IJCSC

ISSN : 0973-7391

Vol. 3, No. 1, January-June 2012, pp. 15-21

IMPLEMENTATION OF DIGITAL WATERMARKING USING VHDL

Mohammad Imroze Khan[1], Samiksha Soni[2], Bibhudendra Acharya[3], and Shrish Verma[4]

[1,2,3,4]Department of Electronics & Telecommunication, National Institute of Technology Raipur, Chhattisgarh, India
[1]E-mail: imroze786@gmail.com, [2]samiksha.soni786@gmail.com, [3]E-mail: bacharya.etc@nitrr.ac.in, [4]shrishverma@nitrr.ac.in

ABSTRACT

Digital watermarking technology is a frontier research field and it serves an important role in information security. Digital Watermarking is a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm. The basic characteristics of digital watermark are imperceptibility, security, reliability, low complexity of watermarking algorithm and security of the hiding place. According to the analysis of the definition and basic characteristics of digital watermarking technology, the system model of digital watermarking is given. The system consists of two modules which are watermark embedding module and watermark detection and extraction module. In this paper we employed the two dimension wavelet transform on the Windows platform by using VHDL program language to embed the watermark. VHDL implementation is done to save resources and for faster operation. The embedding and retrieving of watermark using this is faster than that done through high level programming languages. The experiment result shows that the digital watermark is non-perceptible; the watermark information can be extracted even if it has been attacked, and the expected effect can be achieved.

Keywords: Digital Watermarking, Wavelet, Embedding Watermark, DWT, IDWT and VHDL

1. INTRODUCTION

With the rapid development of the information technology and computer network technology, the security of digital multimedia information has become an important issue [1]. The traditional information security technology based on cryptography theory mostly has its limitations. In order to resolve the shortcomings of traditional information security technology, more and more researchers has been starting to study the digital watermarking technology because it can effectively compensate for the deficiencies of the security and protection application of traditional information security technology [2]. The watermark information can be copyright information, authentication information or controlling information so as to determine the copyright owner of the digital works, certify the authenticity and integrity of multimedia works, control copying according to the embedded control information, achieve the purpose of copyright protection [3]. Digital watermarking technology has many applications in protection, certification, distribution, anti-counterfeit of the digital media and label of the user information. It has become a very important study area in information hiding.

The rest of the paper is organized as follows: Section II explains the various watermarking technology; Section III explains the architecture details of watermarking; Section IV describes the proposed algorithm for Digital Watermarking; Section V talks about the experimentation results of the proposed algorithm; Section VI concludes the paper.

2. DIGITAL WATERMARKING TECHNOLOGY

As an emerging interdisciplinary application technology, digital watermarking involves the ideas and theories of different subject coverage, such as signal processing, cryptography, probability theory and stochastic theory, network technology, algorithm design, and other techniques.

It can embed copyright information into the multimedia data through certain algorithms [4]; the information may be author's serial number, company logo, images or text with special significance, and so on. Their function is served as copyright protection, secret communication, authenticity distinguish of data file, etc. The embedded iconic information is usually not visible or imperceptible, and it can only be detected or extracted through a number of special detectors or readers [6]. Digital watermark is closely integrated with and hided into the source data and it is becoming an inseparable part of the latter. It can be survived by experiencing some operation or attacks.

A. Classification of Digital Watermarking

(1) Digital watermarking can be divided into robust watermarking and fragile watermarking according to its characteristic: Robust watermarking is mainly used to sign copyright information of the digital

works[5], the embedded watermark can resist the common edit processing, image processing and lossy compression, the watermark is not destroyed after some attack and can still be detected to provide certification. Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

(2) ***Digital watermarking can be divided into image watermarking, video watermarking, audio watermarking, and text watermarking and graphic watermarking based on the attached media [7]:*** Image watermarking refers to adding watermark in still image. Video watermarking adds digital watermark in the video stream to control video applications. Text watermarking means adding watermark to PDF, DOC and other text file to prevent changes of text. Graphic watermarking is embedding watermark to two-dimensional or three-dimensional computer-generated graphics to indicate the copyright.

(3) ***Digital watermarking can be divided into visual watermarking and blind watermarking according to the detection process:*** Visual watermarking needs the original data in the testing course, it has stronger robustness, but its application is limited. Blind watermarking does not need original data, which has wide application field, but requires a higher watermark technology[8].

(4) ***Digital watermarking can be divided into copyright protection watermarking, tampering tip watermarking, note anti-counterfeiting watermarking, and anonymous mark watermarking based on its purpose:*** Copyright protection watermarking means if the owners want others to see the mark of the image watermark [9], then the watermark can be seen after adding the watermark to the image, and the watermark still exists even if it is attacked. Tampering tip watermarking protects the integrity of the image content[10], labels the modified content and resists the usual lossy compression formats. Note anti counterfeiting watermarking is added to the building process of the paper notes and can be detected after printing, scanning, and other processes. Anonymous mark watermarking can hide important annotation of confidential data and restrict the illegal users to get confidential data.

B. Basic Characteristic of Digital Watermarking

The basic requirement of digital watermarking is closely related to its purpose of applications, different application has different demand. In general, the characteristics of digital watermarking are as follows [3]:

(1) ***Robustness:*** Robustness refers to that the watermark embedded in data has the ability of surviving after a variety of processing operations and attacks. Then, the watermark must be robust for general signal processing operation, geometric transformation and malicious attack. The watermark for copyright protection does need strongest robustness and can resist malicious attacks, while fragile watermarking do not need resist malicious attacks.

(2) ***Non-perceptibility:*** Watermark can not be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits.

(3) ***Verifiability:*** Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.

(4) ***Security:*** Watermark information owns the unique correct sign to identify, only the authorized users can legally detect, extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection.

3. ARCHITECTURE OF DIGITAL WATERMARKING

A. System Model of Digital Watermarking

The process of digital watermarking embeds the special information which stands for the particular identity of the owner of the copyright by some sort of algorithm to multimedia data [11]. We can extract the watermark, verify the ownership of the copyright and ensure the legitimate rights of the copyright owners though the appropriate algorithms. A complete digital watermarking system is composed of two basic modules: watermark embedding module and watermark detection and extraction module. Watermark embedding module is responsible for adding the watermark signal to the original data. The watermark can be any form of data, such as numeric, text, image, and so on. The watermark embedding module is as shown in Figure 1.

Figure 1: Watermark Embedding Module

Watermark detection and extraction module is used to determine whether the data contains specified

watermark or the watermark can be extracted. The module input may be image, watermark or original image the output is a watermark or some kind of credibility value. It indicates the possibility of the data having a given watermark. The watermark embedding module is as shown in Figure 2.

Figure 2: Detection and Extraction Module of Watermark

B. Main Algorithms of Digital Watermarking

In recent years, the study of digital watermarking technology makes great progress. There are a lot of good algorithms which can be divided into spatial domain algorithm and transform domain algorithm[12].

(1) Spatial domain: Spatial domain digital watermarking algorithms directly load the raw data into the original image. The classification of spatial domain algorithm is as follows:

- *Least significant bit algorithm:* The algorithm embeds the information with the form of the least significant bits selected randomly which can ensure the embedded watermark is invisible. But the algorithm has poor robustness, and watermark information can easily be destroyed by filtering, image quantization, and geometric distortion.
- *Patchwork algorithm:* Based on the statistics, t he algorithm uses the statistical characteristics of pixels to embed the information into the brightness values of pixel. It can resist lossy compression coding and malicious attacks. However, the amount of embedded information is limited, in order to embed more watermark information; we can segment the image, and then implement the embedding operation each image block.
- *Texture mapping coding method:* It hides the watermark in the texture part of the original image. The algorithm has strong resistance ability to attacks for a variety of deformation, but only suitable for areas with a large number of arbitrary texture images, and can not be done automatically.

(2) ***Transform domain digital watermarking algorithm:*** Transform domain algorithm is a method of hiding data similar to spread-spectrum communication technology. Firstly, it does a kind of orthogonal transformation for image, and then embed watermark information in the transform domain of image, finally use the inverse transform to recover the image in spatial domain, the detection and extraction of the watermark are also realized in transform domain. There are several common used transform domain methods, such as discrete Fourier transform (DFT), discrete cosine transform (DCT)[14], discrete wavelet transform (DWT)[15], and so on. As a classical mathematical transformation method, DWT does a very important role in image compression, coding and other applications. Wavelet transform decomposes an image into a set of band limited components which can be reassembled to reconstruct the original image without error. The fact that wavelet-based data structure has been adopted in the established image coding standard JPEG2000 encouraged extensive watermarking research in wavelet transform. As pointed out in [7], wavelet-based watermarking methods exploit the frequency information and spatial information of the transformed data in multiple resolutions to gain robustness. The advantages of wavelet transform compared to discrete cosine transform (DCT) and discrete Fourier transform (DFT) were mentioned in [13].

- *Wavelet transform[16]:* Wavelets are mathematical functions that satisfy certain criteria, like a zero mean, and are used for analyzing and representing signals or other functions. A set of dilations and translations $\Psi\ \tau, s(t)$ of a chosen mother wavelet $\Psi\ (t)$ is used for analysis of a signal. This set can be compared with basic functions of Fourier Transform and is defined as equation (1-2):

$$\Psi\tau,s(t) = \frac{1}{\sqrt{s}}\ \Psi(t-\tau/s) \qquad (1)$$

$$C\tau,s = \int_{-\infty}^{\infty} f(t)\ \Psi\tau,s(t)\ d(t) \qquad (2)$$

  The inverse transform, conversely, uses the computed wavelet coefficients and superimposes them in order to calculate the original data set.

- *Discrete Wavelet Transform:* In Discrete Wavelet Transform (DWT) the scale and translate parameters are chosen such that the resulting wavelet set forms an orthogonal set, i.e. the inner product of the individual wavelets . To this end, dilation factors are chosen to be powers of 2. For Discrete Wavelet Transform, the set of dilation and translation of the mother wavelet is defined as in equation (3):

$$Y_{j,k}(t) = 2^{\,j/2}\ \Psi(2^{-j}t-k) \qquad (3)$$

Here j is the scaling factor and k is the translation factor. It is obvious that the dilation factor is a power of 2. Forward and inverse transforms are then calculated using the following equations (4-5):

$$C_{j,s} = \int_{-\infty}^{\infty} f(t)\, \Psi_{j,k}(t)\, d(t) \quad (4)$$

$$f(t) = \sum_{j,k} C_{j,s}\, \Psi_{j,k}(t) \quad (5)$$

Wavelet Transform has several advantages. Here we list a number of these in regard to image compression and processing.

(*i*) One of the main features of Wavelet Transform, which is important for data compression and image processing applications, is its good decorrelating behaviour.

(*ii*) Wavelets are localized in both the space (time) and scale (frequency) domains. Hence they can easily detect local features in a signal.

(*iii*) Wavelets are based on multi-resolution analysis. Wavelet decomposition allows analyzing a signal at different resolution levels (scales).

(*iv*) Wavelets are smooth, which can be characterized by their number of vanishing moments. The higher the number of vanishing moments, the better smooth signals can be approximated with the wavelet basis.

4. PROPOSED METHOD

A. Encoder Design

The encoder performs the following functions as shown in Figure 3.

(*i*) The separation of the bits of the image into high frequency and low frequency components.

(*ii*) Embedding the bits of the watermark into the high frequency components.

(*iii*) Combining the watermarked high frequency component and the low frequency component to get the watermarked image.

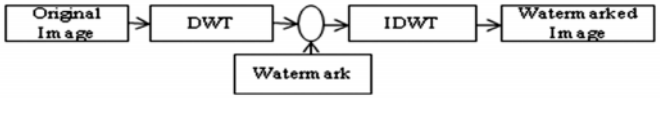


Figure 3: Encoder Block

DWT block : This block separate out high frequency and low frequency components form the original image pixel so that watermark can be embedded in it. This block contains registers, adders, buffers and 2's compliment block as shown in Figure 4.

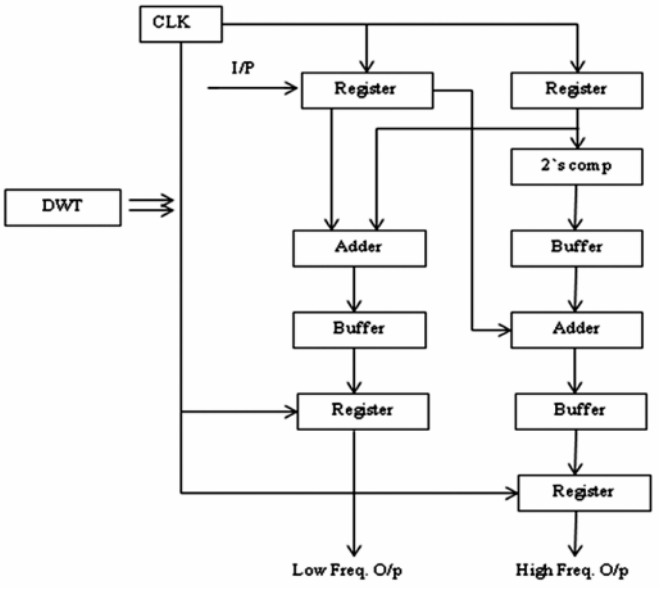


Figure 4: Internal Structure of DWT Block

I/P: we are giving 16 bits (which represent each Pixel of the image) as input to the DWT block.

Register: We have designed a 16 bit register for storing the previous bits at various stages in the DWT block. Here we have designed the register using D flip flop as component in structural modeling. We are storing a 16 bit input in the register and getting a 16 bit output. We have used 4 register blocks in the DWT block.

Adder: We have designed a 16 bit adder. Here we have first designed a one bit adder in structural modeling. Then we have designed a 16 bit adder by port mapping using structural modeling. In these case we have used one bit adder as component while designing a 16 bit adder. Here we have used 2 adder blocks in DWT block. Each adder has two 16 bit inputs and 16 bit output

Two's compliment: Here we have designed a 16 bit 2's compliment. In this case we have first designed a 16 bit adder using one bit adder in structural modeling, same as we have designed a 16 bit adder above. Here we have defined Cin = '1' in the initial stage while in case of adder we have considered it as '0'. Here the input is a 16 bit and the output is also a 16 bit.

Buffer: Here we have designed a 16 bit buffer. We have designed it using behavioral modeling. We have used 3 buffers in DWT block. Each buffer has 16 bit input and a 16 bit output.

Clock: Here the clock is given to all the registers in the DWT block. As the clock is given only to registers we have a certain delay here initially i.e. for two clock pulses till the pixels entered in both the registers. Afterwards it works normally.

High frequency output: The high frequency output is the output where the bits of original image do not change frequently. Therefore the watermark bits are embedded in the high frequency output.

Low frequency output: The low frequency output is the output where the bits of original image change frequently.

IDWT block: This block regenerates the original image with watermark in it i.e. watermarked image. Here we have used register, buffer, adder and right shift by one register block as shown in Figure 5

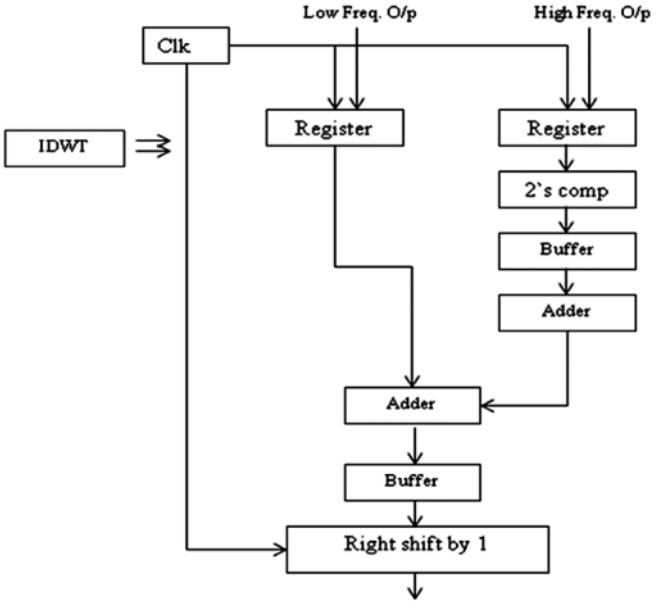


Figure 5: Internal Structure of IDWT Block

Right shift by 1 block: Here we have design a 16 bit right shift register we have designed it by using behavioral modeling. This block is required to get the desired output

Clock: Here the clock is given to all the registers in the IDWT block and right shift by1 block

B. Decoder Design

The decoder performs the following functions as shown in Figure 6.

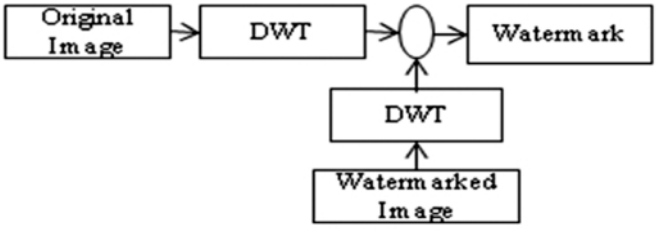


Figure 6: Decoder Block

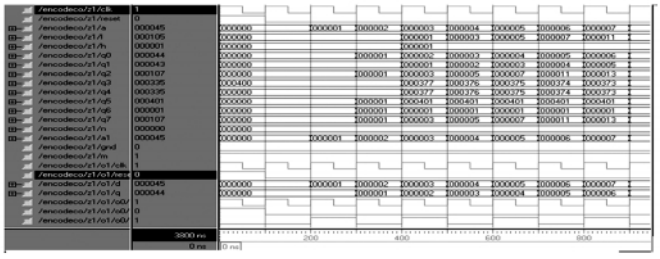
(*i*) Watermarked image is passed through DWT block to get watermarked high frequency and watermarked low frequency component.

(*ii*) Original image is also passed through DWT block to get high frequency and low frequency component.

(*iii*) Watermarked high frequency component and high frequency component of original image are XORed to get watermark bits.

5. RESULT

Discrete Wavelet Transform output waveform



clk: It is the clock given to the various register blocks in DHWT.

reset: It is the reset given to the various blocks in DWT.

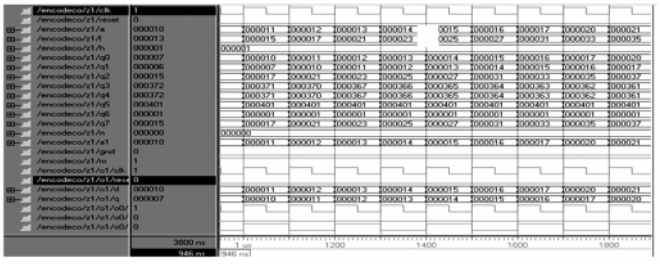
a: It is the input(pixels of the original image) given to the first register in the DWT.

l: It is the low frequency output of the DWT.

h: It is high frequency output of the DWT.

q0: It is the signal defined as the output of first register in DWT.

q1: It is the signal defined as the output of second register in DWT.



q2: It is the signal defined as the output of the first adder in DWT.

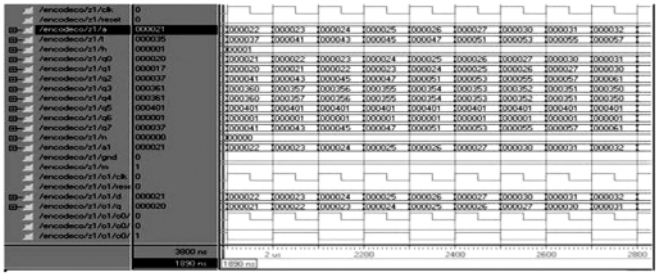
q3: It is the signal defined as the output of the 2's compliment in DWT.

q4: It is the signal defined as the output of the buffer in DWT.

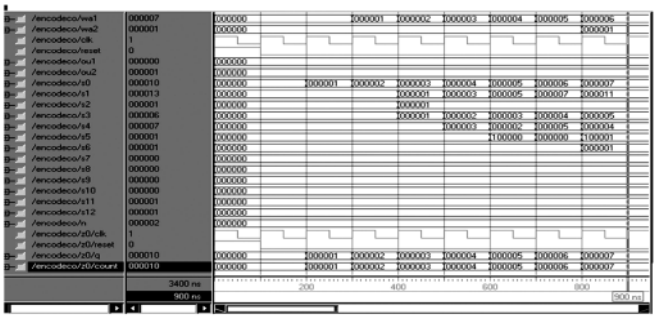
q5: It is the signal defined as the output of the second adder in the DWT.

q6: It is the signal defined as the high frequency output of DWT.

q7: It is the signal defined as the low frequency output of DWT.



n,a1,gnd,m: They are the various signals defined in the architecture of DWT,that are used in the various blocks of the DWT like adder,register,2's compliment



output waveform:

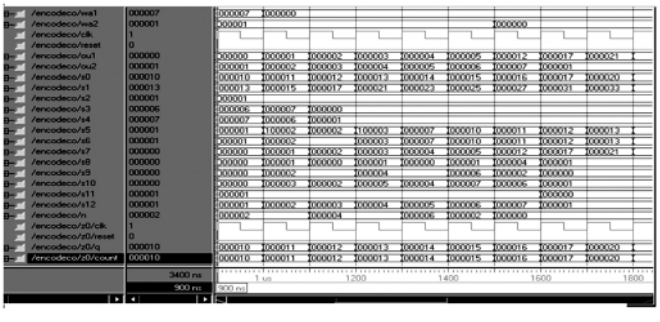
wa1: It is the watermark inserted at the input i.e. in the (encoder) high frequency contents of the original image.

wa2: It is the watermark inserted at the output i.e. in the (decoder) high frequency contents of the watermarked image.

clk: It is the clock given to the various register blocks in DWT.

reset: It is the reset given to the various blocks in DWT.

ou1: It is the low frequency contents of the watermarked image.



ou2: It is the watermark inserted at the input (encoder) high frequency contents of the original image.

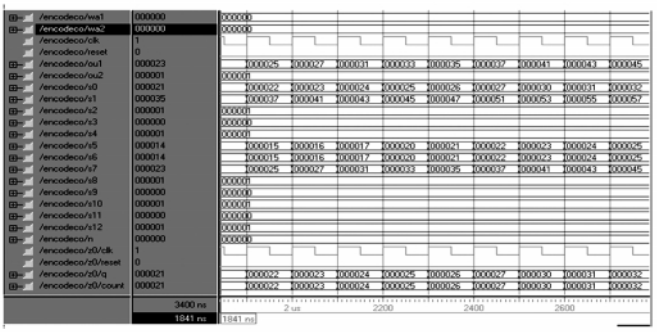
s0: It is the input (pixels of the original image) given to the DWT.

s1: It is the signal defined as the low frequency contents of the DWT (original image).

s2: It is the signal defined as the high frequency contents of the DHWT (original image).

s3: It is the signal defined as the watermark inserted at the input i.e. in the (encoder) high frequency contents of the original image.

s4: It is the signal defined as the high frequency contents of the watermarked image. s5, s6: It is the signal defined as the output of the IDHWT (watermarked image).



s7: It is the signal defined as the low frequency contents of the DWT

s8: It is the signal defined as the high frequency contents of the DWT (watermarked image).

s9: It is the signal defined as the watermark/high frequency contents of the original image.

s10, s11: It is the signal defined in the architecture of decoder.

s12: It is the signal defined as the output (ou2).

6. CONCLUSION

Digital watermarking holds significant promise as one of the keys to protecting proprietary digital content in the coming years. At its heart is the concept of embedding information inside a digital object such that the embedded information is inseparably bound to the object and the embedded information describes who may legally use and/or distribute the object, as well as who legally owns the object.

We have successfully simulated digital watermarking using Discrete Wavelet Transform in VHDL. This can be implemented on a FPGA / CPLD board and converted into a chip. As the explanations above show DWT is a better method to implement digital watermarking than FFT, SVD etc.

We have simulated this method for 256*256 Bitmap grey scale image. The next step would be embedding watermarks into 24 bit color images.

REFERENCES

[1] S. R. Subramanya and BYung. K. Yi. "Digital Rights Management", *IEEE Potentials*, March-April 2006, **25,** Issue 2, pp. 31-34.

[2] Piyali Mandal, Ashish Thakral, Shekhar Verma, "Watermark Based Digital Rights Management", *ITCC* (1) 2005, pp. 74-78.

[3] Cayre F, Fontaine C, Furon T. Watermarking Security: Theory and Practice". *IEEE Transactions on Signal Processing*, 2005, **53** (10) : pp. 3976-3987.

[4] Frank Hartung and Friedhelm Ramme, "Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications", *IEEE Communications Magazine*, Nov 2000, **38,** No. 11, pp. 78-84.

[5] T. Dimitrios, N. Spiridon, D. Lambros. "Applying Robust Multibit Watermarks to Digital Images". *Journal of Computational and Applied Mathematics*, 2009, 227 (2009): pp. 213-220.

[6] Fleet D.J., "Embedding Invisible Information in Color Images". *Proc. of ICIP*, 1997, (1) : pp. 532-535.

[7] Cox I.J., Killian J , Leighton T , et al. "Secure Spread Spectrum Watermarking for Images", Audio and Video. *Proc. of IEEE ICIP,* Lausane, Switzerland, 1996, (3) : pp. 243-246.

[8] Irene G. Karybali, Efficient Spatial Image Watermarking via New Perceptual Masking and Blind Detection Scheme IEEE Transactions on Information Forensics and Security.

[9] G. Voyatzis, I. Pitas. "Protecting Digital Image Copyrights A Framework", *IEEE Transactions on Computer Graphics and Applications*, 1999, 19(1): pp. 18-24.

[10] Ingemar J. Cox, J. P. Linnartz, "Some General Methods for Tampering with Watermarks", *IEEE Journal on Selected Areas in Communication*, 1998, **16**(4): pp. 587-593.

[11] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques", *Proc. IEEE*, 1999, pp. 1079 - 1107.

[12] Digital Watermark Bender, Gruhl, Morimoto, and Lu (1996), "Techniques for Data Hiding", *IBM Systems Journal*, **35,** pp. 313-336

[13] W. N. Cheung, "Digital Image Watermarking in Spatial and Transform Domains".

[14] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-Based Watermark Recovering Without Resorting to the Uncorrupted Original Image", *In Proc. IEEE Int. Conf. Image Processing* (*ICIP* 1997), 1997, pp. 520-523.

[15] Image Compression Devore, Jawerth, and Lucier (1992) Image Compression Through Wavelet Transform Coding, IEEE Trans. Inform. Theory, pp. 719-746 Amara Grapes, "An Introduction to Wavelets". *IEEE Computational Science and Engineering*, Summer 1995, **2,** No. 2, Published by the IEEE Computer Society.

[16] Xiao-wei Zhang, Lin-lin Zhao, Zhi-juan Weng. "A Wavelet-Based Robust Watermarking Algorithm of High Credibility[J]". *IEEE Trans. Proceedings of International Conference on Wavelet Analysis and Pattern Recognition*, 2009, pp. 298-302.