

Improved Performance of Secure Data Hiding Algorithm Using Non Blind Steganography Technique

Mr. Abhishek Sharma¹ & Mr. Vijay Sharma²

¹ M.Tech Scholar RIET Bhankrota, Jaipur, abhisheksharma0688@gmail.com,

² Assistant Professor, RIET, Bhankrota, Jaipur, vijaymayankmudgal2008@gmail.com

Abstract: -

Steganography is the art of hiding secret information into cover media such that no one apart from the intended recipient is knows the existence of the information. In recent years, many successful steganography methods have been proposed. The steganalysis is a type of attack on steganograph so there is requirement to develop new steganography algorithm, which is hard to detect by steganalyais (as RS attack). The cover media that carry the information is known as carrier. It can be any digital media like images, videos, sound files. In this paper, a method has been proposed using which a large size secret image (containing hidden encrypted message) can be hidden into small size of cover image securely. The main aim here is the absolute invisibility of the large size secret image. The proposed method does not require the sender to send the cover image to the receiver for obtaining the secret image. The performance of the proposed method is measured in terms of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE).

Key words: Steganography; steganalysis; Discrete wavelet transform (DWT); Alpha blending

I. INTRODUCTION

The term steganography arrived from two Greek worlds stegos and graphica, which basic meaning is "covered writing" (stegos means covered and graphica means writing). Embedder can select any digital cover media (like: image, audio file) that results in the least detectable stego file. Today, computers and internet have become the most powerful source of communication, among the people in the different parts of the world. However, the safety and security of the exchanged data is very

important, if it is confidential. There is need to develop good steganography algorithm, because steganography is more power full technique for secure communication [1]. Figure 1 shows the covered lizard, soothing is hidden inside the cover media but inside portion is not identified by outsider.

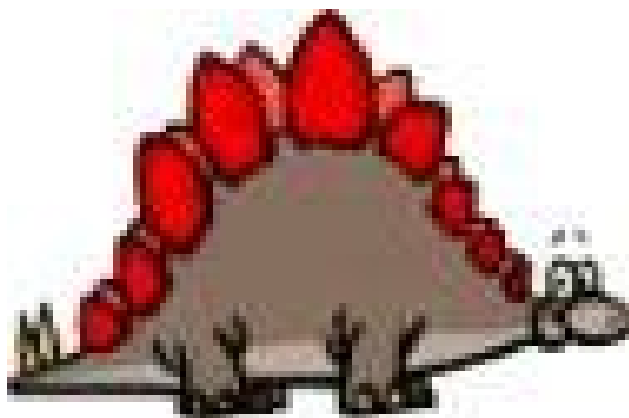


Fig.1 Stegosaurus: a covered lizard (but not a type of cryptography)

Information System Security (Watermarking and Steganography) is a discipline that protects the Confidentiality, Integrity and Availability of information and information services. Steganalysis is a type of attack that always tries to break the security. Steganography's ultimate objectives and the main factors separate it from the related techniques such as cryptography and watermarking. Steganography tends to hide the existence of the message itself, which makes it difficult for an observer to figure out where the message is [2][3]. Sometimes, sending encrypted information may draw the attention of an observer, while invisible information will not. Watermarking is similar, but has a completely different purpose. Watermarking is

the process of embedding information on the multimedia. Placing a watermark in media file serves to identify the artist or author of the work i.e. it is used for copyright protection [4].

II. PROPOSED METHOD

The proposed method consists of two processes- the encoding process and the decoding process. In encoding process, each process has three stages to complete. In encoding process it hide encrypted secret message inside secret media, and then host media added with secret image. The proposed algorithm provide single level of encryption. In the proposed technique contain three level of data hiding process.

The **encoding process** of proposed technique, as follow:

- Stage 1. Encrypt the secret message.
- Stage 2. Hide encrypted message into secret image and generate output image S.
- Stage 3. Hide image S with cover media and then get stego image.

Decoding process:

Decoding process is just reverse of the encoding process with on additional feature. There is no need to send cover media. Cover image is automatically generated at receiver end with the help of stego image.

Experimental results:

Figure 3 shows the image to be hidden and its intensity matrix.

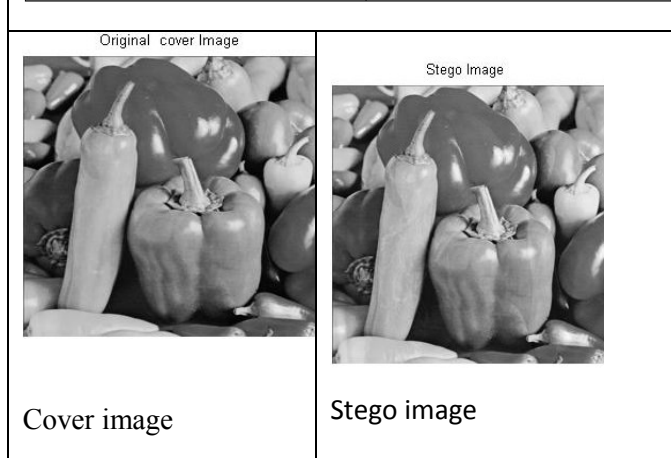
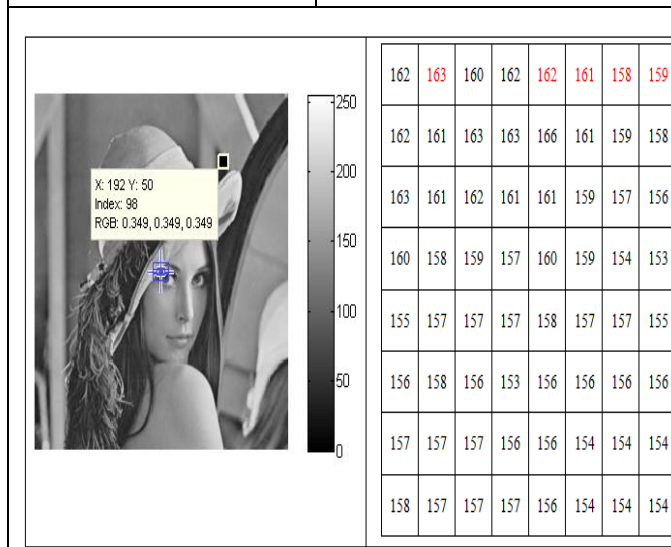
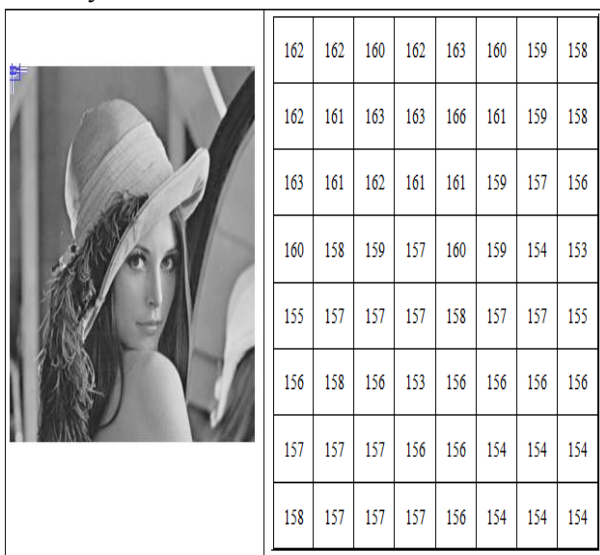


Fig 3. Secret image and its top Left corner intensity Image block of size 8 X 8.

After embedded the encrypted secret message, intensity of image pixel may change by one. In figure 4 intensity which is change after embedding the message shown with red color.

Fig 4. Secret image with embedded encrypted message and its top Left corner intensity Image block of size 8X 8. This encrypted message is embedded in to secret image lenna and resulted image is secrete image with Encrypted message, as shown in figure 5 below.

Fig 5: Experimental results of proposed technique
Performance of the proposed method is analyzed by comparing the cover image and the stego image in terms of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE). PSNR measure the distortion between the original cover image and the stego image. It is defined as follow:

$$PSNR = 10 \log \frac{255^2}{MSE} \text{ DB}$$

The proposed method is tested for the different cover images and secret images for the various values of Fine tuning the embedding strength factor alpha improves the quality level of stego image and the extracted secret image[]. The picture quality measurements for some of the tested images have been illustrated in Table 2. The results show high PSNR and low MSE values which indicate the effectiveness and accuracy of our proposed method.





Cover Image	Secret Image with hidden message	PSNR	MSE
Pepper.Tiff 	Lenna.Tiff 	26.890 2	7.4502e+0 6
Goldhill.Tiff 	Lenna.Tiff 	27.850 4	6.3504e+0 6

TABLE 2: Picture quality measurements for some of the tested images

III. DISCUSSIONS

The algorithm proposed in the current work describes a method such that the stego image which

is obtained thereby cannot be proved as stego image using the steganalysis approach. A secure steganography algorithm based on level of encryption is proposed in this research. Benefited from the effective optimization, a good balance between the security and the image quality is achieved. This small degradation is acceptable as the stego image behave like as cover image. The future work will focus on improving the efficiency of the proposed algorithm by adjusting second LSB of Image.

REFERENCES

- [1] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt “Digital image steganography: survey and analysis of current methods” Signal processing, Volume 90, Issue 3, March 2010, Pages 727-752.
- [2] Harvinder Singh, Anuj kumar and Prateek Bansal, “Analysis and Implementation of Algorithm to Hide Secret Message” International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 2, February - 2013, pages 327-333.
- [3] Farooq Husain, “A Survey of Digital Watermarking Techniques for Multimedia Data”, MIT International Journal of Electronics and Communication Engineering Vol. 2, No. 1, Jan 2012 pages 37-43.
- [4] Abbas Cheddad , Joan Condell, Kevin Curran, Paul Mc Kevitt “Digital image steganography: Survey and analysis of current methods”, Elsevier Signal Processing volume 90, January 2010, Pages. 727-752.
- [5] Marvel, L.M., Boncelet, C.G. and Retter, C.T., "Spread spectrum image steganography", IEEE Trans. Image Process., vol. 8, no. 8, pp. 1075–1083, 1999.
- [6] J. Fridrich, R. Du, and L. Meng, “Steganalysis of LSB Encoding in Color Images,” Proc. IEEE Int’l Conf. Multimedia

- and Expo, CD-ROM, IEEE Press, Piscataway, N.J., 2000.
- [7] Katzenbeisser S. and F.A.P. Petitcolas, "Information Hiding Techniques for Steganography and digital watermarking", Artech House, INC., Norwood, London, pp.149-154, 2000.
- [8] Andrew D. Ker, "Steganalysis of LSB Matching in Grayscale Images", IEEE Signal Processing Letters, vol. 12, pp. 441-444, no. 6, June, 2005.
- [9] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, "Overview: Main Fundamentals for Steganography", Journal of Computing (JOC), Vol.2, Issue 3, ISSN: 2151-9617, P.P 158-165, March 2010, New York, USA.
- [10] Lee J S, Papathanassiou K P, Ainsworth T L," A New Technique for Noise Filtering of SAR Interferometric Phase Images". IEEE Transactions on Geoscience and Remote Sensing, 36(5): 1456-1465,1998.
- [11] M. I. Khalil" Image Compression Using New Entropy Coder" International Journal of Computer Theory and Engineering, Vol. 2, No. 1, ISSN 1793-8201, February, 2010.
- [12] Mohammed Abo-Zahhad, Sabah M. Ahmed & Ahmed Zakaria "ECG Signal Compression Technique Based on Discrete Wavelet Transform and QRS-Complex Estimation" Signal Processing – An International Journal (SPIJ), Volume (4) : Issue (2) pp.138-160, 2010.
- [13] Dr. H. B. Kekre, Tanuja Sarode, Prachi Natu & Shachi Natu" Performance Comparison of Face Recognition Using DCT Against Face Recognition Using Vector Quantization Algorithms LBG, KPE, KMCG, KFCG" International Journal Of Image Processing (IJIP), Volume (4): Issue (4) pp.377-389,2010.
- [14] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography", in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically).