On the Security Enhancement of Multimedia Copyright Protection for E-Business

M. A. Suhail[1] and M. S. Obaidat[2]

[1] University of Bradford, UK, ** Monmouth University, USA
[2] Corresponding Author: Prof. M. S. Obaidat, Department of Computer Science, Monmouth University, W. Long Branch, NJ 07764, USA.

Abstract. An important factor that slows down the growth of multimedia networked services is that authors, publishers and providers of multimedia data are reluctant to allow the distribution of their documents in a networked environment. This is due to the fact that it is easy to reproduce digital data in their exact original form, which encourages copyright violation, data misappropriation and abuse. Watermarking security enhancement is highly required for multimedia copyright applications. This work enhances the security of watermarking algorithm without affecting the robustness of the watermark by implementing the wavelet filter parameterization (WPF). Our experimental work shows that the watermarking algorithm based WPF robustness can enhance the security of watermarking.

Keywords. E-Business, Security Enhancement, Multimedia Copyright, Watermarking, Discrete Wavelet Transform, Wavelet Filter Parameterization.

1 Introduction

Information is becoming widely available via global networks. The advent of multimedia is allowing different applications to mix sound, images, and video and to interact with large amounts of information (e.g. in e-business, distance education, and human-machine interface). The industry is investing to deliver audio, image and video data in electronic form to customers, and broadcast televisions companies, major corporations, and photo archivers are converting their archives from analogue to digital form. This movement from traditional content, such as paper documents, analog recordings, to digital media is due to the several advantages of digital media over traditional media [1].

Moreover, modern electronic commerce (e-commerce) is a new activity that is the direct result of a revolutionary information technology, digital data and the Internet. E-commerce is defined as the conduct of business transactions and trading over a common Information Systems (IS) platform such as the web or Internet. The amount of information being offered to public access grows at an amazing rate with current and new technologies. Schemes used in e-commerce are allowing new and more efficient ways of carrying out existing business. These have impacted not only all

S. Obaidat M. and A. Suhail M. (2004).
On the Security Enhancement of Multimedia Copyright Protection for E-Business.
In *Proceedings of the 1st International Workshop on Electronic Government and Commerce: Design, Modeling, Analysis and Security*, pages 104-115
DOI: 10.5220/0001404901040115

commercial enterprises, but also social life. The e-commerce potential was developed through the World Wide Web (www) in the 1990s. E-commerce can be divided into E-Tailing, E-Operations and E- Fulfillment; all supported by an E-Strategy. E-Fulfillment is an area within e-commerce, which still seems quite blurred. It complements E-Tailing and E-Operations as it covers a range of post-retailing and operational issues. The core of e-fulfillment is payment systems, copyright protection of intellectual property, security (which includes privacy) and order management (i.e. supply chain, distribution, etc). In essence, fulfillment is seen as the "fuel" to the growth and development of e-commerce. The focus of this paper is copyright protection of multimedia copyright projection for e-business. The paper starts by introducing the problem of copyright protection of intellectual property in the digital environment, and then it provides a discussion about digital watermarking as one solution of this problem. A review on security enhancement is given in section 3. The paper discusses the discrete wavelet domain (DWT) and its features. Then, it explains how the wavelet mother can be parameterized and adapted in the work to enhance the security of the watermarking process. Results of our experimental work of the watermarking embedding process and the conclusions are given at the end of the paper.

2 Copyright Protection of Digital Intellectual Property

An important factor that slows down the growth of multimedia networked services is that authors, publishers and providers of multimedia data are reluctant to allow the distribution of their documents in a networked environment. This is because of the ease of reproducing digital data in their exact original form which makes copyright violation, data misappropriation and abuse easy. These are basically problems of theft and illegal distribution of intellectual property. Therefore, creators and distributors of digital data are actively seeking reliable solutions to the problems associated with copyright protection of multimedia data. Also, this ease of transmitting digital multimedia content over the Internet, has raised questions about how these rights apply in the new environment? How can digital intellectual property be made publicly available while guaranteeing ownership of the intellectual rights by the rights-holder and free access to information by the user?

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.

3 Digital Watermarking

Digital watermarking is an efficient technique to protect intellectual property from illegal copying. It provides a means of embedding a message in a piece of digital data without destroying the value of the digital data. Digital watermarking techniques embed a known message in a piece of digital data as a means of identifying the rightful owner of the data. These techniques can be used on many types of digital data including still imagery, movies, and music. This work focuses on digital watermarking for images and in particular invisible watermarking. A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations that may degrade the host document.

Digital Watermarking techniques derive from steganography, which means covered writing (from the Greek words stegano or "covered" and graphos or "to write"). Steganography is the science of communicating information while hiding the existence of the communication. The goal of steganography is to hide an information message inside harmless messages in such a way that it is not possible even to detect that there is a secret message present. Both steganography and watermarking belong to a category of information hiding, but the objectives and conditions for the two techniques are just the opposite. In watermarking, for example, the important information is the "external" data (e.g. images, voices, etc.). The "internal" data (e.g. watermark) is additional data for protecting the external data and to prove ownership. In steganography, however, the external data (referred to as a vessel, container, or dummy data) is not very important. It is just a carrier of the important information; the internal data. A watermark is designed to permanently reside in the host data. If the ownership of a digital work is in question, the information can be extracted to completely characterize the owner.

Digital watermarking is an enabling technology for e-business strategies: conditional and user specific access to services and resources. Digital watermarking offers several advantages. The details of a good digital watermarking algorithm can be made public knowledge. Digital watermarking provides the owner of a piece of digital data the means to mark the data invisibly. The mark could be used to serialize a piece of data as it is sold or used as a method to mark a valuable image. For example, this marking allows an owner to safely post an image for viewing but legally provides an embedded copyright to prohibit others from posting the same image. Watermarks and attacks on watermarks are two sides of the same coin. The goal of both is to preserve the value of the digital data. However, the goal of a watermark is to be robust enough to resist attack but not at the expense of altering the value of the data being protected. On the other hand, the goal of the attack is to remove the watermark without destroying the value of the protected data. The contents of the image can be marked without visible loss of value or dependence on specific formats. For example a bitmap (BMP) image can be compressed to a JPEG image. The result is an image that requires less storage space, but cannot be distinguished from the original. Generally, a

JPEG compression level of (70%) can be applied without humanly visible degradation. This property of digital images allows insertion of additional data in the image without altering the value of the image. The message is hidden in unused "visual space" in the image and stays below the human visible threshold for the image [1, 2].

4 Literature Review

Digital watermarking can be developed using spatial and frequency domain transforms. In frequency domain, researchers are using discrete cosine transform (DCT), Discrete wavelet transform (DWT), fractal, etc. However, many watermarking techniques address the utilization of the feature of DWT for the watermarking embedding algorithms. Also, more attention has been given in recent years to the security of watermarking algorithms using the DWT [1-10]. Watermark attackers are making use of their knowledge of watermarking algorithms to defeat watermarks. Some algorithms do not protect the location of the watermark information; therefore anyone with knowledge of these watermarking processes can attack them easily. Such algorithms cannot guarantee security. There is a trade-off between robustness and capacity versus security [3]. Fridrich presents in [4-5] a model of key-dependent basis functions intended to protect a watermark from attacks. His algorithm improves resistance to attacks by inserting the watermark information into a secret transform domain [10]. However, this algorithm is not practical because of its computational complexity. It has huge computational requirements producing many orthogonal patterns of the size of the host image. Kundur [6] proposed another watermarking algorithm, which protects the location where the watermark information is embedded. However, the algorithm is not secure enough to protect the location where the watermark information is embedded. Also, both of these security techniques limit the robustness of the algorithm. Meerwald *et al.* [3] introduced secret wavelet filters using parameterization to decompose the host image. They tested their idea with different known algorithms. They did not propose a new watermarking system; only experimented with this idea on existing watermarking systems.

In this paper, we describe the enhancement of the security of a watermarking algorithm without affecting its robustness by implementing wavelet filter parameterization (WPF). This protects the location of the embedded watermark information. We also present the watermarking process based on the WPF. The proposed watermarking system relies on discrete wavelet domain decomposition, which allows the independent processing of the resulting components without significant perceptible interaction between them because the image is separated into bands. Experimental results presented here show that the robustness of the WPF-based watermarking algorithm is sufficient for the watermark to be extracted.

5 The Proposed Security Enhancement Scheme

The decomposition of the signal into different frequency bands is simply obtained by successive high-pass and low-pass filtering of the spatial domain signal. A half band low-pass filter removes all frequencies that are greater than half the highest frequency in the signal. The new proposed watermarking scheme in this paper builds secret wavelet filters. This is achieved by decomposing the host signal using wavelet parameterization filters (WPF) [7] and keeping the parameter values secret. The location of the watermark is protected because of the secret wavelet transform domain. The security of digital watermarking schemes operating in the transformed domain is improved without affecting the robustness or the invisibility of the watermark. Also, incorporating WPF in the algorithm does not add significant computational overhead. This section describes how to construct secret wavelet filters by building parameterized 2-channel perfect reconstruction quadrature mirror filter banks. The relation between the quadrature mirror filters (QMFs) $H(e^{-j\omega})$ and $G(e^{-j\omega})$ is given by:

$$G(e^{-jw}) = -e^{-jw} H^*(e^{-j(w+x)}) \qquad (1)$$

H^* (.) denotes the complex conjugate of H(.). In reference [8], it is shown that the sequence $\{h_k\}$ should satisfy the following conditions:

1. Normalized Condition: $\sum h_k = 2$ (2)

2. Orthogonality Condition:

$$\sum h_k h_{k+2m} = 2\delta(m) \qquad (3)$$

3. Vanishing Moment Condition:

$$\sum (-1)^k k^m h_k = 0 \text{, for } m = 0, 1, \ldots, M-1 \qquad (4)$$

where $M \geq 1$ and $\delta(m)$ is a discrete delta function. Condition 2 indicates that

$H(e^{-j\omega})$ and $G(e^{-j\omega})$ are perfect reconstruction (PR) filters. This implies that the following matrix:

$$\mathrm{H}(e^{-j\omega}) = \frac{1}{2}\begin{bmatrix} H(e^{-j\omega}) & H(e^{-j(\omega+\pi)}) \\ G(e^{-j\omega}) & G(e^{-j(\omega+\pi)}) \end{bmatrix} \qquad (5)$$

is unitary [9]. Therefore, $H(e^{-j\omega})$ and G $(e^{-j\omega})$ form a 2-channel perfect reconstruction QMF bank [8]. H $(e^{-j\omega})$ has a zero of order M at $\omega = \pi$ when the third condition is satisfied. This implies that the term $(1 + e^{-j\omega})^M$ must be a factor of H $(e^{-j\omega})$ [7]. Defining Q $(e^{-j\omega})$ to be a polynomial in $e^{-j\omega}$, H $(e^{-j\omega})$ can be written in the form:

$$H(e^{-j\omega}) = (1 + e^{-j\omega})^M Q(e^{-j\omega}) \qquad (6).$$

The above Equations indicate also that $G\ (e^{-j\omega})$ will have a zero of order M at $\omega = 0$ when condition 3 is satisfied [8]. Therefore, to construct a compactly supported orthogonal wavelet a sequence of scaling coefficients, h_k must be built such that:

1. The matrix $\mathbf{H}(e^{-j\omega})$ is unitary i.e.:

$$\mathrm{H}^{*T}(e^{-j\omega}) = \mathrm{H}^{-1}(e^{-j\omega})$$

2. $H(e^{-j\omega})$ has a zero of order M at

$\omega = \pi$.

Denoting the z transforms of the real sequences h_k and g_k (when $z = e^{-j\omega}$) by H (z) and G (z) [10],

$$H(z) = \sum h_k z^k \qquad (7)$$

$$G(z) = \sum g_k z^k \qquad (8)$$

The polyphase matrix is fundamental to many applications in multirate digital signal processing. These include perfect-reconstruction analysis systems and efficient real time implementation of decimation and interpolation filters. The polyphase matrix is introduced here for the derivation of the WPF. The polyphase matrix E (z) is shown in reference [9], to have the following parameterization:

$$E(z) = V_{N-1}(z)V_{N-2}(z)\ldots V_1(z)V_0 \qquad (9)$$

where: $V_0 = \begin{bmatrix} \cos\theta_0 & -\sin\theta_0 \\ \sin\theta_0 & \cos\theta_0 \end{bmatrix}$ (10)

$$\theta_0 \in [0, 2\pi]$$

$V_k(z) = I + (z-1)v_k v_k^T$
for $1 \le k \le N-1$ (11)

where, vk is a 2 × 1 real vector with unit norm ($v_k^T v_k = 1$) and can be written in the following form [3, 9]:

$$v_k = \begin{bmatrix} \cos\theta_k \\ \sin\theta_k \end{bmatrix} \qquad (12)$$

Then, the polyphase representation of the filters H (z) and $z^{2(N-1)}G$ (z) based on $\boldsymbol{E}$ (z) can be written as:

$$\begin{bmatrix} H(z) \\ z^{2(N-1)}G(z) \end{bmatrix} = \sqrt{2}E(z^2)\begin{bmatrix} 1 \\ z \end{bmatrix} \qquad (13)$$

It is shown in reference [9] that **H** (z) will be unitary if and only if the matrix ***E*** (z) is unitary. The filter $z^{2(N-1)}$ *G* (*z*) is used in (18) rather than the filter *G* (*z*) to guarantee that the relation $g_k = (-1)^k h_{1-k}$ is satisfied. The filter *H* ($e^{-j\omega}$) must vanish (have a zero value) at some order $\omega = \pi$ to be a scaling filter. When

ω=π, i.e., $z = e^{j\pi}$ = -1, then, $V_k(z^2)\Big|_{z=-1} = I + (z^2-1)v_k v_k^T\Big|_{z=-1} = I$ (14)

Thus:

$$E(z^2)\Big|_{z=-1} = IV_0$$

$$V_0 = \begin{bmatrix} \cos\theta_0 & -\sin\theta_0 \\ \sin\theta_0 & \cos\theta_0 \end{bmatrix}$$

Then, for *k* = 1, 2, … , *N* – 1, equation (13) becomes:

$$\begin{bmatrix} H(z) \\ z^{2(N-1)}G(z) \end{bmatrix}_{z=-1} = \sqrt{2}V_0\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \sqrt{2}\begin{bmatrix} \sin\theta_0 + \cos\theta_0 \\ \sin\theta_0 - \cos\theta_0 \end{bmatrix} \qquad (15)$$

To make the filter *H* ($e^{-j\omega}$) have a zero value at some order $\omega = \pi$, equation (15) must be forced to be as shown below:

$$\begin{bmatrix} H(z) \\ z^{2(N-1)}G(z) \end{bmatrix}\Bigg|_{z=-1} = \begin{bmatrix} 0 \\ \sqrt{2} \end{bmatrix} \qquad (16)$$

Comparing equations (15 and 16),

$$\sin\theta_0 + \cos\theta_0 = 0,$$

$$\sin\theta_0 - \cos\theta_0 = \sqrt{2}\ .$$

To satisfy these two equations with $\theta_0 \in [0, 2\pi]$,

$$\theta_0 = 3\pi / 4.$$

This guarantees that H ($e^{-j\omega}$) has at least a zero of order one at $\omega = \pi$. Also, the wavelet has at least one vanishing moment. In this work, the Daubechy 1 (Haar) wavelet is used. The associated scaling function is given by a sequence of two coefficients $\{h_0, h_1\}$ where $h_0 = h_1 = 1$ [8]. Other wavelet functions can be used and even can produce better results since the Daubechy 1 (Haar) wavelet suffers from discontinuous.

$$\phi(x) = \begin{cases} 1 & \mathit{if}\ 0 \le x \le \frac{1}{2} \\ -1 & \mathit{if}\ \frac{1}{2} < x \le 1 \\ 0 & \mathit{elsewhere} \end{cases} \qquad (17)$$

The parameterization of this wavelet is derived starting from equation (13). For a sequence of two coefficients $N = 2$ and equation (13) becomes:

$$\begin{bmatrix} H(z) \\ z^2 G(z) \end{bmatrix} = \sqrt{2} E(z^2) \begin{bmatrix} 1 \\ z \end{bmatrix} \qquad (18)$$

Accordingly $\boldsymbol{E}$ (z^2) [9] will be:

$$E(z^2) = V_1(z^2) V_0 \qquad (19)$$

$$V_0 = \begin{bmatrix} \sin\theta_0 & -\cos\theta_0 \\ \sin\theta_0 & \cos\theta_0 \end{bmatrix} \qquad (20)$$

It has been proven [9] that $\theta_0 \in [0, 2\pi]$ should be equal to $\theta_0 = 3\pi / 4$, then,

$$V_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Since $N = 2$ there are two parameters θ_0 and θ_1. With $\theta_0 = 3\pi/4$:

$$\begin{bmatrix} H(z) \\ z^2 G(z) \end{bmatrix} = [I + (z^2 - 1) v_1 v_1^T] \begin{bmatrix} 1+z \\ 1-z \end{bmatrix} \qquad (21)$$

and,

$$v_1 {v_1}^T = \begin{bmatrix} \cos^2 \gamma_1 & \sin\gamma_1 \cos\gamma_1 \\ \sin\gamma_1 \cos\gamma_1 & \sin^2 \gamma_1 \end{bmatrix} \qquad (22)$$

γ_1 is a parameter for wavelet filters. Substituting equation (22) in equation (21),

$$\begin{bmatrix} H(z) \\ z^2 G(z) \end{bmatrix} =$$

$$[I + (z^2 - 1)\begin{bmatrix} \cos^2 \gamma_1 & \sin\gamma_1 \cos\gamma_1 \\ \sin\gamma_1 \cos\gamma_1 & \sin^2 \gamma_1 \end{bmatrix}]\begin{bmatrix} 1+z \\ 1-z \end{bmatrix}$$

……………………………………………(23)

Or

$$\begin{bmatrix} H(z) \\ z^2 G(z) \end{bmatrix} =$$

$$\begin{bmatrix} 1 + (z^2 - 1)\cos^2 \gamma_1 & (z^2 - 1)\sin\gamma_1 \cos\gamma_1 \\ (z^2 - 1)\sin\gamma_1 \cos\gamma_1 & 1 + (z^2 - 1)\sin^2 \gamma_1 \end{bmatrix}\begin{bmatrix} 1+z \\ 1-z \end{bmatrix}$$

……………………………………………(24)

Therefore,

$$H(z) =$$

$$(1+z)[1 + (z^2 - 1)\cos^2 \gamma_1 - (1-z)^2 \sin\gamma_1 \cos\gamma_1]$$

………………………………………………(25)

Taking the inverse z transform [9] of (30):

$$h_0 = \sin\gamma_1 \sin\left(\gamma_1 - \frac{\pi}{4}\right) \qquad (26)$$

$$h_1 = \sin\gamma_1 \sin\left(\gamma_1 + \frac{\pi}{4}\right) \qquad (27)$$

$$h_2 = \cos\gamma_1 \sin\left(\gamma_1 + \frac{\pi}{4}\right) \qquad (28)$$

$$h_3 = \cos\gamma_1 \sin\left(\frac{\pi}{4} - \gamma_1\right) \qquad (29)$$

In order to build secret wavelet filters, the parameter γ_1 should be kept secret. This parameter is the key to the wavelet transform domain obtained when decomposing an image using the associated wavelet filters. Keeping it secret ensures that the location of the watermark, impressed on the transform coefficients, is also protected. The parameterization of wavelet filter coefficients described above generates perfect reconstruction filters.

6 Results

Experiments were carried out on images of sizes 256x256 and 512x512 to test the proposed filter parameterization algorithm. The secret parameter γ_1 is chosen to be (-0. 786534685492 rad) in this experiment and can be changed to any value between 0 and π rad. This value should be kept secret when building secret wavelet filters. The image and watermark were both transformed using the parameterized DWT. The impact of wavelet parameterization on the robustness and visibility of the resulting watermark was then investigated. Experiments were performed with and without parameterization for various kinds of attack. The impact of wavelet parameterization on the watermarking robustness and invisibility were studied. An analysis was done with and without parameterization against various kinds of attacks. Experimental results obtained on different images. Sample results for the “fruit” image (Figure 1) are shown in Figure 2 which is watermarked based on DWT-WPF. Figure 3 shows the watermarked ‘fruit’ image attacked by JPEG compression. The analysis with and without parameterization against JPEG can be seen in Figure 4. The watermark is still easily recovered after using WPF since the correlation coefficient is well above the threshold as can be seen in Figure 4. The threshold is determined based on empirical studies and it is found to be 0.1. Hence, the security parametric filters are implemented without perceptible image degradation. JPEG compression is applied on different compression ratios, which varies from 5 to 50. Corresponding to that, the correlation coefficient varies between 0.6 and 1. Figure 4 demonstrates the robustness against compression attack that can be achieved with WPF even though there is a tradeoff between security and the robustness.

7 Conclusion

This work improves the security of a watermarking algorithm without damaging the robustness of the watermark. This is done by implementing wavelet filter parameterization for use by the watermarking algorithm in the transform domain. The location of embedded watermark information is protected by keeping the key for the WPF secret. No one can extract the watermark without having the key for the WPF filters as well as the key to generate the watermark. The experimental results show some reduction of robustness when using WPF, but not enough to prevent the watermark from being extracted. Adding the WPF to the DWT algorithm does not cause much computational overhead.

References

1. M. Suhail and M. S. Obaidat," Digital Watermarking-Based DCT and JPEG Model," IEEE Transactions on Instrumentation and Measurement, Vol. 52, No. 5, pp. 1640-1647, October 2003.
2. M. Suhail, and M. Dawoud, Watermarking Security Enhancement Using Filter Parameterization in Feature Domain" *Multimedia and Security Workshop at the ninth ACM Multimedia 2001 Conference*, pp. 15-18, September 2001.
3. P. Meerwald, A. Uhl, "Watermark security via wavelet filter parameterization," *International Conference on Image Processing, ICIP01*, vol. 3, pp. 1027-1030, October 2001.
4. J. Fridrich, "Key-dependent image transforms and their applications in image watermarking," *Proceeding of International Conference on Image Science, Systems and Technology*, *CISST 99*, pp. 237-243, June 1999.
5. J. Fridrich, A. Baldoza, and R. Simard, "Robust digital watermarking based on key-dependent basis functions," *Proceeding of the 2nd Information Hiding Workshop, LNCS*, vol. 1525, pp. 143-157, 1998.
6. D. Kundur, "Improved digital watermarking through diversity and attack characterization," *Proceeding of ACM Workshop on Multimedia Security*, pp. 53-58, October 1999.
7. H. Zou and A. Tewfik, "Parameterization of compactly supported orthonormal wavelets," *IEEE Transactions on Signal Processing*, vol. 41, no. 3, pp. 1428-1431, March 1993.
8. I. Daubechies, *Ten Lectures on Wavelets.* SIAM, Pennsylvania, USA, 1992.
9. P. Vaidyanathan, "Multirate digital filters, filters banks, poly-phase networks, and applications: a tutorial," *Proceedings of the IEEE*, vol. 78, no. 1, January 1990.
10. A. Oppenheim and R. Schafer, *Discrete-Time Signal Processing,* Prentice Hall, New Jersey 1989.

Appendix

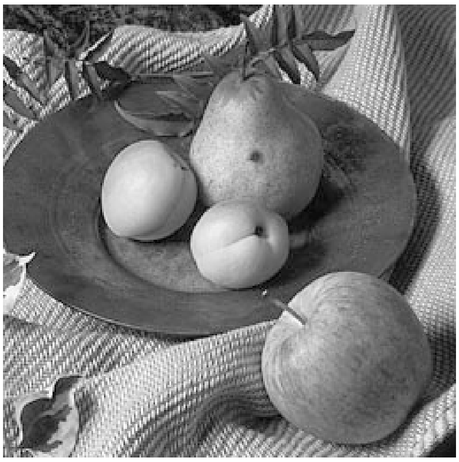

Fig.1. Original Image.

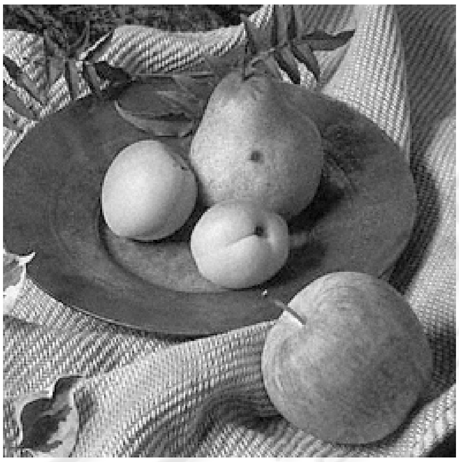

Fig. 2. Watermarked Image**.**

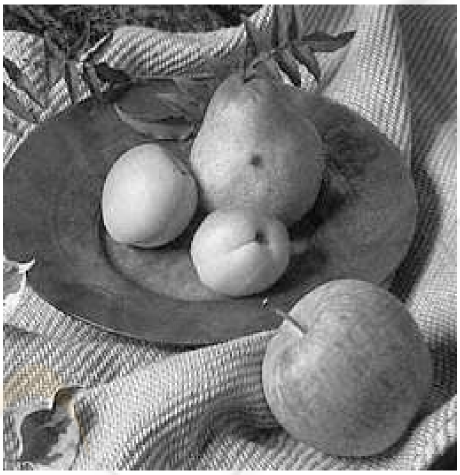

Fig. 3. Compression of Watermarked image using JPEG of CR 6:1.

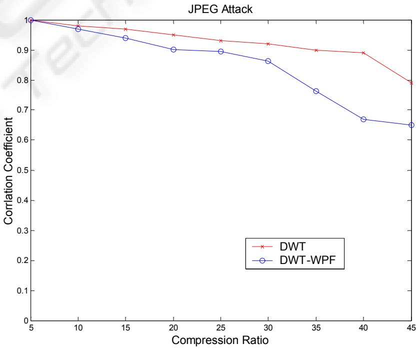

Fig. 4. Results of applying JPEG compression on the watermarked image with and without parameterization filters.