A Digital Watermarking for images using wavelet transform domain

Rawsam Abduladheem Hasan
University of AL-Mustansiriya /The College of Science

1. Introduction

With the revolution of information technology and Wide Area Networking, data has become less and less private where the accesses of media as well as the attempts to change and manipulate the contents of media data have become a common case. For that, we need to use a watermarking technique to protect the copyright of the media as well as for digital right management but without leaving a visual effect. [1]

The concept of digital watermarking arose while trying to solve problems related to the copyright of intellectual property in digital media. It is used as a means to identify the owner or distributor of digital data. Watermarking is the process of encoding hidden copyright information since it is possible today to hide information messages within digital audio, video, images and texts, by taking into account the limitations of the human audio and visual systems. [2]

2. Digital Watermarking Techniques:

A watermark is hidden information within a digital signal. For the watermarking several techniques have been developed. Watermarking technique can be divided into two main groups:

- Spatial domain watermarking,
- Frequency domain watermarking.

Techniques that work in spatial domain can suffer from signal compression and hostile attacks. Frequency domain techniques are much more robust against compression and geometrical transformations than spatial domain techniques. Nevertheless, one weakness for may be spatial frequency approaches is that the human visual system is not taken into account when selecting positions to insert the watermark. Because of the invisibility constraint of a watermark, these techniques have to use signals of relatively lower power than would otherwise be possible, to avoid degrading the image quality, inevitably limiting the robustness of the watermark [3]. Proposed properties were shown that for watermarked media several requirements must be satisfied:

- Imperceptibility – the watermark should be imperceptible, not to affect the viewing experience of the image or the quality of signal.
- Undeleting – the watermark must be difficult or even impossible to remove by a hacker, at least without obviously degrading the host signal.

- Statistically undetection – A pirate should not be able to detect the watermark by comparing several water-marked signals belonging to the same author.
- Robustness – The watermark should be survived by the using of the lossy compression techniques and signal processing operations (signal enhancement, geometric image operations, noise, filtering, etc.) [4,5]

Robustness is crucial to the success of watermark embedding. To achieve an imperceptible watermarking is not difficult by minor modification of the host data. Making the watermark indestructible, however, is not a trivial problem. The process of image watermarking can be represented by the addition of a noise term that is a function of the watermark signal, *w*, and possibly of the original image, *I*. Watermarked image, *I'*, can be created in wavelet trans-form domain. When an image undergoes wavelet decomposition, its components are separated into bands of approximately equal bandwidth on a logarithmic scale much as the retina of the eye splits an image into several components. It is, therefore, expected that use of discrete wavelet transform will allow the independent processing of the resulting components much like the human eye. [4] The algorithm of embedding of digital watermark in frequency domain, in generally is shown on Figure (1). For watermark extraction is needed watermarked image and also the original image. Than the process of watermark extraction can be realized by figure (2).

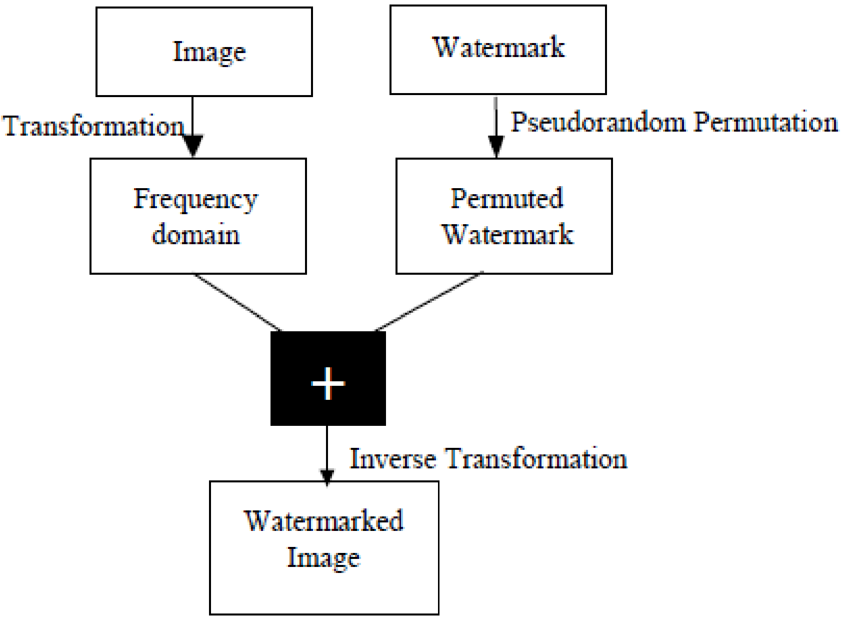

Figure (1) the process of digital watermarking in frequency domain

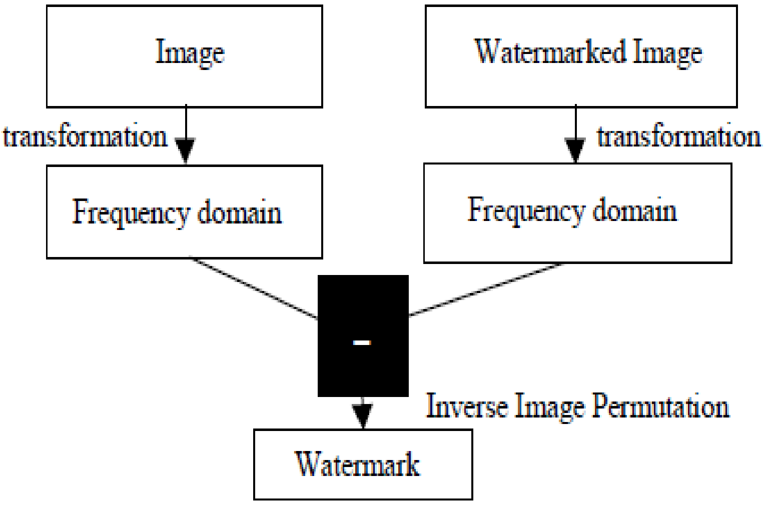

Figure (2) Process of watermark extraction

3. Watermarks and Wavelets:

Most image watermarking schemes operate either in the Discrete Cosine Transform (DCT) or the Discrete Wavelet Transform (DWT) domain. A few watermarking algorithms employ more exotic transforms such as the Fourier-Mellin Transform and the fractal transform [6]. The DWT domain is better suited for image watermarking than the DCT and other transform domains for several reasons:

1. The DWT offers excellent **space-frequency localization** of salient image features such as textures and edges. Specifically, the high-frequency content of an image corresponds to large coefficient in the detail subbands. Hence, watermark encoders operating in the wavelet domain can easily locate the high-frequency features of an image and embed most of the watermark energy there. Such embedding will result in implicit visual masking of the watermark since the Human Visual System (HSV) has a limited ability to detect high frequency signals. [6]
2. The wavelet transform's **multi-resolution representation** of images facilitates progressive transmission of image data and hierarchical decoding of nested watermarks.
3. The DWT provides **superior modeling of the HVS**. The dyadic frequency decomposition of the wavelet transform resembles the pyramid decomposition of the hypothetical Cortex Transform which models the human visual system. As a result, the DWT allows the different perceptual bands of the HVS to be excited individually. [7,8]
4. The wavelet transform is **computationally efficient**. The DWT can be computed in linear time, while the DCT has O ($n \oplus \log n$) time complexity.
5. The DWT is very **flexible**: there are infinitely many wavelet filters. The multitude of possible filters and filter bank configurations enables highly

customized processing of individual images. The flexibility in the choice of wavelet filters can also be exploited to increase the security of the watermarking schemes operating in the wavelet domain. [9]

4. The proposed Watermark Embedding Algorithm:

In this paper we embedding watermark in still image by using wavelet transform. The proposed system embeds watermark four times in subbands. The watermarking will be able to survive in spite of a high degree of compression by using the compression standard JPEG2000 attack, lowpass and highpass filter. 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 [10,11]. Therefore, embedding the watermark into the maximum coefficients of the detail subbands is difficult for the human vision system to perceive.

The watermark and password are copied in each subband (LH, HL HH), and each subband embeds watermark in it by using the following step:-

The first step stores all coefficients of a subband in array 2-D.

The array contains the value of coefficients and locations of coefficients, the location can be calculated by using the equation:

Location = $x \times width + y$ … (1)

the Width of subband

x,y mean position in two dimension array

We need to make the watermark able to survive even though a high degree of compression is imposed on the watermarking image by using the compression standard JPEG2000 attack.

One of the most important attacks to watermarking systems is the compression because it could be intentional or unintentional. The prior studies in this field adopted trial and error trends. They build a watermarking system, and then test it against compression's techniques, especially JPEG, to see if the watermark could be extracted from watermarked image after it is subjected to compression.

In this method, the process of embedding the watermark it is need to input the threshold value in the coefficients that watermark embedded in. This value represents limit to JPEG2000 compression (higher difference) that makes extraction of watermarking from image watermark.

Check the max coefficients before embedding the watermark because some of them cause error when extracting watermark.

In this method, when embedding watermark bit is (0) then embedded into the coefficient embedding, this decreases the coefficients of amount threshold value, and if the embedded watermark bit is(1) then embedded into the coefficient embedding, this increases the coefficients of amount threshold value. This work adopts trial and error trend, therefore this value is the difference between one image, and another.

Any coefficients in array return into same locations in the subband.

Then repeat these ways in three subbands (HL, LH and HH) to embed the watermark in each subband by the same steps.

After embedding the watermark message in host coefficients, then reconstruct the image by applying the inverse wavelet transform of decomposition operation.

In the end saves watermarked color image as BMP (24-bit) file format.

5. The proposed Watermark Extraction Algorithm:

To extract watermark from image, it is need to compare the original image with image watermark. In this paper we need to input the original image, watermarking text and threshold and the output watermarking text, so the extraction algorithm is shown below. Algorithm for Extraction Watermark in Wavelet Transform:

After input original image, image watermark and threshold, it is compared 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.

And then 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.

6. Experimental and Results:

In this algorithm, implements into many images, this result for one image by wavelet transform, as shown in Figure (3) the original image and Figure (4) shows image after embedded watermarking, the results are discussed as follows:

Figure (3) Original Image

Figure (4) Image Watermark

The image dimensions are 280x280, the size of image before compression is: 229.7 kb, Data Payload: 250 bit.

1. The example of implementation in wavelet method gives the results for PSNR after embedding and after using lowpass, highpass filters are shown in table (1) and Figure (5). The result of PSNR depends on threshold, when the threshold increases PSNR decreases in the same image.
2. Apply image in example for JPEG2000. The results are discussed in table (2) and Figures (6), (7). In this table, when you select threshold (1) and quality (88.0) the image size is (43.3) and compression ratio (5.30), 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 (42.2) and compression ratio (5.44) increases. This shows the watermark bit success rate is (99.0%), the solution for this case is by increasing the threshold we can see that in threshold (2), the success rate is (100%) in (87.9) quality .When increases the threshold the PSNR decreases.

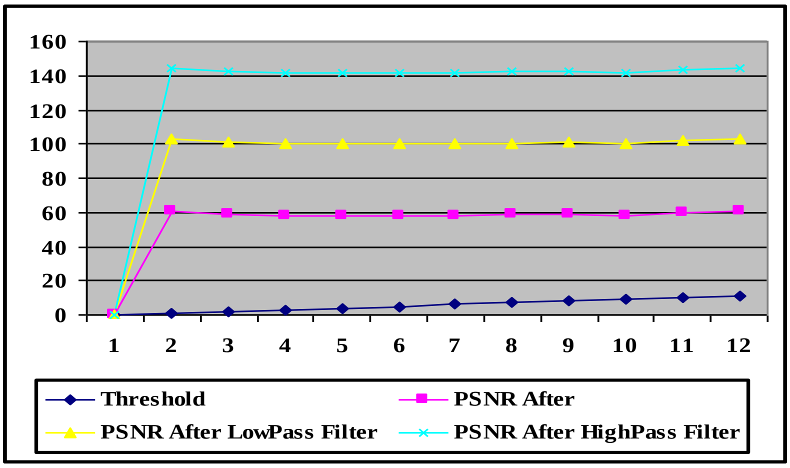

Figure (5) Relation PSNR After Embedding, Lowpass and Highpass

Table (1) PSNR for Image Watermarking in Wavelet Transform

Threshold	PSNR After Embedding	PSNR After LowPass Filter	PSNR After HighPass Filter
1	59.882	42.160	41.652
2	56.871	42.158	41.651
3	55.110	42.155	41.648
4	53.861	42.151	41.645
5	52.892	42.145	41.640
6	52.100	42.139	41.635
7	51.431	42.131	41.629
8	50.851	42.121	41.621
9	49.339	42.111	41.613
10	49.822	42.100	41.604
11	49.468	42.087	41.594

Table (2) Image Watermarking after JPEG2000 in Wavelet Transform

Threshold	Quality	Image Size	Comp. Ratio	PSNR	Success Rate
1	88.0 87.9	43.3 42.2	5.30 5.44	59.794 59.866	100% 99.0%
2	87.9 85.0 80.0	42.2 40.8 38.3	5.44 5.62 5.99	54.934 54.175 52.598	100% 100% 99.5%
3	80.0 75.0 70.0 65.0	38.3 35.9 33.6 31.0	5.98 6.39 6.83 7.40	52.031 51.390 50.499 49.812	100% 100% 100% 99.5%
4	65.0 60.0	31.3 28.8	7.33 7.97	49.638 48.895	100% 99.5%
5	60.0 55.0 50.0	28.5 26.1 23.9	8.05 8.80 9.61	48.787 48.310 48.056	100% 100% 98.0%
6	50.0	24.1	9.53	47.933	99.5%
7	50.0 45.0	24.0 21.7	9.57 10.58	47.740 47.392	100% 98.5%
8	45.0	21.6	10.63	47.110	99.5%
9	45.0	21.3	10.78	46.940	99.0%
10	45.0	21.5	10.68	46.847	99.5%
11	45.0	21.3	10.78	46.546	100%

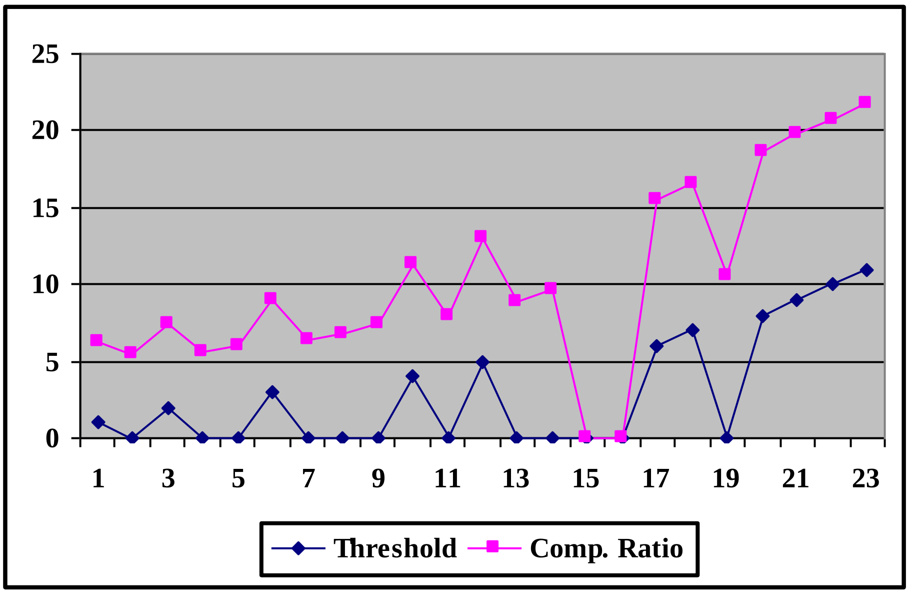

Figure (6) Relation between Threshold and Comp. Ratio

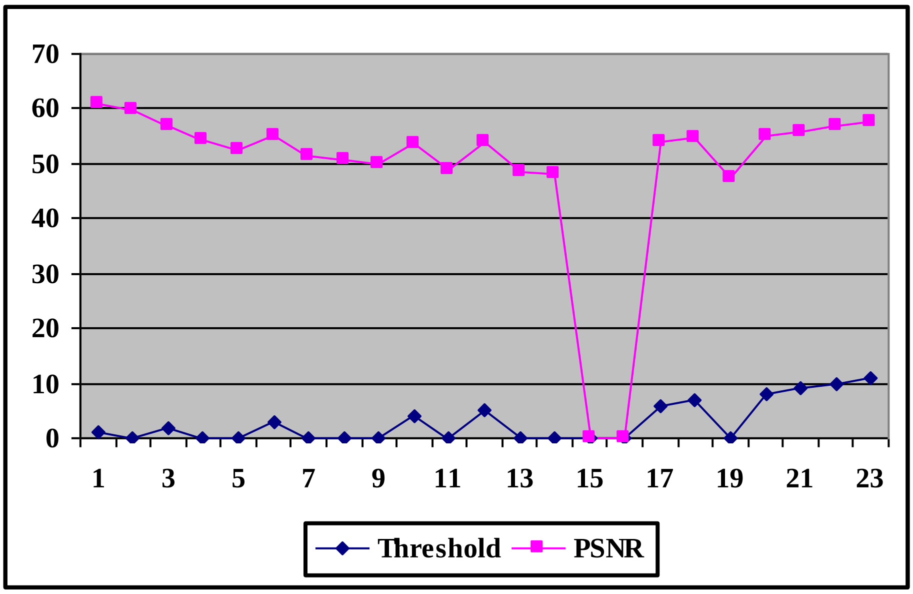

Figure (7) Relation between Threshold and PSNR

7. Conclusion

This paper emphasized on the digital watermarking provides a comprehensive evaluation algorithm that embeds and extracts the watermark information effectively. In this paper, there are number of conclusions were derived from this research:-

When the compression ratio increases the survived embedded watermark bits will decrease.

Repeating watermark four times in image increases robustness against attack (JPEG2000, lowpass and highpass filter). 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.

References

[1] Mohammed F. Al-Hunaity, Salam A. Najim and Ibrahiem M. El-Emary "**Colored Digital Image Watermarking using the Wavelet Technique** ", Department of Information Technology, Prince Abdullah Bin Ghazi Faculty of Science and Information Technology, Al-Balqa' Applied University, Jordan and Department of Computer Engineering, Faculty of Engineering, Al-Ahliyya Amman University, Amman, American Journal of Applied Sciences, 2007, Jordan.

[2] Chun-Shien Lu, " **Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property**", Institute of Information Science Academia Sinica, Taiwan, ROC, 2004.

[3] TAO, B., DICKINSON, B.**: Adaptive watermarking in the DCT domain**, IEEE Int. Conf. ASSP '97, 1997.

[4] M. ČANDÍK, E. MATÚŠ, D.LEVICKÝ, "**DIGITAL WATERMARKING IN WAVELET TRANSFORM DOMAIN**", Radioengineering Digital Vol. 10, No. 2, July 2001.

[5] Ersin Elbasi1 and Ahmet M. Eskicioglu2, “ **Naïve Bayes Classifier Based Watermark Detection in Wavelet Transform ”,** 1 The Graduate Center, The City University of New York, 365 Fifth Avenue, New York, NY 10016, 2 Department of Computer and Information Science, Brooklyn College, The City University of New York, 2900 Bedford Avenue, Brooklyn, NY 11210, 2006.

[6] Emina Torlak "**Wavelet-Based Solutions to the Digital Image Watermarking Problem**", Massachusetts Institute of Technology, 18.327 Wavelets, Filter Banks and Applications, Final Project Report, Apr 2010.

[7] Santa Agreste & Guido Andaloro, “**A new approach to pre-processing digital image for wavelet-based watermark ” ,** Journal of Computational and Applied Mathematics**,** Volume 221 , Issue 2 (November 2008), ISSN:0377-0427 .

[8] A. B. Watson, “ **The cortex transform: Rapid computation of simulated neural images**”, Computer Vision, Graphics, and Image Processing, vol. 39, no. 3, 1987, pp. 311-327.

[9] P. Meerwald and A. Uhl, “ **Watermark security via wavelet filter parametrization** ” , Proceedings of the IEEE International Conference on Image Processing, ICIP '01,Thessaloniki, Greece, vol. 3, October 2001, pp. 1027-1030.

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

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

العلامة المائية الرقمية للصور باستخدام نطاق التحويلات الموجية

م. م . روسم عبد العظيم حسن
الجامعة المستنصرية- كلية العلوم

الخلاصة:

يقدم هذا البحث خوارزمية للعلامة المائية مبنيه على أساس التحويلات الموجية (DWT) ، حيث طبقا الى خصائص الرؤية الانسانية فأن العلامة المائية تخفى في المعاملات الكبيرة لمجاميع الترددات العالية. العلامة المائية في هذه الخوارزمية قادره على مقاومة ضغط صورة JPEG2000 ويتم استخراجها باستخدام الصورة الاصلية.

تم تطبيق هذا البحث على عدد من الصور حيث أظهرت نتائج المحاكاة ان هذه الخوارزمية غير مرئية وقوية باستخدام مرشحات (lowpass وhighpass) و ضغط JPEG2000 في حمل بيانات ٢٥٠ بت حيث يكون أستخراج العلامة المائية بمعدل ٩٠-٩٥%.