Image Watermarking Using Wavelet Transform

Dr. Jane J. Stephan
Iraqi Commission for Computers and Informatics
Informatics Institute for Postgraduate Studies/Baghdad
E-mail: JaneJaleel@yahoo.com
Esraa Jaffar Baker
Al-Mustansiriyah University/ Baghdad
E-mail: esraajaffer2005@yahoo.com

ABSTRACT

This research, embedding watermarking in still images (BMP) true color, this method embedding watermark in large coefficients in high frequency subbands by using discrete wavelet transform, the watermark in this method is capable of surviving against the JPEG2000 compression, the watermark extracted using original image (non-blind watermark).

The research applied to many images, and the results for this method is robust against extraction watermarking on the average 90-95% (in data payload 208 bits) and using lowpass, highpass filters and JPEG2000 compression.

Keyword: Digital Watermark, Wavelet Transform, JPEG2000 compression.

1. Introduction

The more information is placed in the public's reach on the internet, the more owners of such information need to protect themselves from unwanted surveillance, theft and false representation and reproduction; they can use information hiding to protect themselves [1].

Data hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly[2].

There are two types of data hiding the first one is, steganography and the second is digital watermarking.

Steganography, is a word derived from Greek meaning “covered writing”, is the hiding of a secret message inside another message so that no one can detect or decode the secret message. Steganography is used in espionage – both corporate and in the intelligence industry, for example the entertainment industry for copyright purposes, and there is speculation that terrorists use it for some means of communication as well [3].

Digital Watermark is the process of embedding a signal, called the watermark, into another signal, called the host or cover, robustly and at the same time imperceptibly. The host signal can either be an image, audio, video or a text document (for example, program source code)[4].

Several watermarking have been proposed. Some methods embed the watermark in the spatial domain of the image. Other watermarking techniques use transform methods, such as the FFT, DCT, or the wavelet transform to embed the watermark. Recent developments have also seen the use of the Human Visual System to improve watermark performance [5].

2. Wavelet domain techniques

Wavelet domain techniques are becoming very popular because of the developments in the wavelet stream in the recent years. Wavelet based compression is used in the JPEG2000 compression; this feature can be exploited in embedding the watermark [6].

Advantages of Watermarks in the Wavelet Transform

1- Watermarking in the wavelet domain is compatible with the JPEG 2000 compression standard.

2- The capability to better localize the features (edges, textures) to which changes the human eye is more sensitive. With the wavelet transform the edges and textures are represented by large coefficients in high frequency sub-bands: a slight modification of these coefficients is difficult for the human eye to perceive.
3- The capability to localize information in time and frequency: in the case of 2-D color images the time domain is the spatial location of pixels and the frequency domain is the color variation around a pixel. The wavelet functions have a compact support and are local both in frequency and in time. This localization makes a watermark scheme based on wavelets more robust.
4- The watermark transform requires a lower computational cost than the Fourier or the Cosine transform (O (n) instead of O (n×log(n)), where n is in the length of the signal to be transformed). [7]

2.1. Wavelet Transform

This research applies wavelet transform by using Haar wavelet. In this method the proposed system embeds watermark three times in subbands. In this method the watermarking will be able to survive in spite of a high degree of compression by using the compression standard JPEG2000. Data are embedded in blue color. It is better than green and red colors for embedding watermark because the human visual system is less sensitive to this color. In level one choose the three subbands to host the data of watermarking and, the three subbands which are (low-high, high-low, and high-high), because 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 of an image, the subband (low-low). With the DWT, the edges and textures usually exist in high frequency sub bands, such as HH, HL, and LH. The large coefficients in these bands usually indicate edges and texture in the image [7, 8, and 9]. Therefore, embedding the watermark into the maximum coefficients of the detail subbands is difficult for the human vision system to perceive.

2.2. Embedding Watermark in Wavelet Method.

First step input the original image (24-bit), watermark text and**,** threshold and the output image watermarking (24-bit). Below is shown the embedding algorithm.

Algorithm for Embedding Watermark in Wavelet Transform

Step1: Input the image, watermark, threshold.
Step2: Convert the watermark into a stream of bits (zeroes, and ones).
Step3: Decompose image by using Haar wavelet transform.
Step4: Load the subbands that used to host the watermark data are (LH, HL and HH) in level one, and repeated the watermark in each subband.
Step5: Insert the data in the wavelet coefficients (which have the largest values) in subbands.
Step6: Reconstruct the image by using inverse Haar wavelet transform.
Step7: Save watermarked color image.
Step8**:** Display watermarked image.

2.3. Extraction of Watermark in Wavelet Transform.

To extract watermark from image we need to compare the original image with image watermark. In this method we need to input the original image, watermarking text and threshold and the output watermarking text, Below is shown the extraction algorithm.

Algorithm for Extraction Watermark in Wavelet Transform.

Step1: Input original image, image watermarking and threshold.
Step2: Decompose image by using Haar wavelet transform.
Step3: Extract data from (LH, HL and HH) in level one.

Step4: Sort data in each subbands in original image to extract the max coefficients and location for coefficients

Step5: Compare between coefficients in two images depending on locations of them,

If coefficient embedding > coefficient original then the data store in it is 1.

If coefficient embedding < = coefficient original then the data store in it is 0.

Step6: Compare between binary bits that generate three copies to extraction the watermark bits, if difference is more than half it means we get the incorrect value.

Step7: Display watermark text.

3-Experimental and Results

In this research implements into many images, This results for one image by Haar wavelet transform, as shown in Figure (1) the original image. The results are discussed as follows.

Figure(1) Original Image

The image dimensions are 264x264, Image size before compression: 204.2 kb, Data Payload: 208 bit.

1. The example of implementation in wavelet method gives, the results for PSNR after embedding and after using lowpass, highpass filters shown in table (1) and Figure(2).

Table (1) PSNR for Computer Image in Wavelet Transform

Threshold	PSNR After Embedding	PSNR After LowPass Filter	PSNR After HighPass Filter
1	59.626	46.656	46.167
2	56.616	46.639	46.154
3	54.855	46.612	46.132
4	53.605	46.574	46.102
5	52.636	46.527	46.064
6	51.844	46.470	46.018
7	51.175	46.405	45.965
8	50.595	46.333	45.906
9	50.084	46.253	45.840
10	49.626	46.167	45.769
11	49.212	46.077	45.693

The result of PSNR depends on threshold, when the threshold increases PSNR decreases in the same image.

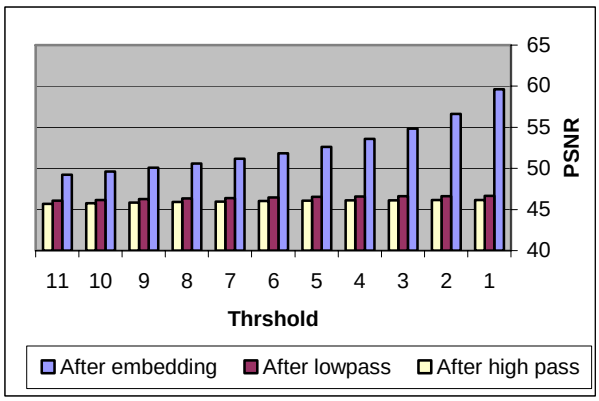

Figure (2) Relation PSNR After Embedding, Lowpass and Highpass

2. Apply image in example for JPEG2000. The results are discussed in table (2) and Figures (3), (4).

Table (2) Computer Image after JPEG2000 in Wavelet Transform

Threshold	Quality	Image Size	Comp. Ratio	PSNR	Success rate
1	88.0 87.9	51.5 37.5	3.96 5.44	59.597 50.959	100% 89.9%
2	87.9	37.5	5.44	50.816	98.5%
3	87.9 85.0 80.0 75.0 70.0	37.3 36.3 33.8 32.0 29.9	5.47 5.62 6.04 6.38 6.82	50.564 50.445 50.126 49.900 49.707	100% 100% 100% 100% 99.5%
4	70.0 65.0 60.0	29.9 27.8 25.5	6.82 7.34 8.00	49.535 49.391 48.890	100% 100% 99.5%
5	60.0 55.0 50.0 45.0	25.3 23.0 21.1 19.0	8.07 8.87 9.67 10.74	48.644 48.163 47.945 47.662	100% 100% 100% 99.5%
6	45.0 40.0	19.2 17.1	10.63 11.94	47.531 47.387	100% 99.0%
7	40.0 35.0	17.1 15.0	11.94 13.61	47.252 46.890	100% 98.5%
8	35.0 30.0 25.0	14.9 12.9 10.7	13.70 15.82 19.08	46.782 46.377 46.001	100% 100% 96.6%
9	25.0	10.8	18.90	45.950	99.0%
10	25.0	10.7	19.08	45.850	99.5%
11	25.0	10.8	18.90	45.769	100%

In this table when you select threshold (1) and quality (88.0) the image size is (51.5) and compression ratio (3.96), this shows the watermark extraction is completely (success rate is 100%), and in the same threshold when the quality deceases (87.9), image size decrease (37.5) and compression ratio (5.44) increases. This shows the watermark bit success rate is (89.9%), the solution for this case is by increasing the threshold we can see that in threshold (2), the success rate is (98.5%) in (87.9) quality and in threshold (3), the success rate is (100%) in (87.9) quality .

When increases the threshold the PSNR decreases.

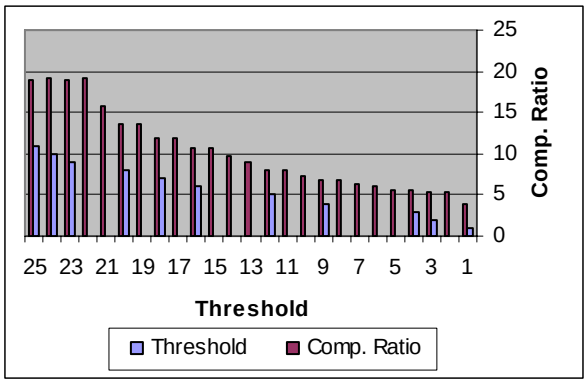

Figure (3) Relation between Threshold and Comp. Ratio

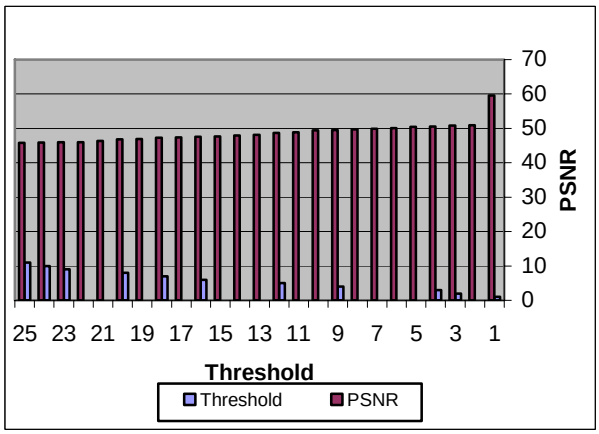

Figure (4) Relation between Threshold and PSNR

5. Conclusion

There are number of conclusions were derived from this research:-

1- Destroying measure methods are acceptable in method.
2- Repeating watermark three times in image increases robustness against attack.
3- In wavelet transform, when the threshold increases between the magnitude of the wavelet coefficients of the transformed image and the reconstructed (after compressed by JPEG 2000) image, the PSNR decreases.
4- In wavelet transform, when the compression ratio increases the survived embedded watermark bits will decrease.

References:

[1] N.F. Johnson, Z. Duric, S. Jajodia, "*Information Hiding Steganography and Watermarking-Attacks and Countermeasures*", Kluwer Academic Pub.2000.

[2] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "*Information Hiding-A Survey*", proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 87(7): 1062-1078, July 1999.

[3] T. Armstrong, K. Yetsko, "*Steganography*", CS-6293 Research Paper, Instructor: Dr. Andy Ju An Wang, 2004. http//cse.spsu.edu/jwang/research/security/steganography.pdf

[4] A. Sequeira "*Enhanced Watermark Detection* ",M. Sc., thesis, University of Toronto, Canada, 2003

[5] Project Report, "*Digital Image Watermarking*", EE381K-Multimedia Signal Processing", 12/5/1998.

[6] G. Jain, "*Digital Image watermarking* ", Indian Institute of Information Technology, 2002,Internet Report, gaurav@gdit.iiit.net, gjain_iiit@chequemail.com

[7] A. lumini, D. Maio "*A blind Watermarking System for Digital Images in the Wavelet Domain*", University of Bologna, Viale Risorgimento, PDF. E-mail: [alumini, dmaio]@deis.unibo.it

[8] X. G. Xia, " *A Multi Resolution Watermark for Digital Images*" proc. IEEE Int. Conf. on Image Processing ,vol.1, pp.548-551, oct. 1997.

[9] A. K. Musa, "*Watermark Applications in Color Image using Wavelet Transforms* ", PH.D, thesis, Iraqi Commission for Computer and Informatics, Baghdad, Iraqi, 2004