Robust DWT Based Technique for Digital Watermarking

Mamta Jain
Department of Electronics & Communication
Institute of Engineering & Technology
Alwar
er.mamtajain@gmail.com

Neha Singh
Department 0f Electronics & Communication
Institute of Engineering & Technology
Alwar
nneha.singh01@gmail.com

***Abstract*—** Hiding the information over other information plays a vital role in securing the data. Steganography is art of hiding the information into other information in such a manner that hidden information cannot be easily perceptible by human eye. This paper presents a new technique for image hiding based on DWT. In our approach, single-level DWT is performed on the cover image by Haar wavelet and then its HL and LH detail components are used for embedding two watermark images associated with embedding algorithm.
The proposed method gives an improved bit correct ratio which is nearly about 99%.

Keywords- Steganography, single-level DWT.

I. INTRODUCTION

With the widespread use of multimedia information, digital forgeries and unauthorized sharing of digital content have increased threat among multimedia content creators, distributors and users. This phenomenon coupled with the exponential increase of computer performance, has facilitated the distribution of multimedia data such as images. Publishers, artists, and photographers, however are unwilling to distribute pictures over the internet due to lack of security; images can be easily duplicated and distributed without the owner's consent. This problem can be solved by using Steganography technique. *Steganography* is the process of hiding of a secret image within an ordinary image and extracting it at its destination. Anyone else viewing the message will fail to know that it contains secret/encrypted data. The term *Steganography* is retrieved from the Greek words *stegos* means *cover* and *grafia* meaning *writing* defining it as *covered writing* [1]. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, Steganography focuses on keeping the existence of a message secret [2].

The objectives of Steganography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data [3].

II. VARIOUS STEGANOGRAPHY TECHNIQUE

Currently the digital watermarking technologies can be divided into two categories by the embedding position-spatial domain and transform domain watermark [4]. It can also classify in two categories based on retrieval of hidden data and original image: Reversible and Irreversible [5]. It can further classify into Robust and fragile techniques depend on whether the hidden data is destroyed or not after

modifying the file [1] [8]. In Fragile digital watermarking, if the file is modified the hidden data is destroyed.

III. DWT Based Watermarking

Wavelet transform is used to convert a signal from time domain to spatial domain [6]. Discrete Wavelet Transform (DWT) allows images to be viewed and processed at multiple resolutions and provides a powerful insight into an image's spatial and frequency characteristics. It separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components which is shown in fig1. The process can then be repeated to computes multiple "level" wavelet decomposition which is shown in fig2.

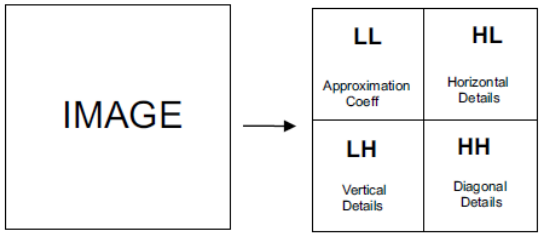
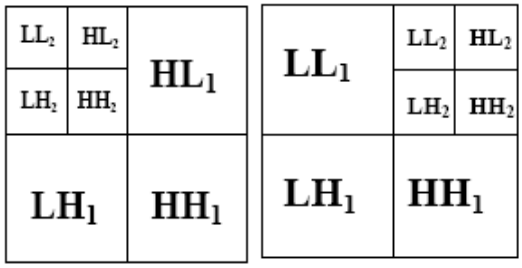


Fig. 1 Output of 1-level 2-D decomposition



(a) (b)

Fig.2 (a) Second level decomposition of approximation sub-band. (b) Second level decomposition of horizontal sub-band.

The frequency domain transform applied in our method is Haar-DWT, the simplest DWT [7]. A 2-dimensional Haar-DWT consists of two operations: one is the horizontal operation and the other is the vertical one. In the first step, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) and differences represent the high frequency part of the original image (denoted as symbol H). In the second step, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom. Repeat this operation until all the columns are processed. Finally we will get 4 sub-bands denoted as LL, HL, LH and HH. After each transform is performed the size of the square which contains the most important information is reduced by a factor of 4 [7].

The LL sub-band is the low frequency portion and hence looks very similar to the original image. Human eyes are very sensitive in this sub-band. So we can hide secrete data in the other three sub-bands, because human eyes are less sensitive in these sub-bands. In this work, the frequency coefficients of LH sub-band and HL sub-band of Haar-DWT is used for hiding two watermark images.

IV. Proposed Algorithm

In this paper, we proposed a new algorithm for embedding two watermark images in a single cover image. The block diagram of proposed technique is shown in fig3 and fig4 for embedding and extracting the watermark images.

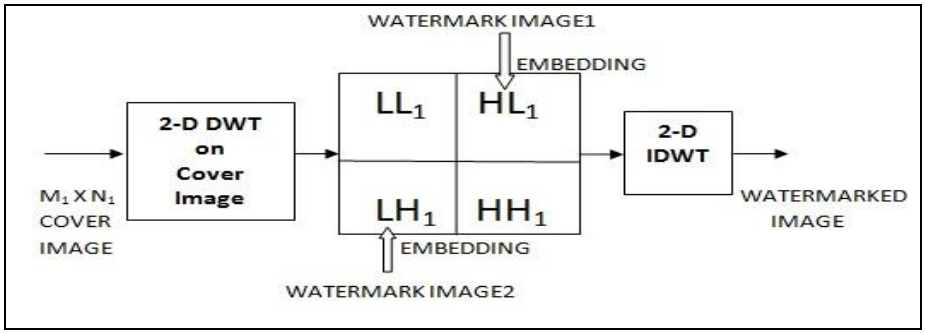


Fig. 3 Block Diagram of Proposed Embedding Algorithm

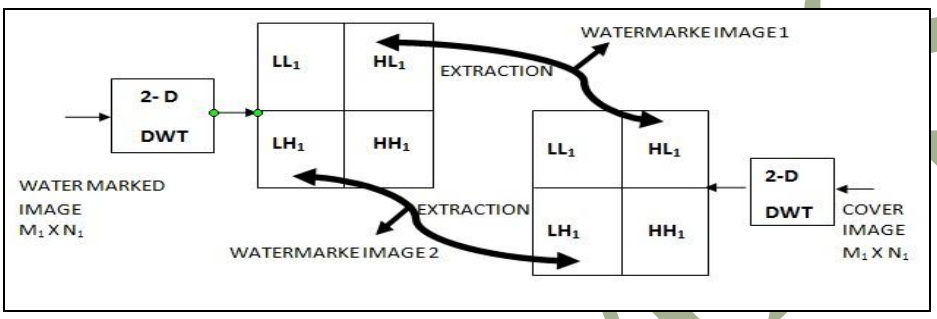


Fig. 4 Block Diagram of Proposed Extraction Algorithm

The process of embedding two watermark images in a cover image is given by embedding algorithm and the reverse process i.e. extracting the watermark images from the watermarked image is given by extraction algorithm.

Embedding Algorithm:

Input: - Cover image and two watermarks.

Output: - watermarked image.

Step 1. Input the cover image and two watermark images in MATLAB.

Step 2. Perform the single-level two-dimensional wavelet decomposition of cover image by 'Haar' wavelet.

Step 3. Take detail horizontal and vertical coefficient matrix corresponding to high-low and low-high frequency band of Dwt.

Suppose

D1= detail horizontal coefficient Matrix

D2 = detail horizontal coefficient Matrix

Step 4. Put all the Dwt values of D1 matrix in a vector and sort the vector in descending order and also find their index values.

Step 5. Choose r_1*c_1 index values from the sorted vector starting from 1000.

i.e. 1000 to r_1*c_1 + (1000-1)

Where r_1 is total number of rows in D1 matrix

& c_1 is total number of columns in D1 matrix

Step 6. Find the associated row-column order for vector values from selected r_1*c_1 indexed values by the formula

For associated column in the image

Floor (index value/ r_1) +1

For associated row in the image

Mod (index value, r_1)

Step 7. Insert the secret image in the associated row-column of D1 matrix by changing its coefficient on the basis of coefficient of secret message by the relation

$$C_{D1new} = C_{D1} + \varepsilon C_{D1} * W_i$$

Where ε denotes the watermarking strength

C_{D1} is the coefficient of D1 matrix.

C_{D1new} is the modified coefficient of D1 matrix.

W_i is the i^{th} coefficient of watermark image1.

Step 8. Repeat step 4 to step 7 for D2 matrix and embed watermark image2 in it and get the modified coefficient of D2 matrix

Step 9. Perform single-level two-dimensional wavelet reconstruction (i.e. inverse of Dwt) by taking modified D1 and D2 matrix which gives watermarked image.

Extraction Algorithm for Watermark Images:

Input: - Cover image and watermarked image.

Output: - Recovered watermark images.

Step 1. Take the watermarked image and perform the two-dimensional wavelet decomposition.

Step 2. Extract its HL and LH sub band coefficient matrix.

Step 3. Compare the extracted horizontal and vertical coefficient matrix with D1 and D2 matrix respectively to get the recovered watermark image.

V. Result And Conclusion

In this work, the cover image of 512×512 pixels and two randomly generated watermark images have been used which is shown in fig 5 and fig 7.Simulation of proposed algorithm is done on MATLAB 7.8.0.

Fig. 5 Cover image 1

Fig. 6 Cover Image2

(a) (b)

Fig. 7 (a) Watermark image1 and (b) watermark image2

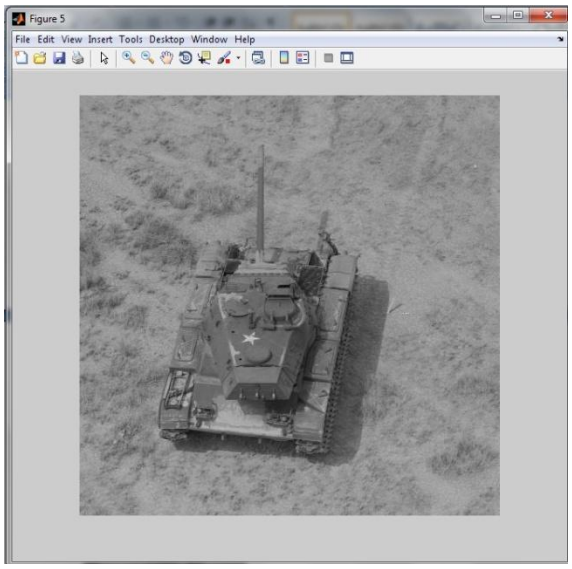


Fig.8 watermarked image1

Fig. 9 Watermarked image2

(a) (b)

Fig. 10 (a) Recovered Watermark image1and (b) Recovered Watermark image2

The proposed algorithm gives a high PSNR value and high BCR (bit correct ratio). The BCR can be increased by varying the parameter ε (i.e. watermarking strength) to nearly about 100%. At ε = 0.20, PSNR and BCR value for both the watermark image is given by table 1.

	Proposed Algorithm	
PSNR	**1.9×10^5**	
BCR	**90.6 for watermark image1**	**99.7 for watermark image2**

Table 1. PSNR and BCR values for proposed method

This method proposes an invisible watermarking technique since we cannot detect embedded watermark in the watermarked image. This method is also unaffected by various attacks that are salt & pepper noise, Meadian filtering, compression attack.

VI. REFERENCES

[1] R.Poornima, R.J.Iswarya, "An Overview of Digital Image Steganography", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1, February 2013, PP 23-31.

[2] Kanzariya Nitin K., Nimavat Ashish V., "Comparison of Various Images Steganography Techniques", International Journal of Computer Science and Management Research, Vol 2, Issue 1, January 2013, ISSN 2278-733X, pp. 1213-1217.

[3] Deepa S, Umarani R, "A Study on Digital Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January - 2013, ISSN: 2277 128X , pp.54-57

[4] Blossom Kaur, Amandeep Kaur, Jasdeep Singh, "Steganographic Approach for Hiding Image in Dct Domain", International Journal of Advances in Engineering & Technology, July

2011, Vol. 1, Issue 3, ISSN: 2231-1963, pp.72-78

[5] Sushil Kumar, S.K.Muttoo, "A Comparative Study Of Image Steganography In Wavelet Domain", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 2, Issue. 2, February 2013, ISSN 2320–088X, pg.91 – 101

[6] Souvik Bhattacharyya, Gautam Sanyal, "A Robust Image Steganography Using DWT Difference Modulation (DWTDM)", I. J. Computer Network and Information Security, july-2012, pp. 27-40.

[7] Santhi K, Anil Kumar M N, "Biometrics based Steganography using Circular Folding in DWT Domain", International Journal of Computer Applications, Volume 61– No.10, January 2013, ISSN 0975 –8887, pp 47-51

[8] Jih Pin Yeh, Che-Wei Lu, Hwei-Jen Lin, and Hung-Hsuan Wu, "Watermarking Technique Based On DWT Associated With Embedding Rule", International Journal Of Circuits, Systems And Signal Processing, Issue 2, Volume 4, 2010, pp 72-82.

[9] Yedla dinesh, Addanki purna ramesh, "Efficient Capacity Image Steganography by Using Wavelets", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1, Jan-Feb 2012, ISSN 2248-9622, pp 251-259.

[10] A.Nag, S. Biswas, D. Sarkar, P.P. Sarkar, "A novel technique for image Steganography based on Block-DCT and Huffman Encoding", International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010, pp 103-112.

[11] H S Manjunatha Reddy, K B Raja, "High Capacity And Security Steganography Using Discrete Wavelet Transform", International Journal of Computer Science and Security (IJCSS), Volume 3, Issue 6, pp 462-472.