

A Novel Technique for Image Steganography Based on DWT and Huffman Encoding

Amitava Nag

*Dept. of Information Technology
Academy of Technology,
West Bengal University of Technology, Hoogly – 721212, India.*

amitava.nag@aot.edu.in

Sushanta Biswas

*Dept. of Engineering and Technological Studies
University of Kalyani,
Kalyani, Nadia – 741 235, West Bengal, India*

biswas.su@gmail.com

Debasree Sarkar

*Dept. of Engineering and Technological Studies
University of Kalyani,
Kalyani, Nadia – 741 235, West Bengal, India*

dsarkar70@gmail.com

Partha Pratim Sarkar

*Dept. of Engineering and Technological Studies
University of Kalyani,
Kalyani, Nadia – 741 235, West Bengal, India*

ppsarkar@klyuniv.ac.in

Abstract

Image steganography is the art of hiding information into a cover image. This paper presents a novel technique for Image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. Firstly two dimensional Discrete Wavelet Transform (2-D DWT) is performed on a gray level cover image of size $M \times N$ and Huffman encoding is performed on the secret messages/image before embedding. Then each bit of Huffman code of secret message/image is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Image quality is to be improved by preserving the wavelet coefficients in the low frequency sub-band. The experimental results show that the algorithm has a high capacity and a good invisibility. Moreover PSNR of cover image with stego-image shows the better results in comparison with other existing steganography approaches. Furthermore, satisfactory security is maintained since the secret message/image cannot be extracted without knowing decoding rules and Huffman table.

Keywords: Steganography, Frequency Domain, DWT, Huffman Coding, Information Hiding.

1. INTRODUCTION

Information hiding is an old but interesting technology [1]. Steganography is a branch of information hiding in which secret information is camouflaged within other information. The word steganography in Greek means “covered writing” (Greek words “stegos” meaning “cover” and “grafia” meaning “writing”) [2]. The main objective of steganography is to communicate securely in

such a way that the true message is not visible to the observer. That is unwanted parties should not be able to distinguish any sense between cover-image (image not containing any secret message) and stego-image (modified cover-image that containing secret message). Thus the stego-image should not deviate much from original cover-image. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Figure. 1 shows the block diagram of a simple image steganographic system.

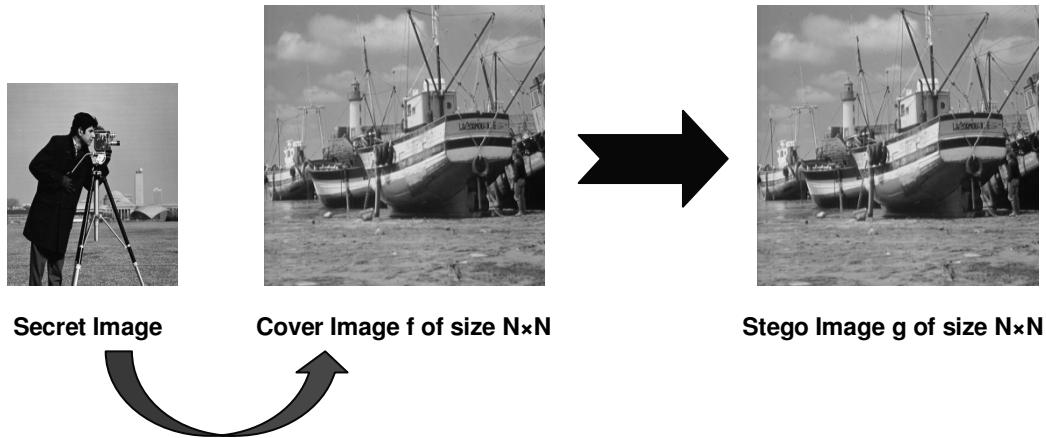


FIGURE. 1: The block diagram of a simple steganographic system

2. RELATED WORK

Image steganography schemes can be classified into two broad categories: spatial-domain [3,4,18] based and transform-domain based [5,6,7]. In spatial domain approaches, the secret messages are embedded directly. The simplest steganography is the Least Significant Bit (LSB) approach which was modified by several algorithms. In [8], a new steganography technique, named, “modified side match scheme” was proposed. It reserves the image quality, increases embedding capacity but is not robust against attack because it is a spatial domain approach and no transfer is used.

In [9] using VQ compression method is compressed the gray-level secret image before embedding. Next the compressed gray-level secret image is encrypted and then embedded into the DWT coefficients of the cover image. Though this paper provides a recovery scheme to repair the secret image if the stego-image is destroyed, but the PSNR of the stego-images are less than 36dB.

In the paper [10], the proposed steganography scheme embeds the secret message by modifying the Gabor coefficient of the cover image.

Abdelwahab and Hassan [11] used a data hiding technique in the DWT domain where 1-level DWT is performed on both secret and cover images. The disadvantage of this method is that the extracted data is not totally identical to the embedded version.

In [12], Bao P. and Ma X. embed a watermark in the singular value decomposition in the wavelet domain of an image.

In [13], Maity S.P. and Kundu M.K. proposes a blind watermarking techniques to embed the watermark redundantly in the multilevel wavelet coefficients of the LL and RR band of the cover image. The scheme is claimed to have robustness and have the ability to detect the degree of external attack already occurred in watermarked image, but PSNR is very low.

In [17], the major importance is given on the secrecy as well as the privacy of text messages, where the authors combines cryptography ,steganography and along with that an extra layer of security has been imposed in between them.

According to Raja et al. [16] fast Fourier transform (FFT) methods introduce round-off errors; thus it is not suitable for hidden communication.

The DWT based approach scheme [14] using a mapping table, the secret message is embeded in the high frequency coefficients resulted from Discrete Wavelet Transform. Among all other methods mentioned earlier, this method provides better quality of image, increases embedding capacity and is also robust against attack. Based on the same embedding capacity of [14], our proposed method improves both image quality and security.

2.1 Huffman Encoding and Huffman Table(HT)

Before embedding the secret image into cover image, it is first encoded using Huffman coding [15]. Huffman codes are optimal codes that map one symbol to one code word. For an image Huffman coding assigns a binary code to each intensity value of the image and a 2-D $M_2 \times N_2$ image is converted to a 1-D bits stream with length $LH < M_2 \times N_2$.

Huffman encoding is used to serve the following three:

Lossless Compression –It increases the embedding capacity

Security by means of encoding – Huffman encoded bit stream cannot reveals anything. To extract the exact meaning, the Huffman table is required to decode.

It provides one type of **authentication**, as any single bit change in the Huffman coded bit stream, Huffman table is unable to decode.

2.2 Discrete Wavelet Transform

Wavelets are special functions which (in a form analogous to sins and cosines in Fourier analysis) are used as basal functions for representing signals. The discrete wavelet transform (DWT) we applied here is Haar-DWT, the simplest DWT. In Haar-DWT the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels.

For 2-D images, applying DWT (Discrete Wavelet Transform) separates the image into a lower resolution approximation image or band (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components as shown in figure 3.

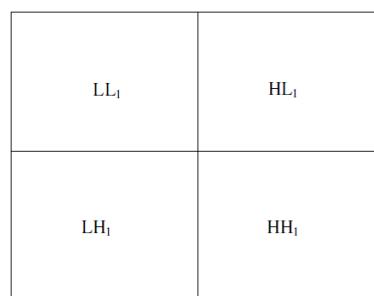


FIGURE 2: Components of 1-level 2-Dimensional Discrete Wavelet Transform

With the DWT, the significant part(smooth parts) of the spatial domain image exist in the approximation band that consists of low frequency wavelet coefficients and the edge and texture details usually exist in high frequency sub bands, such as HH, HL, and LH. The whole procedure

explained above is called the one-level 2-D Haar-DWT. The one-level 2-D Haar-DWT applied on the image “boat” is shown in Figure 4.

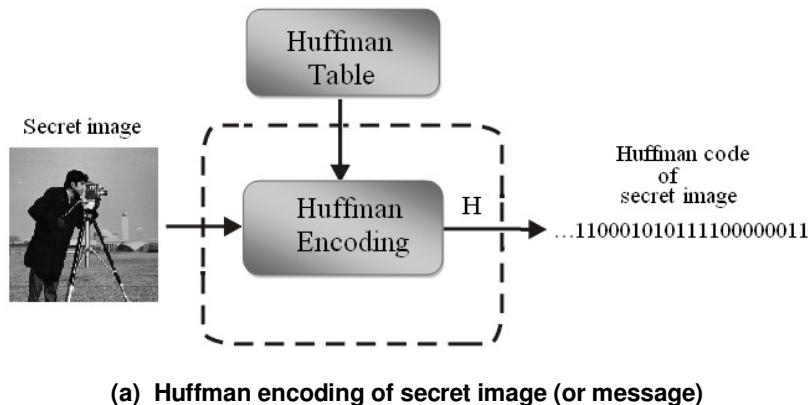


FIGURE 4: (a) Original image of boat, (b) Result after the one-level 2-D Haar-DWT

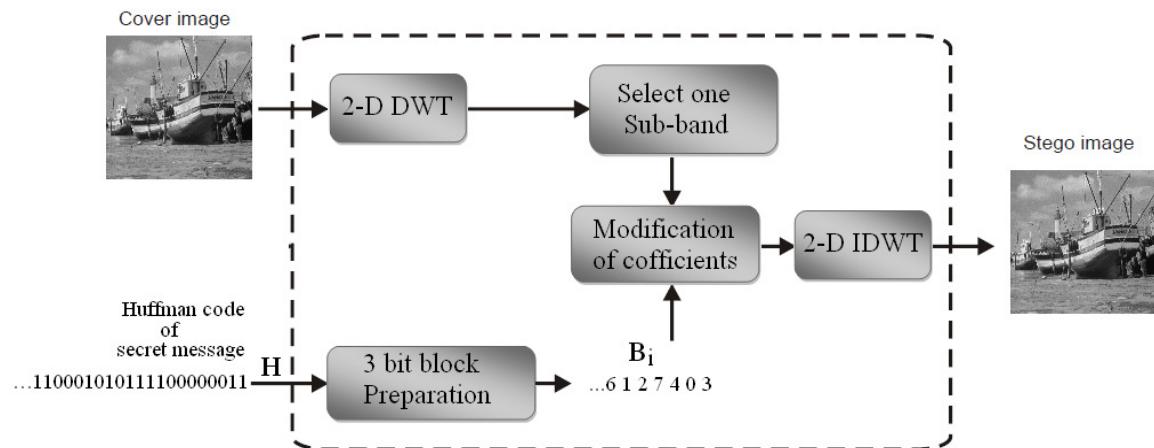
The human eyes are not sensitive to the small changes in the edges and textures of an image but very sensitive to the small changes in the smooth parts. This allows the secret message/image to be embedded at high frequency sub-bands without being perceived by the human eye.

3. PROPOSED IMAGE STEGANOGRAPHY ALGORITHM

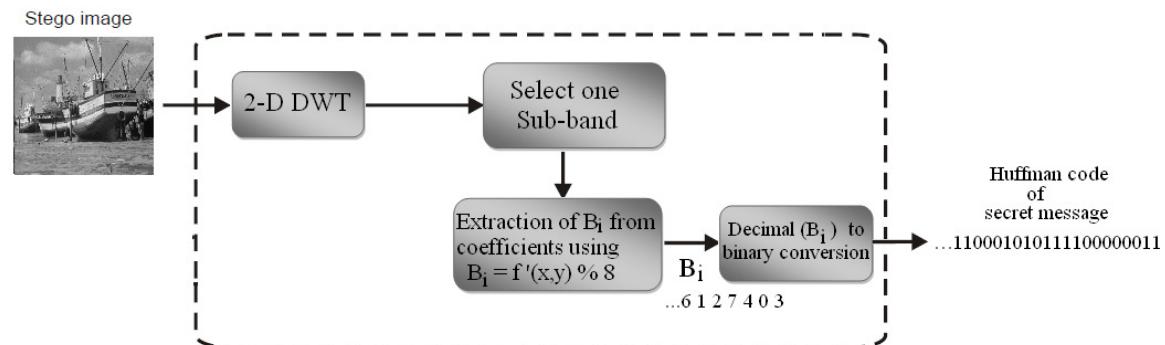
Hiding the secret message/image in the special domain can easily be extracted by unauthorized user. In this paper, we proposed a steganography technique using DWT (Discrete Wavelet Transform) for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The basic idea to hide information using DWT is to alter the magnitude of the DWT coefficients of three sub-bands, HH, HL, and LH of cover image. The schematic/ block diagram of the whole process is given in figure 2((a) to (d)).



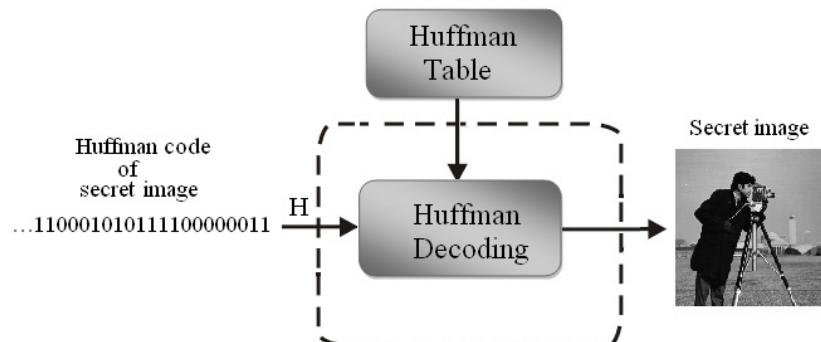
(a) Huffman encoding of secret image (or message)



(b) Insertion of a Huffman code of secret image (or message) into a Cover image



(c) Removal of Huffman code of secret Image (or message)



(d) Huffman decoding of secret image (or message)

3.1 3-bit Block Preparation

Huffman code H is now decomposed into 3-bits blocks and thus form a decimal value ranging from 0 to 7. For example, the binary sequence 110 001 010 111 100 000 011 will be changed to the decimal sequence (D)... 6 1 2 7 4 0 3.... The decimal sequence (D) is defined as follows:

$$D = \left\{ B_i \mid 1 \leq i \leq \frac{8 \times M \times N}{3}, B_i \in \{0,1,2,3,4,5,6,7\} \right\}$$

3.2 Embedding of Secret Message / Image

We proposed the secret message/image embedding scheme comprises the following five steps:

Step 1: Decompose the cover image by using Haar wavelet transform.

Step 2: Huffman encoding.

Perform Huffman encoding on the 2-D secret image S of size $M_2 \times N_2$ to convert it into a 1-D bits stream H .

Step 3: 3-bit block (B_i) preparation

Huffman code H is decomposed into 3-bits blocks and thus form a decimal value ranging from 0 to 7. For example, the binary sequence 110 001 010 111 100 000 011 will be changed to the decimal sequence (B_i) ... 6 1 2 7 4 0 3.

Step 4: Bits replacement

Select one sub-band for embedding the secret message. If we denote ' f' ' as coefficients matrix of the selected sub-band, then using the following equation, the 3 least significant bits of wavelet coefficients is replaced by the 3 bits of Huffman encoded bit stream in the form of 3 bit block B_i .

$$f'(x,y) = f(x,y) - f(x,y) \% 8 + B_i \quad \dots \dots \dots (1)$$

Step 5: IDWT

Apply the Haar inverse DWT (IDWT) on the DWT transformed image, including the modified sub-band to produce a new image f_1 which contains secret image.

Embedding Algorithm

Input: An $M_1 \times N_1$ carrier image and a secret message/image.

Output: A stego-image.

1. Obtain Huffman table of secret message/image.
2. Find the Huffman encoded binary bit stream of secret-image by applying Huffman encoding technique using Huffman table obtained in step 1.
3. Decompose the cover image by using Haar wavelet transform
4. Calculate the size of encoded bit stream in bits.
5. Repeat for each bit obtained in step 4
 - (a) Insert the 3 consecutive bits into 3 LSB position in each DWT coefficient of the selected sub-band.
6. Repeat for each bit obtained in step 2
 - (a) Insert the 3 consecutive bits into 3 LSB position in each DWT coefficient(excluding the first four coefficients in each sub-band) of the selected sub-band.
7. Repeat for each bit of the Huffman table
 - (a) Insert the 3 consecutive bits into 3 LSB position in each DWT coefficient of the selected sub-band.
8. Apply inverse DWT.
9. End.

3.3 Extraction of the Secret Message / Image

The stego-image is received in spatial domain. DWT is applied on the stego-image to transform the stego-image from spatial domain to frequency domain. The following formula is used to extract bit stream from wavelet coefficients in the form of blocks B_i .

$$B_i = f'(x,y) \% 8 \quad \dots \dots \dots (2)$$

The size of the encoded bit stream and the encoded bit stream of secret message/image are extracted along with the Huffman table of the secret message/image. The block diagram of the extracting process is given in figure 4((c) and (d)) and the extracting algorithm as follows:

Extraction Algorithm

Input: An $M_1 \times N_1$ Stego-image.

Output: Secret image.

1. Apply DWT to the stego-image.
 2. The size of the encoded bit stream is extracted from 1st four DWT coefficients in each subband by collecting the 3 least significant bits.
 3. The 3 least significant bits of all of the DWT coefficients inside each sub-bands(excluding the first four coefficients in each sub-bands) are collected and added to a 1-D array.
 4. Repeat step 3 until the size of the 1-D array becomes equal to the size extracted in step 2.
 5. Construct the Huffman table by extracting 3 bits from the LSB of all of the DWT coefficients inside each sub-bands excluding the coefficients used in step 2 and step 3.
 6. Decode the 1-D array obtained in step 3 using the Huffman table obtained in step 5.
 7. End.

4. SIMULATION RESULTS

In this section, some experiments are carried out to prove the efficiency of the proposed scheme. The proposed method has been simulated using the MATLAB 7 program on Windows XP platform. A set of 8-bit grayscale images of size 512×512 are used as the cover-image to form the stego-image. The Figure 6 (a) – (d) shows the original cover (carrier) images and Figure 7 shows the original secret message.

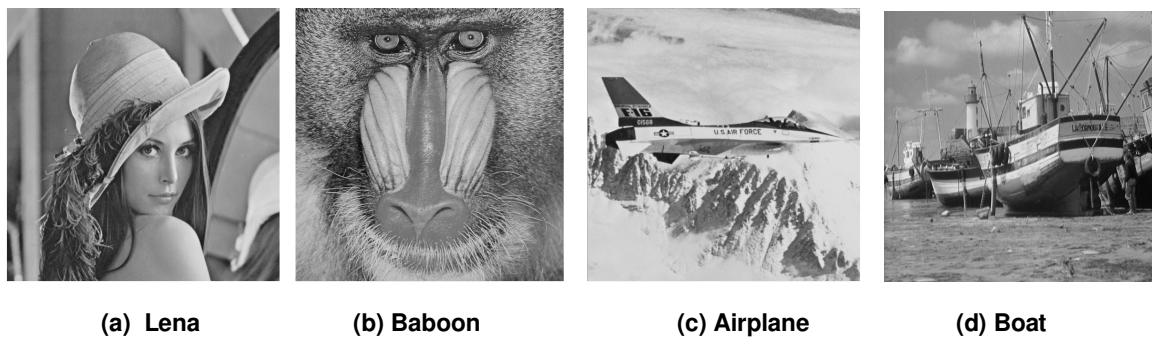
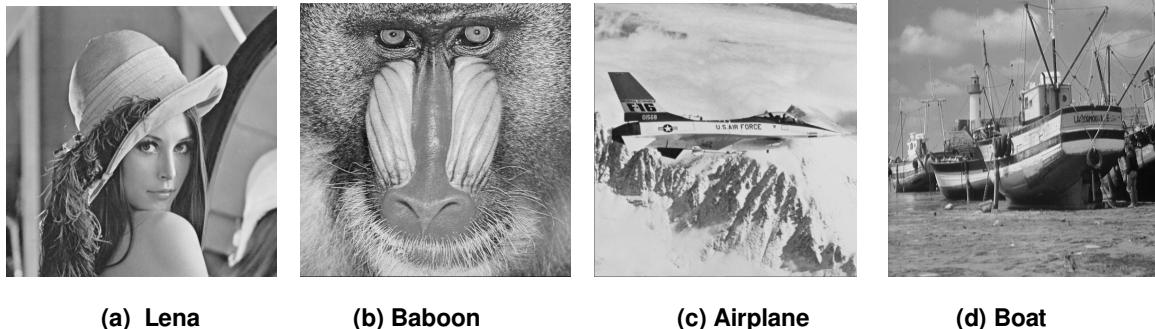


FIGURE 6: Four cover-images for simulations



FIGURE 7: Secret Image to be embedded



(a) Lena

(b) Baboon

(c) Airplane

(d) Boat

FIGURE 8: stego-images of the proposed methods



FIGURE 9: Extracted Secret Image

Here we are embedding a 8-bit grayscale image of size 256×248 into a 8-bit grayscale images of size 512×512 i.e. 507904 bits are embedded into a 512×512 carrier image. Here, PSNR value is utilized to evaluate the invisibility of the stego-images.

TABLE 1: COMPARISON OF RESULTS FOR THE PROPOSED METHOD AND DWT BASED MODEL[14]

Cover Image (512 × 512)	DWT base [14]		Our Method	
	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)
Lena	507856	46.0882	507856	54.93
Airplan	507856	45.9961	507856	54.67
Baboon	507670	46.1948	507670	55.11
Boat	507867	46.1385	507867	54.80

To compare the proposed approach with the DWTIS method [14], table 1 exhibit the capacity and PSNR after the secret data is embedded using those two approaches. From table 1 it is clear that for the same capacity, the PSNR of our proposed algorithm is better than the one in reference [14]. From table 1, it is noticed that for all images, PSNR is nearly 55. Figure 8 shows the resulted stego-images of the proposed methods and figure 9 extracted Image

5. CONCLUSION

Generally, image steganography method does not provide much attention on the basic demand of secrecy and privacy. In this paper, the major importance is given on the secrecy as well as the privacy of information. The embedding process is hidden under the transformation (DWT and IDWT) of cover image. These operations provide sufficient secrecy. On the other hand to obtain privacy we have used huffman encoding. In a similar type of paper[14] the authors have provided their attention on the security by a well designed mathematical mapping. Our paper deals with the Huffman encoding. After comparision it is found that in our paper PSNR is higher than the mentioned paper. Here lies the novelty of our research work.

6. REFERENCES

- [1] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques". Information Hiding, Artech House, pp. 43-78, 2000.
- [2] Moerland, T. "Steganography and Steganalysis". Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.pdf
- [3] Chan, C.K. and Cheng, L.M. "Hiding data in image by simple LSB substitution". Pattern Recognition, 37: 469 – 474, 2003.
- [4] Chang, C.C and Tseng, H.W. "A Steganographic method for digital images using side match". Pattern Recognition Letters, 25: 1431 – 1437, 2004.
- [5] Chen, T.S., Chang C.C., and Hwang, M.S. "A virtual image cryptosystem based upon vector quantization". IEEE transactions on Image Processing, 7,(10): 1485 – 1488, 1998.
- [6] Chung, K.L., Shen, C.H. and Chang, L.C. "A novel SVD- and VQ-based image hiding scheme. Pattern Recognition Letters" 22: 1051 – 1058, 2001.
- [7] Iwata, M., Miyake, K., and Shiozaki, A. "Digital Steganography Utilizing Features of JPEG Images, IEICE Transfusion Fundamentals". E87-A(4):929 – 936, 2004.
- [8] Chen, P.Y. and Wu, W.E. "A Modified Side Match Scheme for Image Steganography". International Journal of Applied Science and Engineering, 7(1): 53 – 60, 2009..
- [9] Chu, Y.P., Guo, S.W., Chan, Y.K. and Wu, H.C. "Image Hiding Based on a Hybrid Technique of VQ Compression and Discrete Wavelet Transform", International Computer Symposium, 313-317,2004.
- [10] Mythreyi S and Vaidehi V. "Gabor Transform based Image Steganography", IETE Journal of Research, 53(2):. 103 – 112,2007.
- [11] A.A. Abdelwahab, L.A. Hassan. "A discrete wavelet transform based technique for image data hiding", in: Proceedings of 25th National Radio Science Conference, Egypt, 2008.
- [12] Bao, P and Ma, X. "Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition", IEEE Transaction on Circuits and Systems for Video Technology, 15(1):2005
- [13] Maity S.P. and Kundu M.K., "A Blind CDMA Image Watermarking Scheme in Wavelet Domain" IEEE International Conference:2633 – 2336,2004.
- [14] Chen, P.Y. and Wu, W.E. "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, 4,3: 275 –290.
- [15] Jayaraman, S., Esakkirajan, S. and Veerakumar, T. "Digital Image Processing", Tata McGraw Hill Education Private Limited, India, 2009.
- [16] K.B. Raja, C.R. Chowdary, K.R. Venugopal, L.M. Patnaik. "A secure image steganography using LSB, DCT and compression techniques on raw images". Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing, ICISIP'05, Bangalore, India, 14–17 December 2005..
- [17]Debnath Bhattacharyya, Poulami Das, Samir kumar Bandyopadhyay and Tai-hoon Kim. "Text Steganography: A Novel Approach," International Journal of Advanced Science and Technology, vol.3, pp.79-85, February2009.

- [18] H. Arafat Ali. “Qualitative Spatial Image Data Hiding for Secure Data Transmission”. GVIP Journal, 7(1):35-43, 2007.