Iraqi Journal of Statistical Science (10) 2006
P.P. [19-37]

A NEW WAVELET-BASED WATERMARKING ALGORITHM

Nidhal H. Alassady* **Dujan B.Taha****

ABSTRACT

Digital watermarks have recently emerged as a possible solution for protecting the copyright of digital materials. The use of wavelets in image coding has increased significantly over the years, mainly due to the superior properties of wavelets compared with the traditional transforms like the DCT.

In this paper a new wavelet-based watermarking algorithm is designed and implemented using the characteristics of an image and the human visual system HVS for invisibility and robustness. For experimental results, we have considered different attacks: JPEG compression, geometric distortions and noising. The results show the good performance of the new proposed method.

الملخص

تعدّ العلامة المائية من الحلول الممكنة لحماية حقوق الملكية للبيانات الرقمية. إن استخدام تحويل المويجة في ترميز الصور قد ازداد بوضوح خلال السنوات الأخيرة بسبب خواصه المثالية مقارنة مع التحويلات التقليدية الأخرى مثل تحويل الجيب تمام المتقطع.

*Prof. / College of Computers and Mathematics Sciences/Dept. of Software Engineering

**Lecturer/ College of Computers and Mathematics Sciences/ Dept. of Software Engineering.

Received: 29/ 8 /2006 Accepted: 3/ 10 / 2006

تم في هذا البحث تصميم وتنفيذ خوارزمية جديدة للعلامة المائية بالاعتماد على تحويل المويجة وباستخدام خصائص الصورة ونظام الرؤية البشري للحصول على علامة مائية غير مرئية وقوية. ولغرض الحصول على النتائج العملية التي أظهرت الأداء الجيد للطريقة الجديدة، استخدمت مختلف أنواع الهجمات مثل كبس JPEG ، التشوهات الهندسية والضوضاء.

1. Introduction

Digital watermarking has recently become a popular research area due to the proliferation of digital data (image, audio, or video) in the Internet age and the need to find a way to protect the copyright of these materials.[Fu,1998][Loo,2002]

Digital watermark is a code that is embedded inside some innocent-looking cover data. Typically, this information is required to be robust against intentional removal by malicious parties. In contrast to cryptography, where the existence but not the meaning of the information is known, watermarking aims to hide entirely the existence of information.[Karzenbeisser,2000]

Different watermarking applications have different requirements. Some of these applications are watermarking for Copyright Protection, watermarking for Copy Protection, Fingerprinting for Pirate Tracing and Watermarking for Authentication.

An effective watermark should have several properties whose importance varies depending on the application area. These properties are described below:

Robustness: Ideally a robust watermarking scheme should resist any form of malicious distortion which does not render the image useless. Some attacks will be more important than others depending on a particular application and the media we are working in(image, audio or video)[Cox,2000]. For example, the method should resilient to generalized geometrical transformations like rotation and scaling, JPEG compression and noise.

Imperceptibility: To preserve the quality of the marked document, the watermark should not be noticeably distorting the original document. Ideally, the original and marked documents should be perceptually identical [Suk,1999].

Security: Unauthorized parties should not be able to read or alter the watermark. Security should be assured for most watermarking applications such as copyright protection. Sometimes, a secret key has to be used for the embedding and extraction processes.

Watermark Recovery with or without Original Data: In some applications such as video watermarking applications, it may be impractical to use the original data in the recovery process due to the large amount of data that would have to be processed. However in many other applications, original data are used to recover or verify the watermark.

2.The Wavelet Transform

The wavelet transform has been extensively studied in the last decade. Many applications, such as compression, detection, and communication of wavelet transform have been found and there are many tutorial books and papers about this topic [Mallat,1999][Pinsky,2000][Lakshmanan,2000].

The foundation of the Discrete Wavelet Transform (DWT) goes back to 1976 when Croiser, Esteban, and Galand derived a technique to decompose discrete time signals. Crochiere, Weber, and Flanagan did a similar work on the coding of speech signals in the same way. They named their analysis scheme as subband coding. In 1983, Burt named it pyramidal coding which is also known as multiresolution analysis [Polikar,2002].

The basic idea of the DWT for a one dimensional signal is as follows. A signal is split into two parts, usually high frequencies and low frequencies. The edge components of the signal are largely confined in the high frequency part. The low frequency part is split again into two parts of high and low frequency. This process is continued until the signal has been entirely decomposed or stopped before by the application at hand. For compression and watermarking application, generally

no more than five decomposition steps are computed. Furthermore, from the DWT coefficients, the original signal can be reconstructed. The reconstruction process is called the inverse DWT (IDWT).

The DWT and IDWT for a two dimensional image *F(m,n)* can be similarly defined by implementing the one dimensional DWT and IDWT for each dimension *m* and *n* separately as shown in figure (1).

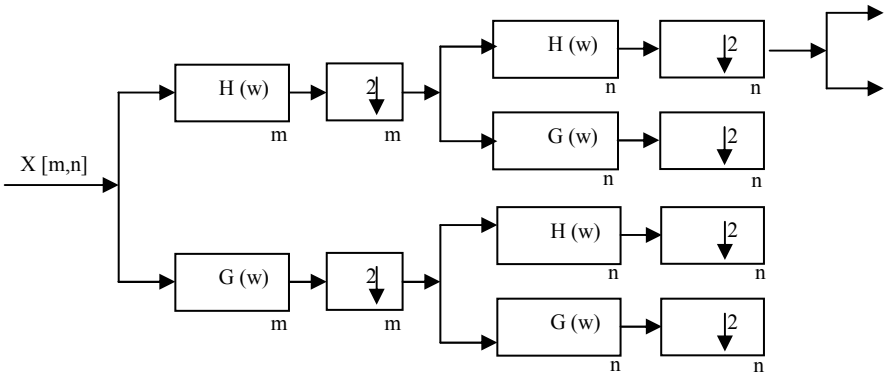


Figure 1: DWT for two dimensional images

3. The Proposed Algorithm

A digital watermarking algorithm is proposed using the characteristics of an image and the human visual system HVS for invisibility and robustness. The binary watermark is modulated before embedding in the perceptually significant wavelet coefficients.

The watermark is embedded into the selected coefficients, using different scale factors according to the level of decomposition.

3.1 Watermark Modulation

A binary sequence of watermark bits has to be embedded into the host image. A logo watermark is used as a perceptual meaningful watermark. The binary sequence {-1,1} of watermark bits has to be embedded into the host image.This sequence is spreaded with a factor to obtain the spread sequence. The purpose of spreading is to improve the robustness by adding redundancy to the embedded bits.

Next, this redundant sequence is modulated by a binary pseudo-noise sequence.

P_i , $P_i \in \{-1,1\}$; i =1, 2, …, M (1)

M denotes length of the watermark bit sequence times the spreading factor. Again, since different adaptive scaling factors are used, the step of watermark amplification is postponed to the embedding step.

3.2 Wavelet-based Watermark Embedding Process

The block diagram of the embedding process is shown in Figure (2).The original image is decomposed with a three-level DWT using Haar filter. The result of decomposition is ten frequency subbands.

Modulated watermark bits are embedded into the perceptual significant coefficients and the IDWT is applied to produce the watermarked image.

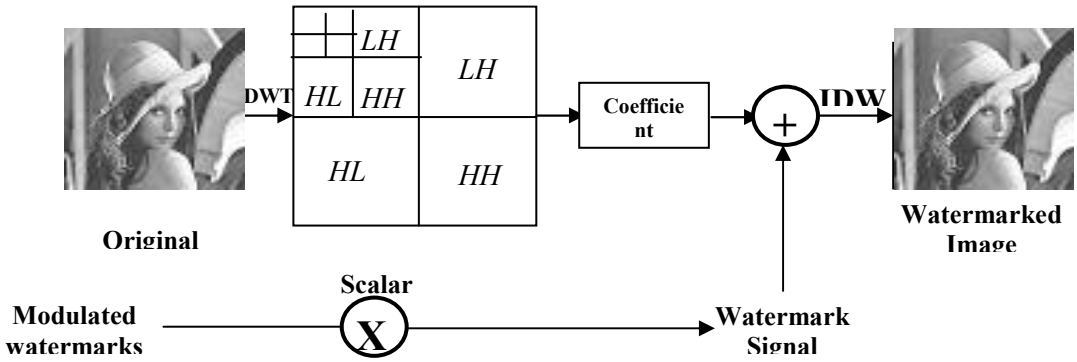


Figure 2: Watermark embedding process

3.2.1 Selection of Perceptual Significant Coefficients

The base band (approximation band or lowest band) of the wavelet-decomposed image includes most of the energy from the original image. Therefore, it has a crucial effect on the image quality.

On the other hand, base band coefficients are not removed or modified by lossy compression and other common signal processing. Therefore, a portion of this band is selected and includes its highest coefficients.

The highest wavelet coefficients on the first two levels (HH_1,HH_2) as well as those on the middle frequency bands on the lowest level (LH_1,HL_2) are excluded in the proposed algorithm because these coefficients can be easily eliminated and modified by lossy compression and other signal processing.

The steps involved in selection of coefficient of each subband are:

1. Calculating the energy of each selected subband where the energy of a subband E_s is defined by [Meerwald,2001].

$$E_s = \frac{1}{M.N} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(m,n)^2 \qquad (2)$$

where M, N denote the size of the subband.

2. The number of watermark bits No_b in each of the detailed subband is proportional to the energy of the subband.

$$No_b = \frac{bandenergy}{totalenergy} * numberofbits \qquad (3)$$

3. Coefficients of each subband are sorted. Watermark bits are embedded in the highest coefficients.

3.2.2 Selection of Adaptive Scalars

The proposed method uses an appropriate value of scale factor α for each subband according to DWT decomposition characteristics.

The mean of the wavelet coefficients is reduced by a half with each descending level and the values of wavelet coefficients for the approximation subband (LL_3) are relatively larger than other subbands in the same decomposition level. This adaptive scale factor improves the performance of both robustness and invisibility.

To the selected coefficients, the watermark is embedded using equation (4).

$$V_i' = V_i + \alpha\, a_i \qquad (4)$$

Where V_i is the selected wavelet coefficients and a_i is the modulated watermark vector.

3.2.3 Watermark Extraction Process

The block diagram of the extraction process is shown in Figure (3).

The original image and the possibly altered watermarked image are decomposed to three levels DWT.

The same coefficients used in the embedded process are selected and the original image coefficients are subtracted from the watermarked image coefficients to remove the major components of the image itself. The result is then demodulated with the pseudo-noise signal P_i that is the same as the one used for embedding.

Demodulation is followed by a summation over a window of length equal to the chip-rate, and thresholding which yields the watermark bits a_i.

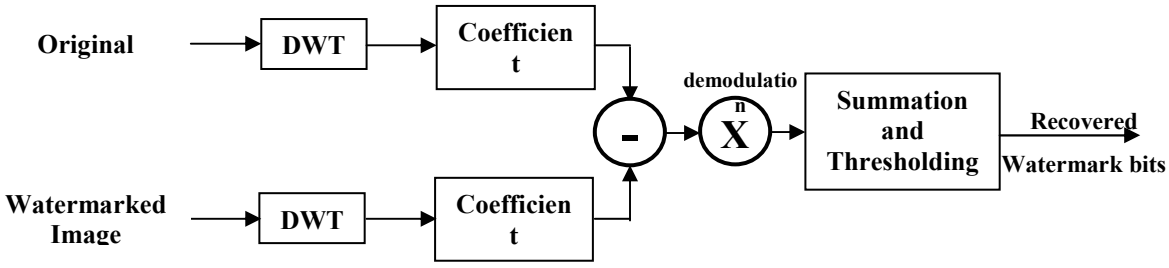


Figure 3: Watermark extraction process

4. Experimental Results

In order to evaluate the proposed algorithm, standard Lena image with 512×512 pixels and 256 grey levels is used as the host image.

A 64×64 binary logo shown in Figure (4), is used as a perceptual meaningful watermark in the experiments.

Experimental results show the invisibility of the watermark and its high robustness against different attacks.

The watermarked version of Lena image is shown in Figure (5) with PSNR = 41.481 dB.

In fact, experimental results show that the proposed algorithm is very robust to JPEG compression even when low quality parameter is used.

The watermark can be distinguished clearly, even when the watermarked image is degraded due to the high compression ratio. Figure (6) shows a JPEG compressed version of watermarked image with 25% quality parameter.

Figure 4: Logo used as a watermark

Figure 5: New watermarked image

Extracted watermarks with different quality parameters, namely 100%, 75%, 50%, 25% with the correlation 1, 0.95, 0.85 and

0.58 respectively are shown in Figure (7). Watermark extracted from 25% quality compressed watermarked image can be easily distinguished as Figure (8) demonstrates. For low pass filtering, a 3×3 averaging filter with coefficients of 1/9 is used. A typical example of the watermarked image under low pass filtering is shown in Figure (9) and the extracted logo is shown in Figure (10). The relative correlation is 0.56 and Figure (11) shows that the detection is very well above random.

A 3×3 median filter is used for medium filtering attack. The detection score is 0.74. Figure (12) shows the watermarked image under this attack. Extract watermark and detection score are shown in Figures (13) and (14) respectively.

Figure (15) shows a cropping version of the watermarked image in which only the central quarter of the image remains.

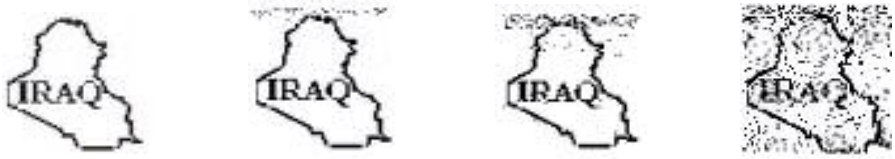
The detected logo watermark is shown in Figure (16) with the correlation 0.42 as shown in Figure (17).

The rotated watermarked image by –17° using bilinear interpolation is shown in Figure (18).

Extracted logo is shown in Figure (19) with 0.6 correlation and detection score presented in Figure (20). The watermarked image is 50% scaled down using bilinear interpolation method. Figures (21)-(23) show the scaled watermarked image, the extracted watermark with 0.47 correlation, and the detection score respectively.

For noise attack, Salt and papper noise is added to the watermarked image with 0.02 noise density as Figure (24) shows. The extracted watermark with 0.71 correlation and its detection score are shown in Figures (25) and (26) respectively.

Figure 6: New watermarked image under JPEG attack



Quality = 100% **Quality = 75%** **Quality = 50%** **Quality = 25%**

Figure 7: Decoded watermarks under JPEG attack

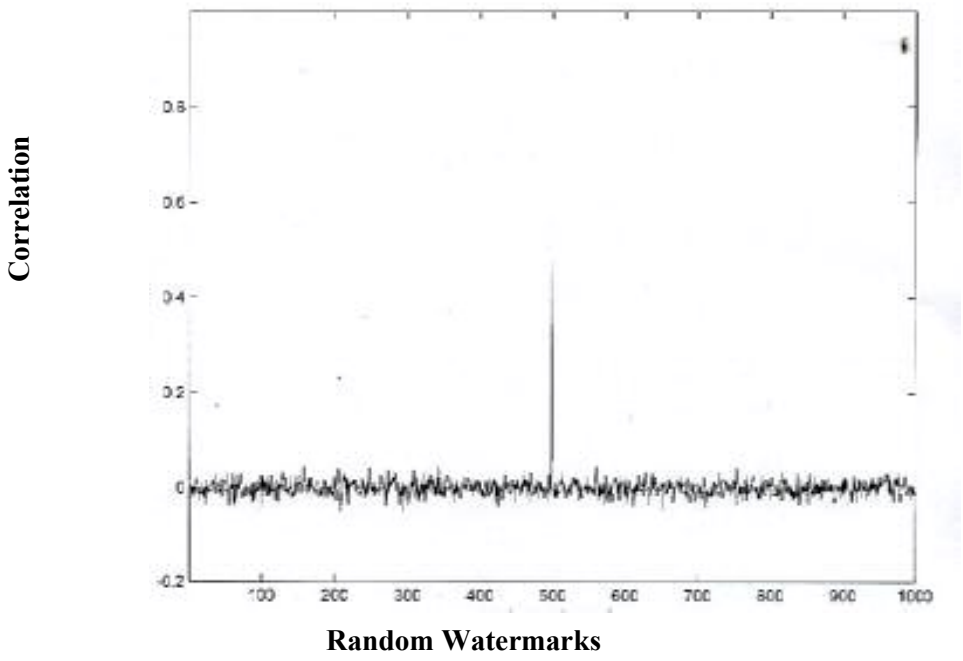


Figure 8: Random watermark detection results under JPEG attack

Figure 9: New watermarked image under LPF attack

Figure 10: Decoded watermark under LPF attack

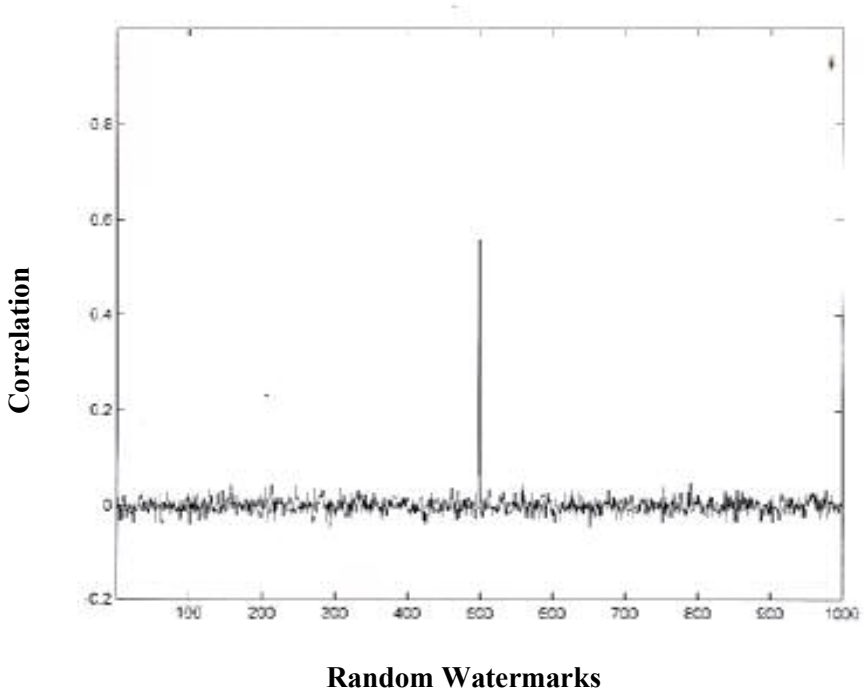


Figure 11: Random watermark detection results under LPF attack

Figure 12: New watermarked image under median filtering attack

Figure 13: Decoded watermark under median filtering attack

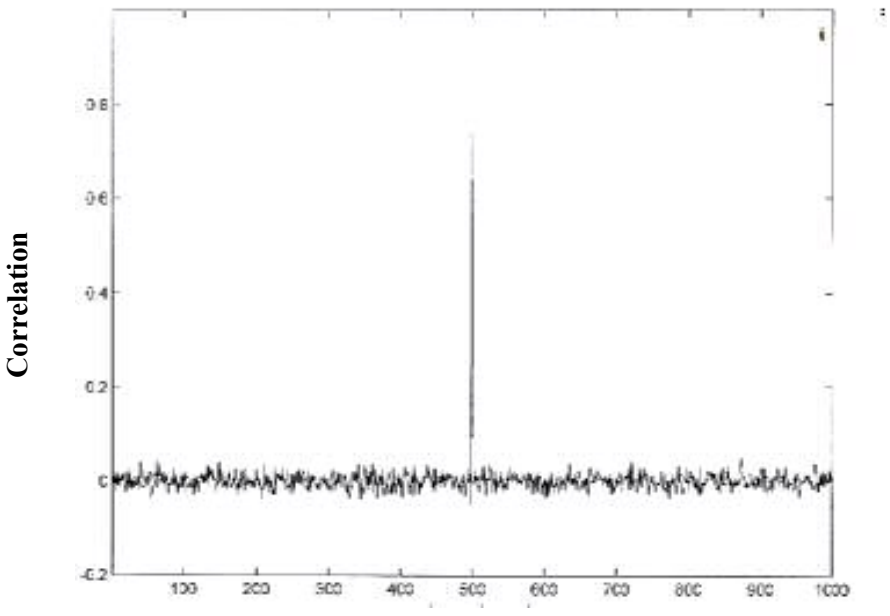


Figure 14: Random watermark detection results under median filtering attack

Figure 15: New watermarked image under cropping attack

Figure 16: Decoded watermark under cropping attack

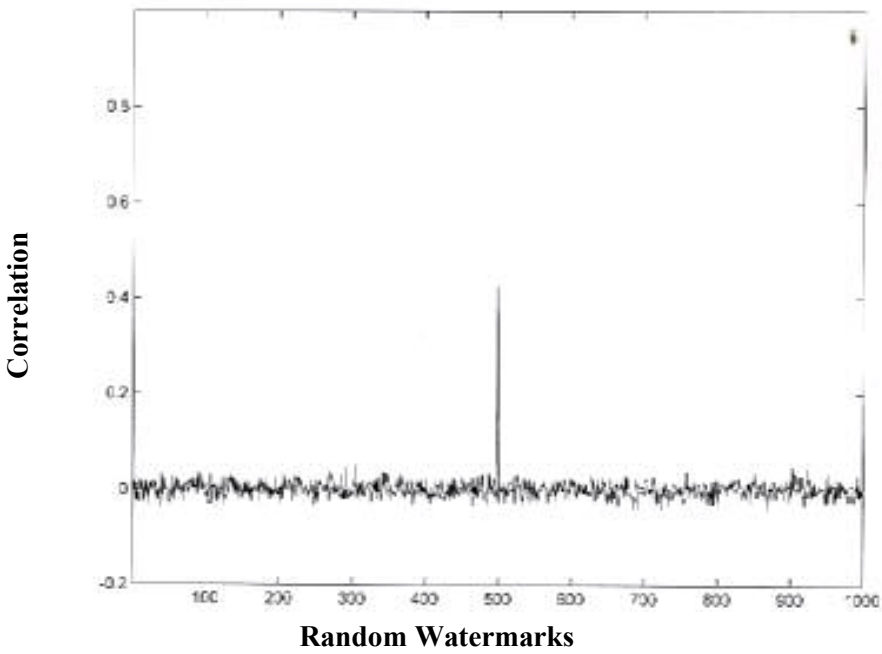


Figure 17: Random watermark detection results under cropping attack

Figure 18: New watermarked image under rotation attack

Figure 19: Decoded watermark under rotation attack

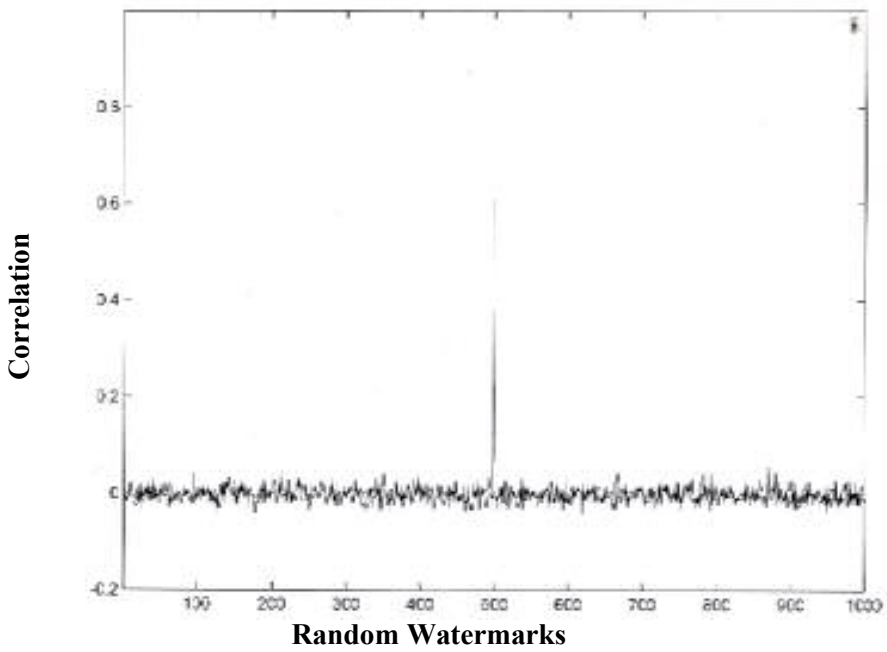


Figure 20: Random watermark detection results under rotation attack

Figure 21: New watermarked image under scaling down attack

Figure 22: Decoded watermark under scaling down attack

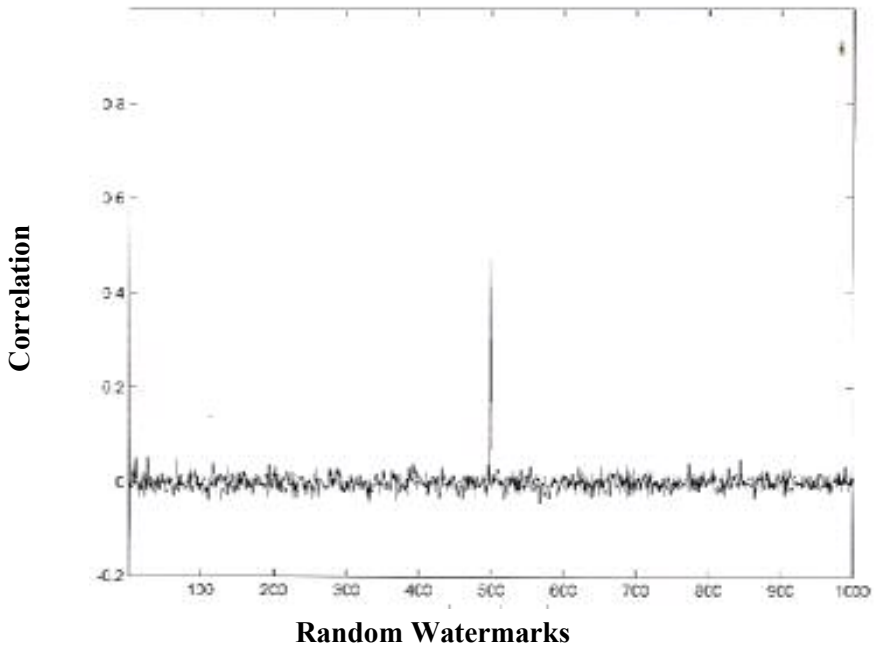


Figure 23: Random watermark detection results under scaling down attack

Figure 24: New watermarked image under salt and pepper attack

Figure 25: Decoded watermark under salt and pepper attack

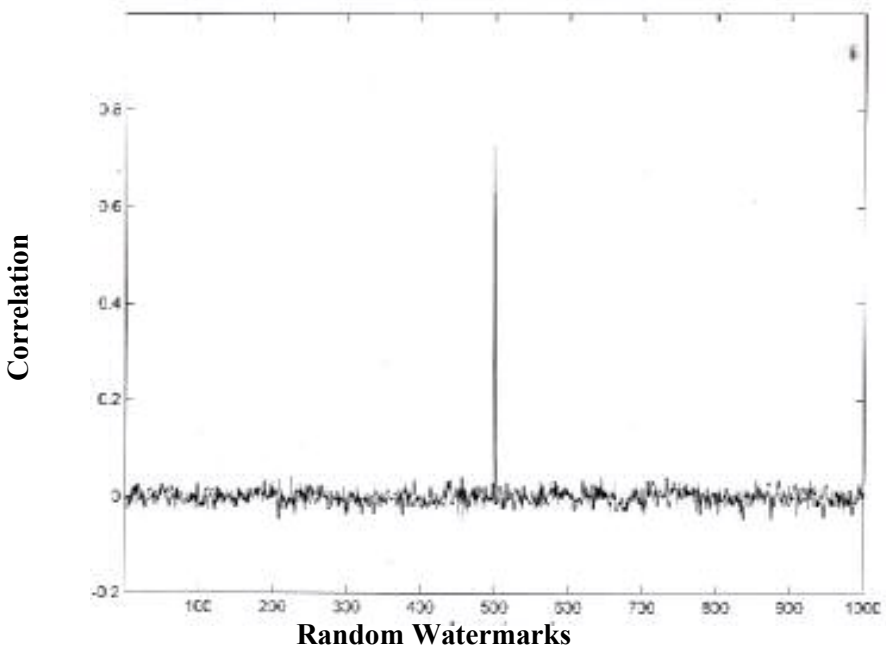


Figure 26: Random watermark detection results under salt and pepper attack

5. Conclusions and Future Suggestions:

The need for digital watermarking as electronic distribution of copyright material becomes more prevalent. In this paper, We have demonstrated that the discrete wavelet transform (DWT) resembles the human visual system and allows better image adaptation than Discrete Cosine Transform (DCT). The proposed watermarking algorithm is based on wavelet transform which has the following advantages:

- The hierarchical image representation due to the multi-resolution characteristics of the wavelet transform is especially suitable for applications where the image is transmitted progressively and a large amounts of data have to be processed, such as in video application, or for real-time systems.
- The wavelet domain allows superior modeling of the human visual system.
- The high-resolution subbands allow locating image features such as edges or textured area easily in the transform domain.
- The wavelet transform is computationally efficient and can be implemented in a variety of ways, e.g. by means of filter convolution.

Application of the described algorithm to color images is straightforward. The most common transformation of a color image is to convert it to black and white. Color image is therefore converted into a YCbCr representation, for example, and the brightness component Y is then watermarked. The color image can then be converted to other formats, but must be converted back to YCbCr prior to extraction of the watermark. Color images are also robust to attacks applied to gray-level images.

Watermarking method presented in this paper is non-blind technique. It may be useful to prove in court that a watermark is present without using the original, unwatermarked image.

We expect that technique mentioned in this paper should be extended straightforwardly to video data. However, special attention must be paid to the time-varying nature of these data.

References

Cox I. J., Miller M. L., Bloom J. A.,2000, "Watermarking Applications and their Properties", International Conference on Information Technology, Las Vegas.

Fu E. H. , 1998, "Literature Survey on Digital Image Watermarking", EE381k- Multidimensional Signal Processing.

Karzenbeisser S., Petitcolas F. , 2000, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House.

Lakshmanan V. , Jan. 2000, " A Short Write-up on Wavelets". Website: www.cimms.ou.ed/~lakshmanan/papers/wavelet/wavelet.html.

Loo P. , March 2002, "Digital Watermarking Using Complex Wavelets", Ph. D. Thesis, University of Cambridge.

Mallat S. , 1999, "A Wavelet Tour of Signal Processing", Second Edition, Academic Press.

Meerwald P. , 2001, "Digital Image Watermarking in the Wavelet Transform Domain", M. Sc. Thesis, Salzburg University, Germany.

Pinsky M. A, 2000, "Introduction to Fourier Analysis and Wavelets", Brooks/Cole.

Polikar R. , 2002, "The Wavelet Tutorial". Web site: engineering.rowan.edu/~polikar/wavelets/wttutorial.html.

Suk J., Hartung F., Girod B. , 1999, "Digital Watermarking of Text Image, and Video Documents", Elsevier Preprint.