STEGANOGRAPHY BASED ON DISCRETE WAVELET TRANSFORM

Riya Saxena[1], Urvashi Swami[2], Abhishek Saxena[3]

[1,2]Student, Arya Institute of Engineering and Technology, Jaipur, Rajasthan, India
[3]Assistant Professor, Arya Institute of Engineering and Technology, Jaipur, Rajasthan, India

---

Abstract - *In this paper, an image steganography approach is used to enhance the visual quality of image. Discrete Wavelet Transform (DWT) decompose the cover image to produce wavelet subbands. DWT is applied on both the cover image and the alpha blending operation is done. By using Stego-image Inverse Discrete Wavelet Transformation (IDWT) we obtained stago image. For high security we used Arnold transformation along with a private key.*

Key Words: *Steganography, Discrete wavelet transform (DWT), Embedding process, Extraction process.*

1. INTRODUCTION

Today, in modern world communication is important as well as necessary technology. Its purpose is sharing and transferring of data but at certain levels this technology is not safe. Steganography was derived from the Greek word stegano, which means covered or secret, and graphy (writing or drawing). Earlier, there was a rapid development of technologies leads to increase interest in the field of hiding different information in images, audio etc. Steganography is basically used because valuable information is transferred from one place to another insecurely and unreliably. The idea and practice of hiding information has a long history. The main focus of Steganography is on making it extremely difficult to tell whether a secret message exists at all or not. Steganography has failed, If an unauthorized third party is able to say with high confidence that a file contains a secret message. In this paper we see an overview of image steganography and its uses and hiding the files (text file, audio file etc.) by using AES and LSB algorithm Steganography. Steganography is a process of hiding a secret message in an ordinary message and the extraction of some secret message, whenever it is required. There are two categories of Image steganography: spatial domain and frequency domain steganography. In spatial domain techniques we see that secret message is embedded in the image pixels, while in frequency domain technique the image is first transformed and then secret message is embedded in the transformed image. In Frequency domain techniques the messages is hide in significant areas of cover image which make them more robust than spatial domain techniques. Several different approaches have been proposed for frequency domain steganography using different transforms. Market *et al.* [1] proposed a watermarking technique in which the secret image is decomposed into wavelet subbands using *DWT*.

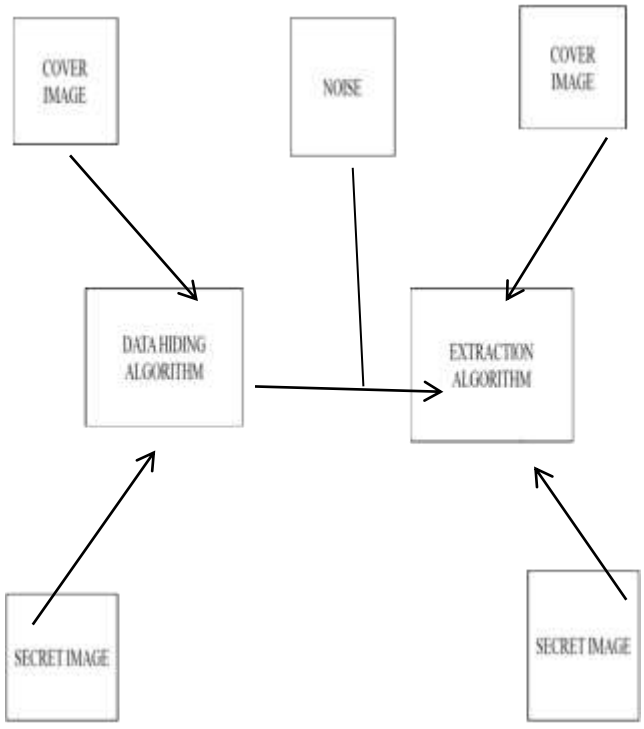


Figure -1: Image Steganography System

1.1 RELATED WORK

A.Nag, S. Biswas et al. [2], Haar-DWT spatial domain of original image was transformed to frequency domain. Gray level and Huffman encoding process is implemented on the secret image and cover image using two dimension 'Discrete Wavelet Transform' (2D-DWT) technique. For preserving the coefficients of

wavelet of an image the quality can be improved using in the low frequency sub band.

1.2 DISCRETE WAVELET TRANSFORM

Wavelet transform is used for converting the spatial field in frequency domain. The wavelets are used in the form of shorthand model lies in a statement. The wavelet transform is obviously splitting the high from the low-frequency information based on different pixels.

The simplest method of wavelet transforms is the Haar wavelet. Low frequency wavelet was created by taking the transform of coefficient of the averaging of the values of two pixel, and it can create the high frequency by taking half difference of the similar two pixels. In Figure (1) there are four bands approximate, Vertical, Horizontal, and diagonal Bands that is represented as LL, LH, HL and HH respectively. The spatial domain image is an very important and necessary part of the low frequency wavelet coefficients, which lies in approximation band. We see that the spatial domain image have the edge details of the high frequency coefficients which Coefficients lies in other bands known as detail bands. [3] [4].

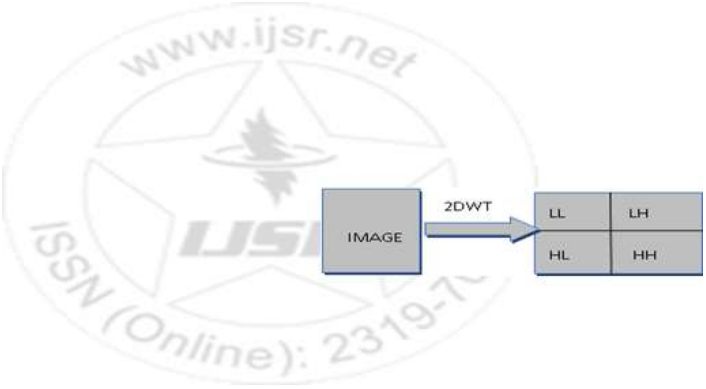


Figure -2: Components of 1-level 2DWT

1.3 THRESHOLD OF A SUB BAND

For calculating threshold for each high frequency sub-bands (i.e. LH, HL and HH) we use DWT technique on cover image that is proposed by Nick Method in [3] as (1) Where T is the threshold of a sub band, is mean of particular sub-band, is a constant valued as -0.15 (Ni-black W., [3]. measured it -0.2), The dimensions of sub band and wavelet coefficient C is used. In the given work, we consider slight lesser of than original constant proposed by Ni-black.

1.4 IMPLEMENTATION OF IMAGE STEGANOGRAPHY BASED ON DWT

Image steganography based on the phenomenon of DWT.It uses two processes i.e. encoding and decoding. In encoding, Arnold transformation is used along with a private key on a secret image which gives high security to the algorithm. Stego-image is obtained by using IDWT.

In decoding, DWT is applied on both stego-image and cover image. Alpha blending operation is then applied and IDWT is used to get scrambled secret image. Finally, original secret image is obtained with the help of private key.

The discrete wavelet transform (DWT) decomposes the image into four different bands: LL, HL, LH and HH. For wavelet analysis, it uses filter banks.

(a) (b)

Figure -3: (a) Lena original image and (b) Lena image after Wavelet decomposition

1.5 EXPERIMENT AND RESULTS

Here, we present the result of embedding in CVG images data set for Image steganography which has two categories. The first size category consists of 512×512, The second one is size 1024×1024. The coefficients of its Vertical and Diagonal subdivisions are embedding in horizontal coefficient to embed the secret data by using haar wavelet algorithm. In our experiment, We choose 6 images with scale of 512×512, and specific capacity of hiding 2040 bit per pixel, Then we study their PSNR and MSE from the RGB perspective. Moreover we take the same number of random images with bigger scale (1024×1024) but with more hidden text with 4096 bpx. A predefined fact of analyzing and measuring the quality of image steganographic techniques are as follows:

1. If the value of PSNR exceeds 36 dB then the visibility of stego and cover images are the same and cannot be identified by HVS (Human Visual System).

2. If the value of Mean Square Error (MSE) is less that means, stego image quality is goodr and large value denotes stego image that contains distortion.

Moreover, the value of MSE should lie between 0 and 6. Otherwise the difference between original and stego images will be perceptible

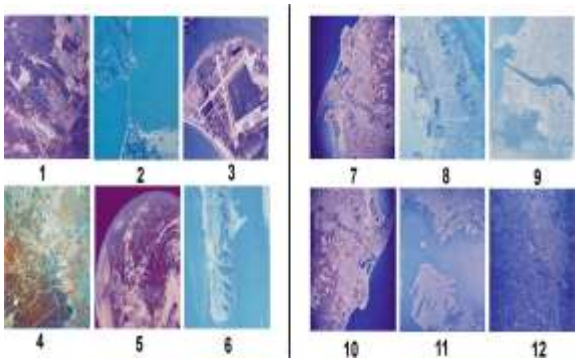


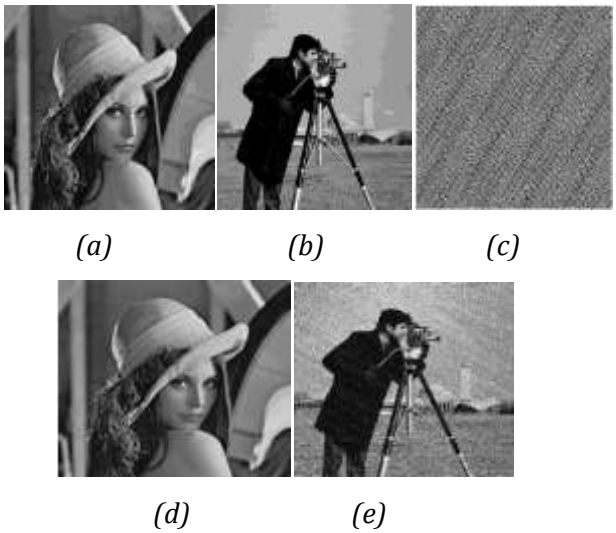
Fig. 4. 12 CVG images (512×512) left side, (1024×1024) right side

Results on Images(1 - 6) : 512X512 Pixel						
Capacity of Hiding : 2040 bpp (bit per pixel)						
Image	PSNR (R)	PSNR (G)	PSNR (B)	MSE (R)	MSE (G)	MSE (B)
1	71.5417	317.4439	65.9071	0.0046	1.174e27	0.1325
2	76.9352	314.5388	70.4778	0.0013	2.2867e27	0.0058
3	65.0924	316.2902	60.3309	0.0201	1.5278e27	0.0603
4	69.7958	314.4276	55.8632	0.0068	2.3460e27	0.1686
5	72.8735	317.5388	62.8017	0.0034	1.460e27	0.0341
6	72.1941	313.4190	67.1657	0.0393	2.9592e27	0.0125

Fig 5. Results on left side images (512×512)

1.6 SIMULATION RESULTS AND ANALYSIS

The stego-image after embedding and recovered secret image is shown in Figure 5 and Figure 6.Three different wavelets are used for embedding. Results are obtained by using MATLAB R2012a. The value of alpha is taken as 0.01.



(a) *(b)* *(c)*

(d) *(e)*

Fig 6: (a) Cover image (lena.tif) (b) Secret image (cameraman.tif) (c) Arnold transformation (d) Stego image (e) Recovered secret image

1.7 APPLICATIONS OF STEGANO-GRAPHY

a) Secret communication does not use steganography to advertise and therefore avoids scrutiny of the sender side, message, and recipient. Without alerting potential attackers a secret, blue print or other sensitive information can be transmitted.

b) For sending out trade secrets without anyone at the company being any the wiser. Steganography can also be used for corporate espionage.

c)To prevent digital data, copyright protection mechanism is used usually from being copied. To protect the copyrighted material which is responsible for the increasing interest in digital steganography and data embedding, watermark technique is used.

TYPES OF STEGANOGRAPHY

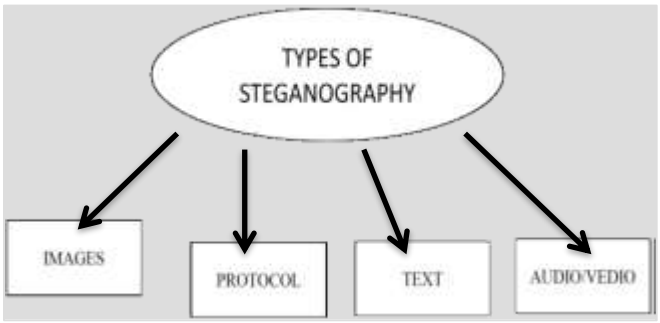


Fig 7: Types of steganography

1.8 THE PROPOSED METHOD

In this section, the main steps of the 'proposed work' will be explained. The main purpose of stegnography based on hide secret gray scale image into a cover gray scale one. The logistic chaotic map method used to increase security before the hiding process by the secret image permutation, the cover image decomposed by 'wavelet Transform (DWT)' and then embedded the encryption ''secret image'' in HH band. The block diagram of the embedding system shown in figure (8) the encryption of the 'secret image' explained in above section.

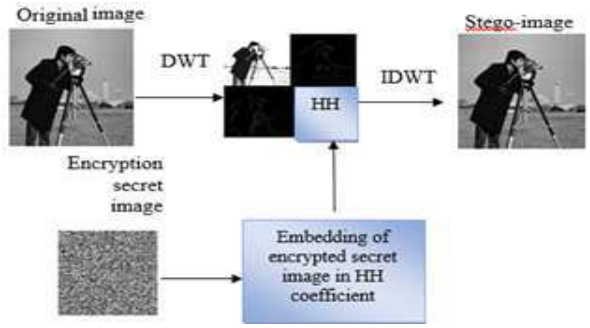


Figure 8: Block diagram of the Embedding Process

1.9 EXTRACTION PROCESS

In figure (9) block diagram for extracting the encryption secret image shown:

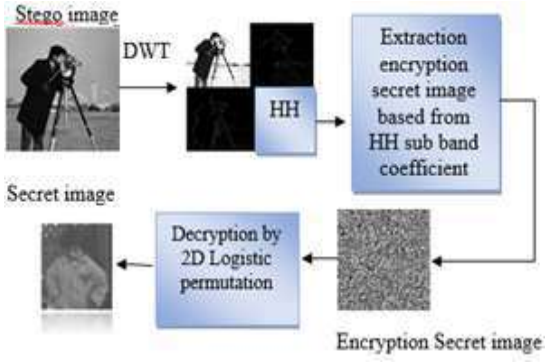


Figure -9: Block Diagram of the Extraction Process

CONCLUSION

In this paper, a novel image steganography approach based on DWT is proposed. Image steganography which is based on DWT is done by using performance analysis using different wavelets. This method is associated to both colored and gray scale images. The stego- image looks unaltered. Hence, results in better quality image.The results show that Arnold Transform based method has higher PSNR values than other existing methods. In future this method can be tested by using other wavelets and different values of alpha.

The Green channel for all 12 images has the highest PSNR and MSE. The reason of that because all proposed images are combined of red and blue more than the green color, Moreover, all values based on PSNR and MSE was satisfied in terms of the imperfectibility and cumulative difference.

ACKNOWLEDGEMENT

The authors would like to express the deep sense of gratitude to Arya Institute of Engineering & Technology, Jaipur for guiding us from the inception till the completion of the research work. We sincerely acknowledge him/her for giving his/her valuable guidance, support for literature survey, critical reviews of research work.

FUTURE SCOPE

The future work on this project is to enhance the compression ratio of the image to the text. In order to enhance the application, we use different attractive and useful manner website function. Further we will study the transformation that will improve its possibility by changing the way of transformation.

REFERENCES

[1] Hsieh M. S., Tsebg D. C. and Huang Y. H., "Hiding Digital Watermark Using Multiresolution Wavelet Transform," IEEE Transactions on Industrial Electronics, vol. 48, no. 5, pp. 875-882, 2001.

[2] A.Nag, S. Biswas, D. Sarkar, P.P. Sarkar. "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security, Volume (4).

[3] Khurshid K., Siddiqi I., Faure C. and Vincent N., "Comparison of Niblack inspired Binarization methods for ancient documents," Proceedings of 16th International Conference on Document Recognition and Retrieval, pp. 1-9, 2009.

[4] G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[5] W.-K. Chen, Linear Networks and Systems (Book style).Belmont, CA: Wadsworth, 1993, pp. 123–135.

[6] H. Poor, an Introduction to Signal Detection and Estimation. New York: Springer-Verlag, 1985, ch. 4.

[7] B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.

[8] E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat., to be published.

[9] J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," IEEE J. Quantum Electron., submitted for publication.