GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

EMBEDDING METHOD FOR STEGANOGRAPHY TECHNIQUE USING HAAR WAVELET

N.THARIQ SHARIF[*1] & M.KRISHNAMURTHY[2]

PG Scholar, Department of Electronics and Communication Engineering, PSNA college of Engineering and Technology, Dindigul-624622, India[*1]

Assistant Professor, Department of Electronics and Communication Engineering, PSNA college of Engineering and Technology, Dindigul-624622, India[2]

Abstract

Steganography is the art of hiding information in ways that prevent detection. Steganography is a technique that hides digital information such as data, audio, video file called secrete object behind another digital object called cover image. In this paper, a new embedding method is proposed for steganography technique to prevent the detection of secrete object that is present behind the cover object such that to improve PSNR value. In image steganography, data in the form of image is hidden under cover image by using DWT transformation and wavelet used in this paper is Haar wavelet. The cover image is divided into higher and lower frequency sub-bands and secrete image data is embedded into any one of these sub-bands. The proposed approach results in high value of PSNR and low MSE value between cover image and stego image

Keywords — Haar wavelet, stego image, PSNR, MSE.

I. INTRODUCTION

Data hiding techniques have taken important role with the rapid growth of intensive transfer of multimedia content and secret communications. Steganography is the one of the popular data hiding technique. "Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (To hide the secret messages) and the graphic which means "writing" (text).Steganography is the technique for storing any digital object called payload (secret image) behind another digital object called cover image. The cover image with the secret data embedded is called the "Stego-Image". One of the most important requirement for steganography is that the length of the cover object must be very high in comparison to payload such that the effect of noise is minimized after the steganography process[2]. Steganography techniques are mainly divided into two categories. One method consists of embedding the secret object in the image domain or also called as spatial domain. The other method hides the secret object in the transform domain or frequency domain of an image. In transform domain there are many transform that can be used in data hidi ng, the most widely used transforms are: the discrete cosine transform (DCT), the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT). In the proposed paper work DWT transform is used and the used wavelet is HAAR wavelet. By using Haar wavelet, value of mean square error (MSE) is decreased and peak signal to noise ratio(PSNR) value is improved.

II. DISCRETE WAVELET TRANSFORM

The wavelet transform describes a multi-resolution decomposition process in terms of expansion of an image onto a set of wavelet basis functions. Discrete Wavelet Transformation has its own excellent space frequency localization property [1]. In DWT method, the image is decomposed based on frequency components into detailed and approximation bands, also called the sub-bands. Detailed band contains vertical, horizontal and diagonal bands. The total Information of the image is present in the approximation band[2][5]. The secrete object is normally embedded in the detailed band and sometimes in the approximation band . Wavelet transforms often have floating point coefficients. Thus, when the input data consists of sequence of integers, the resulting filtered output no longer consists of integers, which does not allow perfect reconstruction of the original image. As a result, the inverse wavelet transform becomes lossy however in wavelet Transform, that map Integers to Integers (IWT), the output can be completely characterized by integers and exact decompression of the original data is achieved[3].

III. HAAR WAVELET

Haar wavelet usually decomposes the signal into two sub-signals of half its length: Running average and Running difference[4]. To understand how haar wavelets work, consider a simple example. Assume a 1D image with a resolution of four pixels, having values [9 7 3 5]. First average the pixels together, pair wise, is calculated to get the new lower resolution image with pixel values [8 4]. Clearly, some information is

lost in this averaging process. We need to store some detail coefficients to recover the original four pixel values from the two averaged values. In our example, 1 is chosen for the first detail coefficient. This number is used to recover the first two pixels (9 and 7) of our original four-pixel image. Similarly, the Second detail coefficient is -1, since 4 + (-1) = 3 and 4 - (-1) =5. Thus, the original image is decomposed into a lower resolution version and a pair of detail coefficients. The decomposition to lower resolution values using haar wavelet is shown in Table 1

TABLE 1

Resolution	Averages	Detail coefficients
4	[9 7 3 5]	
2	[8 4]	[1 -1]
1	[6]	[2]

Thus, for the one-dimensional Haar basis, the wavelet Transform of the original four-pixel image is given by [6 2 1 -1].

IV. PROPOSED STEGANOGRAPHIC MODEL EMBEDDING METHOD

The block diagram of proposed embedding mothod is shown in figure 1

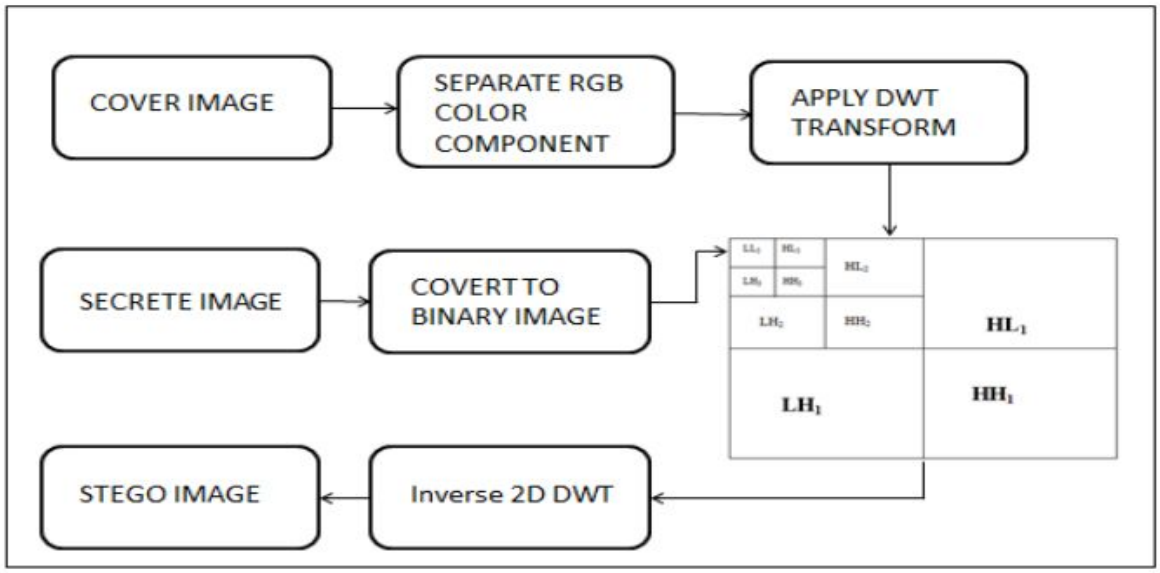

Figure1: block diagram for embedding method

1. Read the cover image and re-size the image so that number of rows and columns in the image should be equal.
2. Separate the RGB color components from the image.
3. Apply three level DWT transform to any of the color component and finally get four subbands LL3, LH3, HL3, HH3.
4. Read the secrete image and also re-size it so that number of rows and columns in the image should be equal. Note that size of secrete image should be smaller than cover image.
5. Convert the secrete image into an binary image and embed into LL3 subband of the color component to which DWT transform is applied.
6. Now carry out inverse DWT transform to generate stego image. The cover-image with the secret data embedded is called the Stego-Image.
7. Then stego image is sent to receivers end where extraction of secrete image from cover image is carried out.
8. The performance of embedding method is good only when the stego image looks similar to the cover image.

V. ASSESMENT CRITERIA

There are some metrics which can be used to check the performance of proposed approach. The commonly used metrics are MSE and PSNR.

Peak Signal to Noise Ratio (PSNR): It is the measure of quality of the image by comparing the cover image with the stego image, i.e., it is the measure of the difference between the cover image and stego image.

$$PSNR=10 \log 255^2/MSE$$

For a good steganography technique PSNR value should be high.

Mean square error(MSE): It is defined as the square of error between cover image and stego image. It is calculated
by:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (f(i,j) - (f'(i,j))^2$$

Where f (i, j) is the original image and f' (i, j) is the stego image. For a good steganography technique MSE should be low.

VI. RESULTS

Cover Image: Lena image is used as cover image, of size 512×512. The image is in .jpg format.
Secrete Image: secrete image of size 64×64 used as data to be hidden in cover image. The image is in .jpg format.
Stego Image: After embedding the secrete images in cover image, stego image is obtained. The cover image, secrete image and stego image is shown in figure 2.1, 2.2 and 2.3.

Fig 2.1: input image

Fig 2.2: secrete image

Fig 2.3: stego image

MSE, PSNR Values of proposed approach is given in Table 2

Table 2

Cover image (512*512)	secrete image (64*64)	Embedding factor	MSE	PSNR
Lena image	vegetables	0.0075	0.39	52.20

Comparison of Proposed Approach with Similar Existing Approaches is shown in table 3
Table 3

Approach	Hsi-eh M. S., et al.	Chen P. Y. et al.	Ataby A. A., et al.	Nag A., et al.	Kumar K. B. S., et al.	Bhattacharya T., et al.	**Proposed approach**
PSNR between cover image and stego image (in dB)	41.7	50.8	40.98	55.1	50.30	27.39	**52.20**

VII. CONCLUSION

Performing image steganography using haar wavelet decreases the value of MSE and improves the value of PSNR so the finally obtained stego image resembles same as that cover image so that intruder cannot suspect the existence of secrete image. So the proposed approach can be used in secrete communication in the areas of military or intelligence operatives or agents of companies to hide secret messages or in the field of espionage.

VIII. REFERNCES

[1] Optimized Image Steganography using Discrete Wavelet Transform (DWT) Parul, Manju, Dr. Harish Rohil"International Journal of Recent Development in Engineering and Technology Volume 2, Issu e 2, February 2014.

[2]A Novel Steganography Technique using Same Scale Wavelet H S Jayaramu, Dr K B Shivakumar, Srinidhi G A, Dr A K Goutam International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 4, April 2014.

[3]K B Shiva Kumar, K B Raja, Sabyasachi Pattnaik, "Hybrid Domain in LSB Steganography", International Journal of Computer Applications (0975 – 8887)Volume 19– No.7, April 2011.

[4]An Image High Capacity Steganographic Methods by Modified OPA Algorithm and Haar Wavelet Transform A.Antony Judice,Dhivya Shamini.P. International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

[5] A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum Tanmay Bhattacharya , Nilanjan Dey and S. R. Bhadra Chaudhuri ,International Journal of Modern Engineering Research (IJMER) Vol.1, Issue1, pp-157-161.

[6]A.A. Shejul and U.L. Kulkarni, "A DWT based Approach for Steganography Using Biometrics", EEE International Conference on Data Storage and Data Engineering, pp 39 -43, 2010.

[7] Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri, "A Session based Multiple Image Hiding Technique using DWT and DCT", International Journal of Computer Applications (IJCA),

Vol. 38, No.5, pp 18-21, 2012.

[8] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography technique Based on Wavelet Transform",the International Arab Journal of Information Technology, Vol. 7,No. 4, pp 358 -364, 2010.

[9] Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security, (IJCSS), Vol. 4, No. 6, pp 561-570, 2010.