

# Image Steganography Using DWT and Semi Hexadecimal Code Based on PSNR

Balkar Singh

PhD Scholar, CSE Department, Thapar University, Patiala,  
Punjab, India

## Abstract:

**I**n this paper, a novel image steganography approach is proposed to enhance the visual quality of stego image. The cover image is decomposed using Discrete Wavelet Transform (DWT) to produce wavelet subbands and threshold value is calculated for each higher frequency wavelet subbands. Wavelet coefficients having magnitude larger than the threshold of its subband are selected to embed the secret data. Semi Hexadecimal Code (SHC) is proposed to convert pixel value of secret image into smaller equivalent value so that it distorts stego image as less as possible. Experimental results shows that maximum PSNR between cover image and stego image is more than 75 dB. Proposed approach is also compared with the existing approaches and this comparison shows that the proposed approach is better than the existing approaches.

**Keywords:** DWT, PSNR, EF, SHC, Threshold.

## I. INTRODUCTION

Steganography is a process of hiding a secret message in an ordinary message and the extraction of secret message, whenever required. Image steganography techniques are divided into two categories: spatial domain and frequency domain steganography. In spatial domain techniques, secret message is embedded in the image pixels, while in frequency domain techniques, image is first transformed and then secret message is embedded in the transformed image. Frequency domain techniques hide messages in significant areas of cover image which make them more robust than spatial domain techniques. Several approaches have been proposed for frequency domain steganography using different transforms [1-2].

Market *et al.* [3] proposed a watermarking technique in which the secret image is decomposed into wavelet subbands using DWT. The watermark is embedded into largest coefficients of high and middle frequency wavelet subbands of an image. Maximum PSNR proposed by their technique is 32.7 dB which is 0.14 dB more than Hsu *et al.* method [4].

Toaba *et al.* [5] proposed a technique in which secret message is embedded into least significant bits of wavelet coefficient of an image. Some pre-processing steps are applied on cover image to adjust saturated pixel components in order to recover the embedding message without losing cover image data. Cover image is adjusted before applying Integer Wavelet Transform followed by two levels DWT. Permutation of stego key is used to embed the bit stream of secret image after inverse IWT after that stego image is collected. Extraction process is just reverse of embedding process. Maximum PSNR offered by their technique is 73.91 dB.

Chen *et al.* [6] proposed a data hiding technique to hide data in high frequency wavelet sub-bands. The proposed technique is divided into two modes and three cases. The modes are fixed and varying. The cases are low embedding capacity, medium capacity and high capacity. Sequence mapping tables are used in raster scan manner to embed the data. For fix mode, 46.83 dB is the highest PSNR value and 39.00 dB is lowest. For varying mode, highest PSNR is 50.85 dB and minimum PSNR is 44.76 dB.

Ataby *et al.* [7] proposed a high capacity image steganography technique to hide the secret message into DWT subbands of cover image. Secret message is arranged into one dimensional data and RC4 is used to encrypt this data and then embedding is done. The maximum PSNR by their technique is 40.98 dB.

Nag *et al.* [8] proposed a DWT based technique for image steganography in which two dimensional (2-D) DWT is applied on the cover image and Huffman encoding is performed on the secret message before embedding. Then each bit of Huffman code of secret message is embedded in the high frequency wavelet coefficients. Maximum PSNR is 55.11 dB.

Kumar *et al.* [9] proposed dual transform technique for robust steganography in which the cover image is segmented into 4x4 size blocks and DWT is applied on each block. In the resulting DWT coefficients, blocks of vertical band of 2x2 each are considered and then IWT is applied to get a single coefficient. Then secret data is embedded into these coefficients using LSB method. Maximum PSNR is 39.8411 dB.

Shejul *et al.* [10] proposed a biometrics based steganography technique. Secret data is hidden in the high frequency subbands of DWT. Two cases are considered for data embedding. First is with cropping and another is without cropping. Both the cases are compared and analyzed from different aspects. Main feature of cropping case is that this results into an enhanced security because cropped region works as a key at decoding side, while without cropping case

uses embedding algorithm that preserves histogram of *DWT* coefficient after data embedding also by preventing histogram based attacks and leading to a more security. Maximum *PSNR* provided by proposed technique is 64.92 *dB*.

Ghasemi *et al.* [11] proposed a wavelet transform and genetic algorithm based steganography technique. Genetic algorithm based mapping function is used to embed data in *DWT* coefficients in  $4 \times 4$  blocks of the cover image. The optimal pixel adjustment process is applied after embedding the message. Maximum *PSNR* is 51.88 *dB*.

Bhattacharya *et al.* [12] proposed a *DWT* based steganography technique in which secret data is embedded in high frequency wavelet sub bands. An amplification factor is used to control the embedding effect. *PSNR* between cover image and stego image is 27.3850 *dB*.

Ioannidou *et al.* [13] proposed a novel image steganography technique to hide the data into sharp areas of image on the basis of the edges present in an image. A hybrid edge detector is used to detect the edges of the cover image. Maximum *PSNR* provided by the proposed technique is 46.88 *dB*.

From this analysis, one can conclude that there is the need to have trade-off between *PSNR* and capacity in image steganography. In this work, an approach is proposed, which provides better *PSNR* and high capacity.

## II. RELATED TERMS and DWT

### 2.1 Related Terms

Cover file is a file which can hide information inside of it. Stego file is one in which data has been hide inside it after steganography process.

### 2.2 DWT

*DWT* is a transform used to decorrelate the image energy into few wavelet coefficients. When *DWT* on one level is applied on an image, combination of four sub-bands with low and high frequencies are obtained. These sub-bands are low low ( $LL_1$ ), low high ( $LH_1$ ), high low ( $HL_1$ ) and high high ( $HH_1$ ). *DWT* can be further applied on  $LL_1$  to get the other four subbands which are  $LL_2$ ,  $HL_2$ ,  $LH_2$  and  $HH_2$ , as shown in Figure 1.

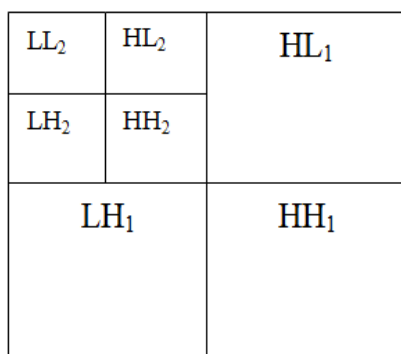


Figure 1. Two level DWT Structure

## III. PROPOSED APPROACH

Proposed approach is based on two observations. First, if the wavelet coefficients are transformed into smaller equivalent coefficients, the distortion in stego image is less. Second, if the secret data is embedded into selected high frequency wavelet subbands of cover image, then also distortion in stego image is less. Selection of the wavelet coefficients is performed using threshold of the wavelet subband.

### 3.1 Semi Hexadecimal Code

Semi Hexadecimal Codes (*SHC*) are used to encode the secret image. These codes reduces the pixel values of the secret image, as less quantative value is required to represent a hexadecimal code than its decimal equivalent. It is beneficial to embed smaller value rather than larger value to affect the stego image as less as possible. It is semi in the sense, in this code we are not using *A, B, C, . . . , F* letters for 10, 11, . . . , 15. We are using their exact value but at decimal place because *DWT* coefficient does not support alphabet embedding.

#### Algorithm 3.1 (Pseudo Code)

```

r1=Mod(N,16)
r2=Floor(N/16)
val=r2*10+r1;
if(r1<10)
    Hx=val;
else
    Hx=r2+r1/100;
end
    
```

Where *N* is the decimal number in base 10 and *Hx* is the equivalent *SHC* code. Mod operation finds the remainder of division of one number by another number. Floor function maps a real number to the largest previous integer.

For example, decimal number 26 is converted into 1.10 *SHC* and decimal number 200 is converted into 128 *SHC*.

### 3.2 Threshold of a Subband

After applying the *DWT* on cover image, threshold for each high frequency sub-bands (*i.e.* *LH*, *HL* and *HH*) is calculated using the approach proposed by Nick Method in [14] as

$$(1)$$

Where  $T$  is the threshold of a subband,  $\mu$  is mean of particular sub-band,  $C$  is a constant valued as -0.15 (Ni-black W., [14]. measured it -0.2),  $C$  is wavelet coefficient and  $n$  are dimensions of sub band. In proposed work, slight lesser of than original constant proposed by Ni-black is considered.

### 3.3 Proposed Approach: Embedding Process

- i. Apply *DWT* on cover image which produces four wavelet subbands, named as *LL*, *HL*, *LH* and *HH*.
- ii. Find the threshold  $T$  for *HL*, *LH* and *HH* using (1).
- iii. If  $S(x, y) \geq T$ ; embed the data using

where  $\tilde{S}$  is modified wavelet coefficient,  $S$  is original wavelet coefficient, and  $Hx$  is semi hexadecimal representation of secret data which is obtained using Algorithm 3.1 and  $(x, y)$  are spatial coordinate of subband.  $EF$  is the embedding factor which is used to balance the embedding effect.

- iv. Apply *IDWT* to produce the Stego image.

Extraction process is just inverse of the embedding process.

## IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed approach is implemented in MATLAB 7.0. The cover image is decomposed into two levels using Haar wavelet. Embedding Factor ( $EF$ ) is used to balance the embedding effect. It is better to use the lesser value of  $EF$ , so  $e^{-n}$  ( $e$  is base of natural logarithms) is used where  $n$  is a positive integer such as  $n \geq 2$ . Some of the images considered are shown in Figures 2-4.



Figure 2. (a) Original Lena cover image ( $512 \times 512$ ), (b) Original Barbara Secret image ( $389 \times 389$ ) (c) Stego Lena image that has image (b) inside it, and (d) Recover image from (c)

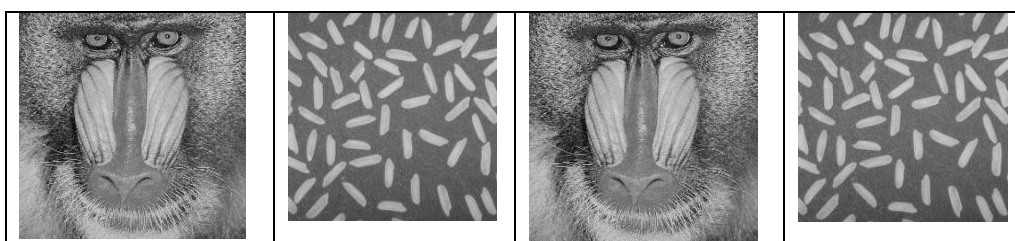


Figure 3. (a) Original Baboon cover image ( $256 \times 256$ ), (b) Original Secret rice image ( $192 \times 192$ ) (c) Stego Baboon image after embedding rice, and (d) Recover rice image from Baboon stego image.



Figure 4. (a) Airplane image ( $512 \times 512$ ), (b) Original Barbara Secret image ( $433 \times 433$ ) (c) Stego airplane image after embedding Barbara image, and (d) Recover Barbara image.

Table 1. PSNR of cover images and secret images using proposed approach

Cover image	Secret image	$EF$	$PSNR^1$ (in dB)	$PSNR^2$ (in dB)	Run time for embedding (in seconds)
Lena 512×512	Barbara 389×389	$e^{-4}$	48.2855	34.5368	3.5938
Baboon 256×256	Rice 192×192	$e^{-7}$	75.1231	49.0147	0.7969
Airplane 512×512	Barbara 433×433	$e^{-5}$	56.4701	31.2687	4.3906
Rose 256×256	Grapes 212×212	$e^{-5}$	53.9722	26.8148	0.7031
Cat 256×256	Grapes 198×198	$e^{-5}$	54.4364	27.5601	0.6875
Cat 256×256	Banana 198×198	$e^{-5}$	55.3960	21.2022	0.7188
Bird 256×256	Elephant 240×240	$e^{-7}$	75.3142	34.3603	0.8125

$PSNR^1$  between cover image and stego image and  
 $PSNR^2$  between secret image and extracted image.

The results shown in Table 1 are the  $PSNR$  between cover image and stego image,  $PSNR$  between original secret and recovered image. Maximum  $PSNR$  of the proposed approach is **75.3142 dB**.

The proposed approach is compared with the existing approaches and the results of this comparison are shown in Table 2. This comparison depicts that the proposed approach is better among existing approaches in term of  $PSNR$ .

Table 2. Comparison of proposed approach with existing approaches

Methods Met-rics	Ref. 4	Ref. 5	Ref. 6	Ref. 7	Ref. 8	Ref. 9	Ref. 10	Ref. 11	Ref. 12	Ref. 13	Proposed Approach
$PSNR^1$ in dB	41.7	73.9	50.8	40.98 <sup>#1</sup> 22.84 <sup>#2</sup>	55.1	39.84 <sup>#1</sup> 50.30 <sup>#2</sup>	64.9	51.88	27.39	46.88	75.314
$PSNR^2$ in dB	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	34.360

$PSNR^1$ : between cover image and stego image  
 $PSNR^2$ : between secret image and recovered image  
#1: Best case for  $PSNR$ , #2: Best case for Capacity,  
N.A.: Not Available

A comparison between the maximum  $PSNR$  of the existing algorithms and proposed algorithm is carried out in Figure 5. In this figure, X-axis represent approaches and Y-axis represents  $PSNR$  between cover image and stego image.

Figure 5. Graph among  $PSNR$  of proposed approach and other approaches.

From this figure, one can conclude that proposed approach has high  $PSNR$  values than the existing approaches. Hence visual quality of stego image is better.

## V. CONCLUSION

In this paper, a novel image steganography approach based on  $DWT$  and  $SHC$  is proposed. Secret data is embedded into those pixels of cover image having magnitude greater than the threshold value. Maximum  $PSNR$  between cover image and stego images is more than 75 dB. The comparative analysis between the proposed approach and the existing approaches shows the superiority of the proposed approach.

## REFERENCES

- [1] Gonzalez R. C. and Woods R. E., "Digital Image Processing," Prentice Hall, 2nd Ed, 2002.
- [2] Morkel T., Eloff J. H. P., and Olivier M. S., "An Overview of Image Steganography," Proceedings of Fifth Annual Information Security South Africa Conference, Sandton, South Africa, pp. 1-12, 2005.
- [3] 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.

- [4] Hsu and Wu, "Hidden digital watermarks in images," IEEE Transactions on Image Processing, vol. 8, pp. 58-68, 1999.
- [5] Tolba M. F., Ghonemy M. A., Taha I. A. and Khalifa A. S., "Using Integer Wavelet Transform in Colored Image-Steganography," International Journal of Intelligent and Cooperative Information System, vol. 4 no. 4, pp. 75-85, 2004.
- [6] Chen P. Y., and Lin H. J., "A DWT Approach for Image Steganography," International Journal of Applied Science and Engineering, vol. 4, no. 4, pp. 275-290, 2006.
- [7] Ataby A. A., and Naima F. A., "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.
- [8] Nag A., Biswas S., Sarkar D. and Sarkar P. P., "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding," International Journal of Computer Science and Security, vol. 4, no. 6, pp. 561-570, 2010.
- [9] Kumar K. B. S., Raja K. B. and Pattnaik S., "Hybrid Domain in LSB Steganography", International Journal of Computer Applications, vol. 19, no. 7, pp. 35-40, 2011.
- [10] Shejul A. A., and Kulkarni U. L., "A Secure Skin Tone based Steganography Using Wavelet Transform," International Journal of Computer Theory and Engineering, vol. 3, no. 1, pp. 16-22, 2011.
- [11] Ghasemi E., Shanbehzadeh J. and Fassihi N., "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm," International Multiconference of Engineering and Computer Scientist, vol. 1, pp. 1-4, 2011.
- [12] Bhattacharya T., Dey N. and Chaudhuri S. R. B., "A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum," International Journal of Modern Engineering Research, vol. 1, no. 1, pp. 157-161, 2011.
- [13] Ioannidou A., Halkidis S. T., and Stephanides G., "A novel technique for image steganography based on a high payload method and edge detection", Expert Systems with Applications, Elsevier, vol. 39, pp. 11517-11524, 2012.
- [14] 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.