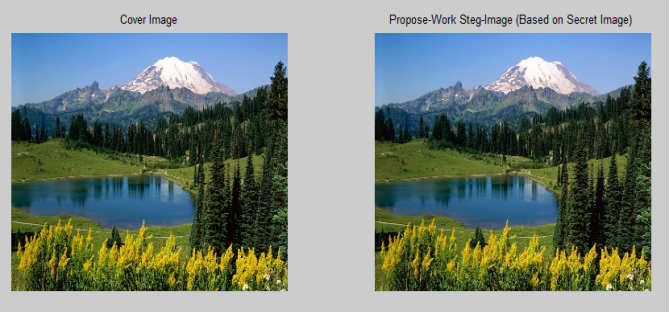

Fig 4.2: Comparison between Cover and stego-image for secret image

Fig 4.3: Cover Images after decryption process

V. RESULT ANALYSIS

There are various ways to find the comparison between various steganography methods. Some of those parameters are PSNR, Correlation, Max difference between Cover & Propose-work steg-images etc. Table II & III shows the performance based comparison of the Proposed work with given base paper work. Table II & III shows the PSNR value comparison between base and proposed work method while taking data as given reference in table I..

TABLE II: PSNR for Secret Texts

S. No.	Base Paper	Proposed Work
1	36.104328	36.104359
2	36.104252	36.104281
3	36.104278	36.10447
4	36.104228	36.104234
5	36.103255	36.104277

TABLE III: PSNR for Secret Images

S. No.	Base Paper	Proposed Work
1	36.104341	36.104454
2	36.104493	36.104547
3	36.103474	36.103863
4	36.103082	36.104283
5	36.103399	36.103428

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 base paper method.

VI. CONCLUSIONS

Digital Steganography is an interesting scientific area which falls under the umbrella of security systems. Image steganography is a considerably new dimension in the field of information hiding. In this paper a secure image steganography technique is proposed to hide images, which also tells how to hide data bits. The experimental results show that the technique produces good quality stego images with good PSNR values.

REFERENCES

[1] N. Provos, P. Honeyman " An introduction to steganography," IEEE Security & Privacy Magazine, Vol. 1, Issue 3, pp. 32-44, 2003.

[2] H. A. Jalab, A. A. Zaidan, B. B. Zaidan, "New Design for Information Hiding with in Steganography Using Distortion Techniques," International Journal of Engineering and Technology (IJET)), ISSN: 1793-8236, Vol 2, No. 1, pp. 72-77, 2010.

[3] K. Bailey, K. Curran, " An evaluation of image based steganography methods using visual inspection and automated detection techniques," Multimedia Tools and Applications, Vol. 30 , Issue 1, pp. 55-88, 2006.

[4] Cheddad, J. Condell, K. Curran, & P. Kevitt, (2010). Digital image Steganography- survey and analysis of current methods. Signal Processing, 90, 727–752.

[5] C. K. Chan, L. M. Cheng, "Hiding data in image by simple LSB substitution", pattern recognition, Vol. 37, No. 3, 2004, pp. 469-474.

[6] R. Z. Wang, C. F. Lin and I. C. Lin, "Image Hiding by LSB substitution and genetic algorithm", Pattern Recognition, Vol. 34,No. 3, pp. 671-683, 2001.

[7] D. Sandipan, A. Ajith, S. Sugata, An LSB Data Hiding Technique Using Prime Numbers, The Third International Symposium on Information Assurance and Security, Manchester, UK,IEEE CS press, 2007.
[8] C. Kessler. (2001). Steganography: Hiding Data within Data. An edited version of this paper with the title "Hiding Data in Data". Windows & .NET Magazine. http://www.garykessler.net/library/steganography.html
[9] N. F. Johnson and S. Jajodia, “Steganalysis: The Investigation of Hidden Information”, IEEE Information Technology Conference, September 1998.
[10] S. Sagiroglu and M. Tunckanat, "A Secure Internet Communication Tool", Turkish Journal of Telecommunications, Vol.1, No.1, pp.40-46, 2003.
[11] ù. Sagiroglu, M. Tunçkanat and M. Altuner, "Kriptolojide Yeni bir YaklaúÕm Resimli Mesaj", Telekomünikasyon Ekseni Dergisi, Telekomünikasyon Kurumu, Vol.2, p.22-24, January 2002.
[12] ù. Sa÷Õro÷lu, M. Tunçkanat, “Gizli bilgilerin internet ortamÕnda güvenli olarak aktarÕmÕiçin yeni bir yaklaúÕm” Popüler Bilim Dergisi, Year.9, Vol.105, p.21-24, September 2002.
[13] M. Tunçkanat and ù. Sa÷Õro÷lu, "Güvenli øletiúim øçin Yeni Bir YaklaúÕm: Resim øçerisine Döküman Gizleme", GAP IV. Mühendislik Kongresi (UluslararasÕKatÕlÕmlÕ), Vol.1, p.665-668, ùanlÕurfa, 6-8 January 2002.
[14] ù. Sa÷Õro÷lu and M. Tunçkanat, "Gizli bilgilerin elektronik ortamda güvenli aktarÕmÕ", TBD 19. Biliúim KurultayÕ, Beylikdüzü, østanbul, p.47-50, 3-6 September 2002.
[15] S. Channalli and A. Jadhav, “Steganography – An Art of Hiding Data”, International Journal on Computer Science and Engineering, vol.1(3): 137-141, 2009.
[16] J. Cummins, P. Diskin, S. Lau and R. Parlett, “Steganography and Digital Watermarking”, School of Computer Science, The University of Birmingham, 2004.
[17] J. Silman, "Steganography and Steganalysis: An Overview", 2001.
[18] P. Wayner, Disappearing Cryptography, Chestnut Hill, MA: AP Professional, 1996.
[19] N. F. Johnson and S. Jajodia, “Steganalysis: The Investigation of Hidden Information”, IEEE Information Technology Conference, September 1998.
[20] J. Watkins, “Steganography – Messages Hidden in Bits”, 2008.
[21] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding - A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062-1078, July 1999.
[22] N.F. Johnson, Z. Duric, S. Jajodia, "The Role of Digital Watermarking in Electronic Commerce".