Quantization-Based Image Watermarking using Multi-resolution Wavelet Decomposition

Safwat Hamad, Amal Khalifa
Faculty of Computer & Information Sciences
Ain Shams University, Cairo, Egypt
safwat@fcis.asu.edu.eg, amal@fcis.asu.edu.eg

Abstract

Watermarking techniques provide efficient methods for protecting copyright of intellectual property. Since the discrete wavelet transform allows independent processing of the resulting sub-bands without significant perceptible interaction between them, it is expected to make the watermark embedding more imperceptible. Furthermore, Wavelet-based watermarking techniques showed to be robust in the face of attacks. In this paper, we introduce an algorithm that applies a quantization step on the sorted detail coefficients of the L^{th} level resolution of the wavelet decomposition of a true color image. The extraction process can be carried out blindly, i.e. without the need to refer to the original host image. Experimental results showed that the proposed embedding strategy causes low distortion on the watermarked images where the PSNR values were successfully greater than 40 dB. Furthermore, the proposed method showed effective resistance to attacks such as JPEG compression, image filtering, and Gaussian noise. More simulations were also carried out to evaluate the performance of the proposed algorithm in comparison to similar transform-domain techniques.

Keywords: *watermarking, image, wavelet transform, quantization, invisibility, Robustness, attack.*

1. Introduction

With the great advances in computers and communication, people can easily copy, manipulate, and communicate almost any kind of files yet very easily even with a cell phone. This has created a strong need for protecting private data and intellectual material from malicious and/or illegal usage. Therefore, watermarking techniques attracted a lot of attention in research providing the ultimate way to embed ownership data in a wide range of digital media such as Documents, sound tracks, images, Videos [1], File systems [2], networks [3] and more interestingly 3D objects [4], and DNA sequences [5].

Due to their popularity on the internet, digital images were the focus of many information hiding techniques. Although the signature data can take any binary form, it is more convenient to be a small image or a logo [6, 7, 8]. In this case, it will be easier to authenticate in the case of judicial dispute. In addition, encryption can be used to further increase the security of the watermarking system [9]. Most of the work done in watermarking applications adopts embedding the watermark data using some image transforms such as Discrete-Cosine Transform (DCT) [10, 11] and discrete Wavelet transforms (DWT) [12, 13, 14].

The wavelet transform is identical to a hierarchical sub-band system, where the sub-bands are logarithmically spaced in frequency. A 2D DWT result in four classes of coefficients: the (HH) coefficients represent diagonal features of the image, whereas (HL and LH) reflect vertical and horizontal information respectively. At the coarsest level, the low pass coefficients (LL) representing the approximation sub-band. As shown in fig. 1, The same decomposition can be further carried on the LL quadrant up to $\log_2$(min (height, width)). Furthermore, the inverse of this operation (IDWT) can be used to reconstruct the original from the DWT coefficients. Research into human perception discovered an intrinsic similarity between the way an eye splits an image and the multi-resolution decomposition of the DWT [8]. Therefore, DWT is expected to make the process of imperceptible embedding more effective.

In this paper, a blind, robust and secure WLT-based watermarking technique is proposed. This method can be considered as an enhancement of the technique proposed in [15]. The proposed technique can invisibly hide any kind of binary watermarks in colored images using Multi-resolution WLT transform. The rest of the paper is organized as follows: the next section describes the details of the embedding and the extraction modules of the proposed scheme. Section three describes the different criteria and metrics that will be used during the performance evaluation process and comparisons with existing techniques. Experimental results are then discussed in section five. Finally comes the conclusions section followed by the used references.

2. The Proposed Model

Before going into the details of the proposed watermarking technique, we need to highlight some aspects that differentiate it from the original one proposed in [15]. Both methods can be classified as transform-domain techniques because the embedding/extraction process takes place in the multi-resolution wavelet domain. However, in the proposed method, the watermark is represented as a 1D stream of elements from the set {0, 1} instead of the set {-1, 1} in [15]. In addition, instead of hiding one value per coefficient, the proposed technique is capable of hiding a group of n-bits per coefficient. Furthermore, in [15], the watermark is repeatedly embedded in all resolution levels of the wavelet decomposition, while the proposed technique hides the watermark in the L^{th} level only.

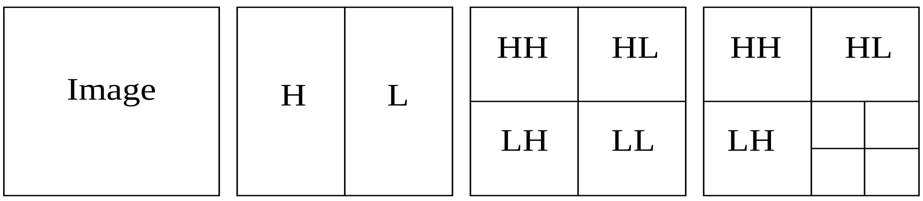

Figure 1: A Two dimensional wavelet decomposition

Throughout the text, we refer to the original host image as I, the resultant watermarked image as I', the stego key as Key, and the watermark as W whose length is denoted by N_W. Furthermore, the order by which the coefficients will be selected for embedding would depend on the value of a secret key. In fact, this is done by supplying the key as the seed value for a pseudorandom permutation module. Obviously, the details of this step must be kept secret for the security of the watermarking system. Figure 2 gives an overview on the steps of the proposed algorithm.

2.1 Embedding

The embedding process starts by computing the L^{th} level discrete wavelet decomposition of the host image. It results in 3L detail sub-bands corresponding to the horizontal, vertical, and diagonal coefficients at each of the L resolution levels. Throughout this paper we will denote the k^{th} detail coefficient of the image at the L^{th} decomposition level by $I_{k,l}(x, y)$ where $k = h, v, d$ (corresponding to horizontal, vertical, and diagonal respectively) and the (x, y) coordinate identifies the coefficient location in the specified sub-band. Furthermore, the approximation coefficients is denoted by $I_{a,L}(x, y)$.

Now, for each coefficient location (x, y) selected for embedding; by the permutation function, do the following:

1. Sort the L^{th} detail coefficients in ascending order such that :
   $I_{k1,L}(x, y) \le I_{k2,L}(x, y) \le I_{k3,L}(x, y)$
   Where $k1, k2, k3$ are distinct and belong to the set $\{ h, v, d \}$
2. If the range between $I_{k1,L}(x, y)$ and $I_{k3,L}(x, y)$ is below a given threshold value, skip the following steps and get another coefficient location.
3. Embed the next n bits of the watermark (W) as follows:
   3.1 let $start = I_{k1,L}(x, y)$ and $end = I_{k3,L}(x, y)$
   3.2. find the middle value (mid) of the range bounded between *start* and *end*
   3.3 if the most significant bit of the n bits is zero, assign the value of *mid* to *end* otherwise assign the value of *mid* to *start*.
   3.4 find the value of Δ

$$\Delta = \frac{|end - start|}{2n - 1}$$

   3.5 let steps be the decimal representation of the least significant *n-1* bits.
   3.6 quantize the middle coefficient $I_{k2,L}(x, y)$ as follows:

$$I_{k2,L}(x, y) = start + \Delta\,(steps+1)$$

Finally, the watermarked image (I') is obtained by applying the L^{th} level inverse wavelet transform (IDWT). Notice that in the case where the host image is a true colored image, the above process can be applied on each color component separately, providing more space to accommodate a larger watermark.

2.2 Extraction

The objective of the watermark extraction process is to reliably obtain an estimate (W') of the original watermark (W) from a possibly distorted version of the watermarked image [15]. Hence, the steps of extraction process are exactly the inverse of those followed during the embedding phase. In this case, only the value of the key is required in order to identify the locations at which the watermark was embedded. So, the extraction process should start by computing the L^{th} level discrete wavelet decomposition of the watermarked image (I'). One should assume that W' is a zero length vector at this point of the process.

Now, for each coefficient location (x, y) was utilized for embedding; do the following:

1. Sort the detail coefficients in ascending order such that:

$$I'_{k1,l}(x,y) \leq I'_{k2,l}(x,y) \leq I'_{k3,l}(x,y)$$

   Where $k1, k2, k3$ are distinct and belong to the set $\{h,v,d\}$

2. If the range between $I_{k1,l}(x,y)$ and $I_{k3,l}(x,y)$ is below a given threshold value, skip the following steps and get another coefficient location.

3. Extract the next n bits of the watermark as follows:
   3.1 let $start = I_{k1,l}(x,y)$ and $end = I_{k3,l}(x,y)$
   3.2. for $i = n$ to 1 do
      3.2.1 find the middle value (mid) of the range bounded between $start$ and end
      3.2.2 if $I'_{k2,l}(x,y) \leq mid$, set the i^{th} bit to zero otherwise set its value to one.
   3.3 update $start$ and end to represent the new range.

4. Concatenate the n extracted bits to W'.

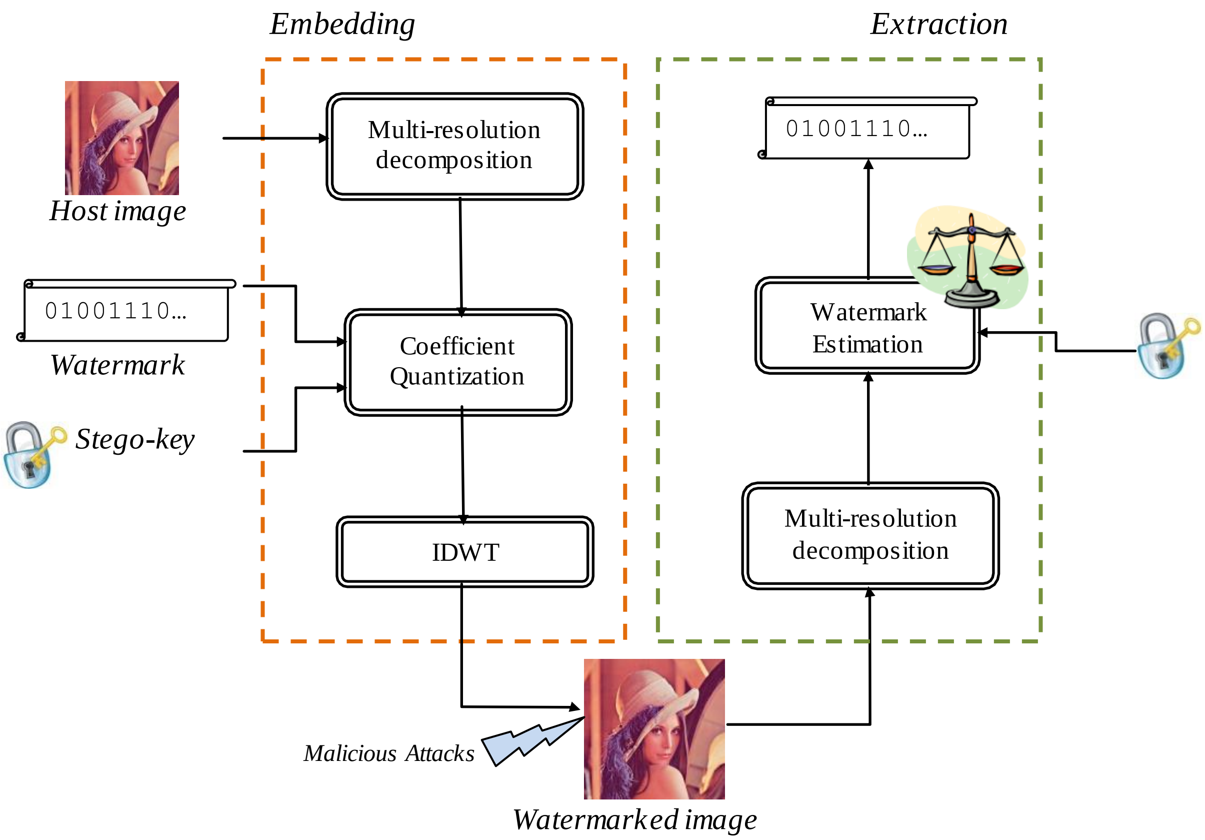

Figure 2: The proposed watermarking model

Once the estimated watermark (*W'*) is extracted it has to be compared to the original watermark (*W*) in order to measure their similarity. To quantify this similarity, the normalized correlation (NC) coefficient can be computed as follows:

$$Sim(W,W') = \frac{W \, . \, W'}{\sqrt{W \, . W'}} \Bigg/ \frac{W \, . \, W}{\sqrt{W \, . W}} \times 100 \qquad (1)$$

where both W and W' are organized as a vectors. Obviously, the higher the similarity the better the quality of the retrieved watermark. In fact, the watermark is considered detected if the value of that correlation is above a pre-specified threshold. The choice of this threshold depends on both the length of the watermark as well as the application [15].

3. Performance metrics

This section describes the metrics used to evaluate the proposed algorithm. Usually, the performance of watermarking techniques is measured in terms of two criteria: payload, and Invisibility.

Fundamentally, the data payload is defined by the amount of information that can be hidden within an image as in (2), where M and N represent the image dimensions in pixels.

$$\text{Data Payload} = \frac{Max\ no.\ of\ hidden\ bits}{size\ of\ the\ \text{cover}} \qquad (2)$$

Furthermore, it is essential to have a measure by which one can judge how an image is degraded after watermarking. Usually the invisibility of the hidden watermark is measured in terms of the Peak Signal-to-Noise Ratio (PSNR). PSNR is measured in decibels (dB) and can be computed as in (3). Usually, values falling below 30dB indicate that the distortion caused by watermarking can be obvious. Thus, a high quality watermarked image should strive for 40dB and above.

$$PSNR = 10\log_{10}\left(\frac{\max(p(x,y))^2}{MSE}\right) \qquad (3)$$

$$\text{MSE} = \frac{1}{\text{XY}}\sum_{\text{x,y}}(\text{p(x, y)} - \tilde{\text{p}}\text{(x, y)})^2 \qquad (4)$$

where p(x,y) represents the shade level of a pixel, whose coordinates are (x,y) in the original image, and $\tilde{p}(x,y)$ represents the same pixel in the distorted image.

4. Experimental Results

This section provides a detailed analysis for the performance of the proposed algorithm based on three main criteria: Payload, Invisibility, and robustness against attacks. Payload is measured in bits per pixel, and invisibility is measured in decibel (dB). Since it is essential for a watermarking algorithm to survive certain image processing manipulations that might occur

via an attack [16], our evaluation will cover the robustness of the algorithm against JPEG compression and other types of attacks such as noise impulses and image filtering.
Basically, in this set of experiments, three standard 512x512 colored images are used as covers: Lena, Baboon, and Pepper. Furthermore, the watermark was chosen to be a 32x34 version of the grayscale image shown in fig. 3.

Figure 3: the secret image used for testing the performance of the proposed algorithm

4.1 Hiding Capacity

As illustrated above, obviously the proposed algorithm can hide up to n bits per each coefficient in the Lth DWT decomposition of each color band of the cover image. Hence, its data payload can be expressed as follows:

$$\text{Payload} = 3\left(\frac{n\,MN}{4L}\Big/ MN\right) = 0.75\, n/L \quad bpp \tag{5}$$

where M and N represent the image dimensions in pixels.

Notice that although the parameter (n) is user defined, it should be chosen to establish an appropriate trade-off between the hiding capacity and visibility of the watermark. That is, a larger value of n will increase the hiding capacity of the host image, however it can have tremendous effect on the integrity of the watermarked image. More analysis on this particular point will be given in the next section.

4.2 Invisibility Analysis

The invisibility performance of the proposed algorithm was tested and measured in PSNR. A number of experiments have been carried on the Lena image using different wavelet families. The collected results are listed in table1 using three different levels of decomposition while embedding only 2 bits per corresponding coefficients. In this table, we highlight the differences not only in imperceptibility, but also in the similarity of the extracting images. The results recommend that using the Haar transform would keep a tradeoff between invisibility and quality of recovery.

Therefore, the next set of experiments were carried out using the Haar transform to investigate the effect of the parameter (n) using three different test images: Lena, baboon and peppers. As shown in table 2, the results show that, despite the high quality of the extracted image at n = 1, the integrity of the resultant image is still affected especially at higher levels of decomposition. The reason behind that is that the quantization step carried out by the embedding process would actually replace the middle coefficient with one of the other extremes depending on the value of the embedded bit. As a result, the structure of the resultant watermarked may greatly differ from the original one. Furthermore, the extraction process can be done at a great level of confidence because of the little effect of rounding errors on the relative values of the changed coefficients giving a more precise estimation of the extracted message. On the other hand, at n=2 and 3, the similarity of the extracted images are very close at different levels of decomposition. This would require more investigations on their robustness against different attacks as will be discussed shortly.

Table 1: Comparison of Invisibility Performance between Different Wavelet Families at n = 2

Wavelet Family	Level One		Level Two		Level Three	
	PSNR (dB)	Similarity	PSNR (dB)	Similarity	PSNR (dB)	Similarity
Haar	63.63	94.49%	55.55	97.87%	45.84	97.54%
Daubechies	65.06	94.68%	57.11	94.05%	48.99	94.68%
BiorSplines	63.28	96.7%	55.41	96.33%	45.65	95.09%
ReverseBior	65.74	93.64%	56.82	94.72%	47.98	92.46%
Symlets	65.91	93.2%	57.18	96.12%	49.23	93.61%
Coiflets	66.12	96.12%	69.29	93.66%	54.71	92.39%

Table 2: Invisibility Comparison for Different Values of n

Bits per coefficient		Lena		Baboon		Pepper	
		PSNR (dB)	Similarity	PSNR (dB)	Similarity	PSNR (dB)	Similarity
n = 1	Level 2	50.28	99.26%	43.61	99.92%	50.15	99.52%
	Level 3	37.27	99.20%	34.13	99.94%	36.40	99.34%
n = 2	Level 2	55.55	97.87%	49.31	99.53%	54.97	98.52%
	Level 3	45.84	97.54%	43.69	99.42%	45.64	98.47%
n = 3	Level 2	56.37	96.00%	50.3	98.23%	55.88	96.24%
	Level 3	48.51	95.50%	45.60	98.17%	47.80	96.49%

4.3 Robustness against JPEG Compression

In this set of experiments we are going to test the robustness of the proposed method against lossy JPEG compression. Once more, the Haar wavelet was employed at the 2^{nd} and the 3^{rd} resolution levels with n varying between 2 and 3 in each case. Here, the Baboon was selected as the test image. Figures 4 and 5 show the extracted results from JPEG-compressed versions of the watermarked images at different compression ratios. The results showed that, embedding the watermark using n = 2 at three levels of decomposition would maintain a steady performance allowing almost perfect recovery of the embedded watermark even at very high compression ratios.

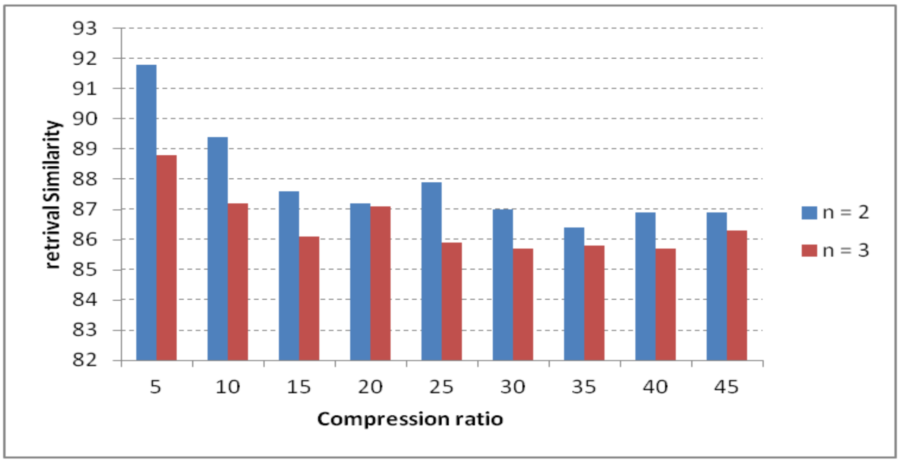

Figure 4: Performance of proposed algorithm against JPEG compression using 2-level decomposition of the Haar transform

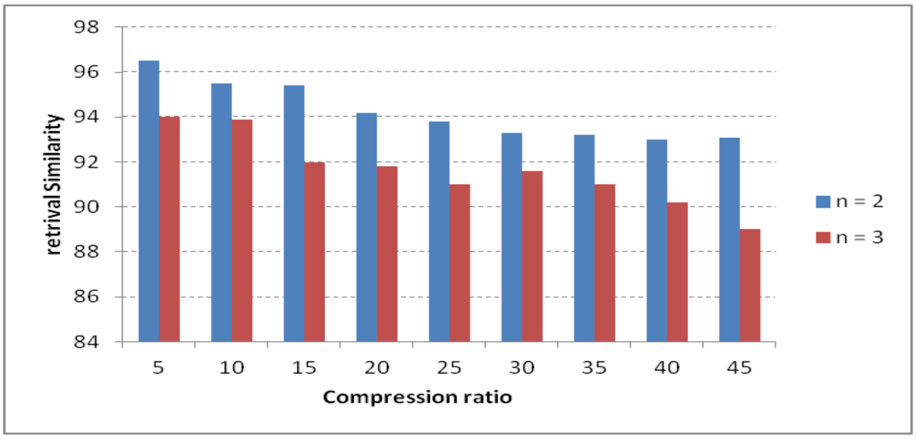

Figure 5: Performance of proposed algorithm against JPEG compression using 3-level decomposition of the Haar transform

4.4 Robustness against Image Processing Operations

In this set of experiments, the robustness of the proposed scheme is tested against some common image processing attacks such as image filtering and noise addition. Image blurring has been carried out with a 3x3 Gaussian low-pass filtering, sharpening with a low-pass filtering and median filtering. With respect to the random-noise adding attack, the watermarked images are attacked with random noise of mean=0 and variance=0.05 as well as pepper & salt noise of density=0.05. Table 3 shows the similarity of the retrieved watermark after each attack. In addition, the PSNR of the watermarked images after each attack are also giving an indication of the corruption caused by the attack. In fact, when PSNR value is lower than 40, the attack becomes obviously visible and hence, the probability of watermark corruption becomes very high. The results demonstrate that the existence of the watermark can still be verified even with high watermarked image corruption.

Table 3: Extracted Watermark Images and their Similarity Measures Under Different Image Attacks

Image operation	PSNR after attack	Similarity
Blur	41.29 dB	96.2%
Sharpen	35.06 dB	91.9%
Median Filter	38.02 dB	90.7%
Random Noise	31.95 dB	87.9%
Pepper & salt noise	35.63 dB	89.4%

4.5 Comparisons with Other Approaches

To further evaluate the performance of the proposed algorithm, several simulations have been performed and the results are compared with other existing transform-domain schemes. For the sake of standardization, this set of experiments used the color Lena (512x512) as the test image. Table 4 collects the measured distortion in PSNR caused by utilizing the max embedding capacity provided by each algorithm measured in bits per pixel (BpP). The results show that the proposed algorithm provided a better invisibility as well as larger hiding capacity compared to most of the listed techniques. Two exceptions were spotted and will be further analyzed. First, although the algorithm proposed in [9] achieved better PSNR and higher capacity, it was not successful in achieving robustness, which is an attractive attribute of the proposed algorithm. Secondly, the skin-tone technique proposed in [8] was successful in achieving better invisibility than the proposed one, but failed to provide a better capacity.

Worth to notice that, when compared to the original algorithm [15], the proposed algorithm showed an outstanding performance by doubling its payload. Furthermore, in the following set of experiments. different attacking operations were conducted investigating the survival of the embedded watermark under JPEG compression as well as mean filtering and assistive Gaussian noise. The results are listed in table 5 showing that the proposed algorithm provides tremendously better robustness under all of the tested attacks. That is, 88.6% of the watermark embedded by the proposed method could be retrieved after the watermarked image is compressed with 20% ratio, compared with a 30% retrieved by the original technique published in [15]. Unfortunately it wasn’t possible to compare their imperceptibility behavior since it was not published in the original work.

Table 4: Comparison of Performance with other Transform-Domain Methods

Method	Type of Transform	PSNR (dB)	Payload (bit/pixel)	Robust?	Blind?
Chang et al. [6]	DCT	30.34	0.14	X	√
Lin et al. [7]	DCT	35.28	0.344	X	X
Tolba et al. [9]	IWT (N=1)	58.4032	3	X	√
Lee et al. [17]	IWT	44	0.6	X	√
Cheddad et al. [8]	DWT, 1st level	49.89	0.25	√	√
Kundur et al. [15]	DWT (3rd level)	NA	0.25	√	√
Khalifa et al. [18]	DWT (2nd level, $\alpha = 0.1$)	44.54	0.375	√	X
Proposed	DWT, 3nd level (n = 2)	45.84	0.5	√	√

Table 5: Comparison of Robustness Against Image Operations with the Method in [15]

Attacking operation	Proposed	Kundur et al. [15]
JPEG Compression (ratio = 10%)	90.58%	70%
JPEG Compression (ratio = 20%)	88.64%	30%
Mean Filtering (M = 5)	92.14%	55%
Gaussian Noise (SNR = 30 dB)	85.86%	85%

5. Conclusions

This paper describes an enhanced version of the watermarking technique; proposed by the authors of [15]. The proposed technique is capable of watermarking images with any form of digital media, like text, sound or even other images. More specifically, the watermark data is embedded in the L^{th} resolution levels of the wavelet decomposition of the host image. The enhancements introduced by the proposed algorithm succeeded to double the hiding capacity of the original one. At the same time, experimental results showed a great improvement in the robustness of the original method against a number of attacks such as JPEG compression. Furthermore, more experiments showed that the proposed algorithm can achieve excellent invisibility and robustness when compared with other transform-domain techniques.

References

[1] P. Davern, M. Scott, "Steganography, its history and its application to computer based data files", Dublin University, Working paper, 1995.

[2] Anderson, Ross, Roger Needham, and Adi Shamir. "The steganographic file system." *Information Hiding*. Springer Berlin/Heidelberg, 1998.

[3] S. J. Murdoch and S. Lewis, "Embedding Covert Channels into TCP/IP," in Proceedings of the Information Hiding Workshop, 2005.

[4] Rama, K., et al. "Survey and Analysis Of 3D Steganography." *International Journal of Engineering Science and Technology (IJEST)* 3.1 (2011): 638-643.

[5] Heider, Dominik, Martin Pyka, and Angelika Barnekow. "DNA watermarks in non-coding regulatory sequences." *BMC research notes* 2.1 (2009): 125.

[6] Chang, Chin-Chen, et al. "Reversible hiding in DCT-based compressed images."*Information Sciences* 177.13 (2007): 2768-2786.

[7] Lin, Chia-Chen, and Pei-Feng Shiu. "High capacity data hiding scheme for DCT-based images." *Journal of Information Hiding and Multimedia Signal Processing*1.3 (2010): 220-240.

[8] Cheddad, Abbas, et al. "A skin tone detection algorithm for an adaptive approach to steganography." *Signal Processing* 89.12 (2009): 2465-2478.

[9] Tolba, M. Fahmy, et al. "High capacity image steganography using wavelet-based fusion." *Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on*. Vol. 1. IEEE, 2004.

[10] You, Xinge, et al. "A blind watermarking scheme using new nontensor product wavelet filter banks." *Image Processing, IEEE Transactions on* 19.12 (2010): 3271-3284.

[11] Kammoun, Fahmi, Ali Khalfallah, and Mohamed Salim Bouhlel. "New scheme of digital watermarking using an adaptive embedding strength applied on multiresolution filed by 9/7 wavelet." *International Journal of Imaging Systems and Technology* 16.6 (2006): 249-257.

[12] Wu, Chih-Chien, et al. "Saturation Adjustment Scheme of Blind Color Watermarking for Secret Text Hiding." *Journal of Multimedia* 5.3 (2010): 248-258.

[13] Tamane, S. C., R. R. Manza, and R. R. Deshmukh. "Digital Watermarking using Image Fusion Method." (2009).

[14] Tripathi, Shikha, et al. "A DWT based Dual Image Watermarking Technique for Authenticity and Watermark Protection." *Signal & Image Processing: An International Journal (SIPIJ)* 1.2 (2010): 33-45.

[15] Kundur, Deepa, and Dimitrios Hatzinakos. "Digital watermarking using multiresolution wavelet decomposition." *Acoustics, Speech and Signal Processing, 1998. Proceedings of the 1998 IEEE International Conference on*. Vol. 5. IEEE, 1998.

[16] Katzenbeisser, Stephan, and Fabien Petitolas. "Information Hiding Techniques for Steganography and Digital Watermaking." (2000): 1-2.

[17] Lee, Sunil, Chang D. Yoo, and Ton Kalker. "Reversible image watermarking based on integer-to-integer wavelet transform." *Information Forensics and Security, IEEE Transactions on* 2.3 (2007): 321-330.

[18] Al-Otum, Hazem Munawer, and Nedal Abdul Samara. "A robust blind color image watermarking based on wavelet-tree bit host difference selection." *Signal processing* 90.8 (2010): 2498-2512.