A Robust Non-blind Algorithm for Watermarking Color Images using Multi-resolution Wavelet Decomposition

Amal Khalifa
Assistant professor of Scientific computing
Faculty of Computer & Information Sciences
Ain Shams University, 11566, Cairo-Egypt

Safwat Hamad
Assistant professor of Scientific computing
Faculty of Computer & Information Sciences
Ain Shams University, 11566, Cairo-Egypt

ABSTRACT

Research in the field of watermarking is flourishing providing techniques to protect copyright of intellectual property. Among the various methods that exploit the characteristics of the Human Visual System (HVS) for more secure and effective data hiding, wavelet-based watermarking techniques showed to be immune to attacks; adding the quality of robustness to protect the hidden message from third-party modifications. In this paper, we introduce a novel algorithm that applies a casting operation of a binary message onto the wavelet coefficients of colored images decomposed at multi-level resolution. In the extraction process, the original “unwatermarked” image is used to estimate the embedded bit-stream. Experimental results showed the low distortion effect cased by the embedding strategy of the proposed method. Furthermore, the resultant watermarked-images proved high resistance to attacks such as Jpeg compression and normal image processing like sharpening, blurring as well as image filtering. More simulations were carried out to evaluate the performance of the proposed algorithm in comparison to similar transform-domain techniques.

General Terms

watermarking, image, wavelet, Robustness, attack.

Keywords

watermarking, secure embedding, image, wavelet, bit casting, invisibility, Robustness, attack.

1. INTRODUCTION

With the introduction of computers along with its diverse applications, the whole world has moved into a truly digital era. Now, with the great advances in communication, migration is made towards the cyber world of the internet where a lot of business activities are virtually taking place on-line. Furthermore, people can simply copy, manipulate, and communicate almost any kind of files yet very easily even with a cell phone. As a result of this increasing dependency on digital media, there is a strong need for techniques to protect intellectual materials from illegal usage. This is where watermarking techniques can be very useful and convenient. In fact, Watermarking techniques have evolved rapidly and succeeded to embed ownership data in a wide range of digital media such as Documents, sound tracks, images, Video [1], File systems [2], networks [3] and more interestingly 3D objects [4], and DNA sequences [5].

Since images are considered the most exchanged digital media on the internet, there has been a lot of research on information hiding techniques on digital images. In fact, Most of the work done in watermarking applications adopts embedding the watermark data by modulating coefficients in a transform domain, such as the Discrete-Cosine Transform (DCT) [6, 7] and Wavelets [8, 9]. Regarding WLT-based watermarking, a number of techniques target only significant coefficients in order to improve their robustness. Although the signature data can be any binary data, it is more convenient to be in the form of a small image or a logo [10, 11, 12]. Hence, it will be easier to authenticate in the case of Judicial dispute. Sometimes signature data are also encrypted to de-correlate the information and/or subjected to some error-correcting coding scheme [13]. Another DWT based dual watermarking technique was introduced in [14].The concept of dual watermarking, is based on embedding two watermarks are instead of one for increased protection and security. On contrast with earlier dual watermarking techniques, this method hides the watermark in the mid-frequency region, in order to achieve perceptual invisibility as well as robustness to attacks.

In this paper, a robust and secure WLT-based watermarking technique is proposed. As will be discussed shortly, any kind of binary messages can be invisibly hidden in colored images using Multi-decomposition WLT transform. The rest of the paper is organized as follows: the next section will provide a quick review on recent image-watermarking techniques. Next, section three describes the details of the embedding and the extraction modules of the proposed scheme. Section four 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 come the conclusions and references.

2. MODEL

In this section we are going to describe the proposed watermarking technique. It can be classified as a transform-domain technique since the embedding/extraction process takes place in the multi-resolution wavelet domain. Here, the cover is assumed to be a true colored image, while the secret message can take any form of digital media, like text, sound or even other images. As its name implies, the main idea of the proposed algorithm; Robust Wavelet Bit-casting (*RWBC)*, is to cast the message bitstream to the wavelet coefficients of the host image with the use of a key for the sake of improved security. Furthermore, the algorithm is considered non-blind since the original image is needed for extraction and verification.

2.1 Multi-resolution Wavelet Transform

The wavelet transform is identical to a hierarchical subband system, where the subbands are logarithmically spaced in frequency. In a one dimensional discrete wavelet transform (DWT), the input signal (s) is convolved with a high pass filter (*Hi_D*) and a low pass filter (*Lo_D*). The result of the latter convolution is a smoothed version of the input (cA_1), while the high frequency part (cD_1) is captured by the first convolution. The reconstruction involves a convolution with the syntheses filters and the results of these convolutions are added.

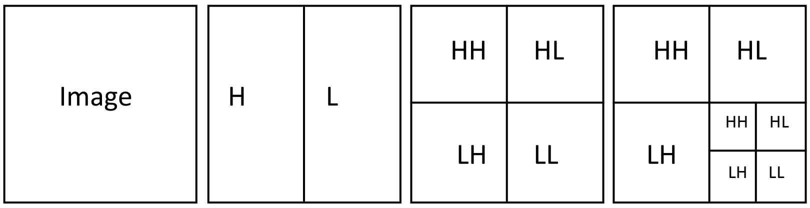


Figure 1: A Two dimensional wavelet decomposition

Two-dimensional signals, such as images, are transformed using a two-dimensional DWT, which operates in a similar manner. In 2D DWT, we first apply one step of the one dimensional transform to all rows. Then, we repeat the same for all columns. In the next step, we proceed with the coefficients that result from a convolution in both directions. As shown in figure 1, these steps 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, we also keep low pass coefficients (*LL)* that represent the *approximation* coefficients. The same decomposition can be further carried on the *LL* quadrant up to $\log_2$(min (height, width)). Furthermore, the original image can be reconstructed from these DWT coefficients. This reconstruction process is called the inverse DWT (IDWT).

Research into human perception indicates that the retina of the eye splits an image in a way similar to the multi-resolution decomposition of the DWT [12]. With this intrinsic similarity to the Human Visual System (HVS) perception, DWT is expected to make the process of imperceptible embedding more effective.

2.2 Embedding

The embedding process starts by transforming the cover image into wavelet domain. However, the used wavelet filters have floating point coefficients. Thus, despite the input image data consist of sequences of integers, the resulting filtered outputs will no longer consist of integers. So, we propose normalizing the cover image before applying DWT. In a normalized image, pixels take values between 0.0 and 1.0 instead of the integer range of (0 – 255). Hence, the magnitude of the corresponding wavelet coefficients will also range between 0.0 and 1.0.

Figure 2 depicts the steps of the proposed *RWBC* algorithm. Since, the cover image is in true-color format, the multi-resolution 2D DWT is applied on each color plane (c) separately. Furthermore, before embedding the secret message must be converted into a 1D bit stream. Of course the details of this step will depend on the type of a particular message. For example, in the case text messages, the bit stream can be formed by simply concatenating the 8-bit binary representation of ASCII code of each character. Similarly, in the case of images each pixel illumination value is converted to binary and concatenated as a sequence.

The embedding step is actually done by casting the message bit-stream to the wavelet coefficients of the host image. The image can be decomposed in any desired level of resolution (L) for the sake of enhanced robustness. Furthermore, for increased security, a key is used to determine the order by which the coefficients will be selected for embedding. This is done by a pseduorandom permutation module. The casting operation itself, is made according to equation (1), where the message bit (b) is added to the original image coefficient ; $f_{c,L}$(x, y), to produce the corresponding watermarked image coefficient $f'_{c,L}$(x, y). The factor α denotes the embedding strength whose value ranges between 0.0 and 1.0.

$$f'_{c,L}(x,y) = f_{c,L}(x,y) + (2b-1)\alpha \qquad (1)$$

In this paper, we embed the watremark into the *approximation* coefficients in order to increase its resistance to attacks. However, the algorithm can still work in the same way if any or all of the four transform sub-bands were considered for embedding. This can provide larger embedding space, however it can greatly affect the imperceptibility. Finally, after the embedding process is done, the normalized watermarked image is obtained by the inverse wavelet (IDWT) that is followed by a de-normalization step to retrieve the final watermarked image.

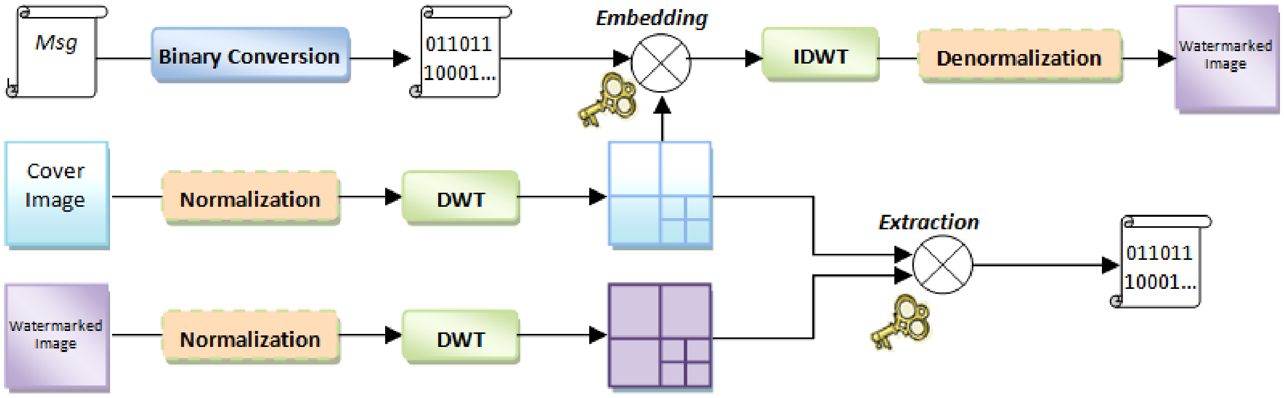


Figure 2: A block diagram for the RWBC algorithm on a true colored image

2.3 Extraction

According to equation (1), if the embedded bit is a 1 then the resultant coefficient would be greater than the original one by approximately α. On the other hand, when the embedded bit is a 0 the plus will turn into a negative sign resulting in a coefficient that is less than the original one. This means that, the extraction process requires the original image. More specifically, the message bitstream is retrieved by comparing the DWT coefficients of image at level (L) with the corresponding coefficients of the watermarked image to decide upon the value of the embedded bit. So, we can generally estimate the i^th embedded message bit using equation (2).

$$m(i) = \begin{cases} 1 & f'_{c,L}(x,y) > f_{c,L}(x,y) \\ 0 & f'_{c,L}(x,y) \le f_{c,L}(x,y) \end{cases} \qquad (2)$$

As shown in figure 2, using the same key it is possible to generate the same permutations and hence retrieve the watermark in the proper order. This ensures that only recipients who know the corresponding secret key will be able to extract the message from a watermarked image.

3. PERFORMANCE MEASURES

In this section we are going to describe 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 equation (3), where *M* and *N* represent the image dimensions in pixels.

$$Data\ Payload = \frac{Max\ no.\ of\ hidden\ bits}{M \times N} \qquad (3)$$

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 equation (4).

$$PSNR = 10\log_{10}\left(\frac{\max(p(x,y))^2}{MSE}\right) \qquad (4)$$

$$MSE = \frac{1}{XY}\sum_{x,y}(p(x,y) - \tilde{p}(x,y))^2 \qquad (5)$$

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.

Although PSNR is a good quality metric when considering random errors in images, it was not developed to include the features of the HVS. On the other hand, the Weighted PSNR (WPSNR) takes into account the fact that the human eye is less sensitive to changes in textured areas than in smooth areas [15]. The expression for WPSNR is given in equation (6), where *NVF* stands for noise visibility function that can be calculated using the formula in (7).

$$WPSNR = 10\log_{10}\left(\frac{\max(p(x,y))^2}{MSE \times VNF}\right) \qquad (6)$$

$$NVF = NORM\left(\frac{1}{1 \times \delta_{block}^{2}}\right) \qquad (7)$$

where δ_{block} is the standard deviation of luminance of the block of pixels. Just like PSNR, high value of WPSNR indicates that the image is less distorted. 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.

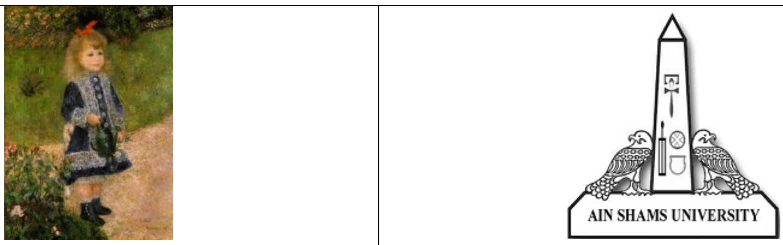
Furthermore, a measure is needed to quantify the similarity between the embedded watermerk and the extracted one. This similarity can be computed using the normalized correlation (NC) coefficient, computed as follows:

$$Sim(x,x^*) = \frac{X.X^*}{\sqrt{X.X^*}} \bigg/ \frac{X.X}{\sqrt{X.X}} \times 100 \qquad (8)$$

where *X* is the original message components organized as a vector, and *X** is the recovered vector. Obviously, the higher the similarity the better the quality of the retrieved watermark.

4. EXPERIMENTAL RESULTS

In this section, we are going to analyze the performance of the proposed (*RWBC*) algorithm based on three main criteria: Payload, Invisibility, and robustness against attacks. As we have just mentioned, payload reflects the embedding capacity provided by the algorithm measured in bits per pixel. While Invisibility; or sometimes called imperceptibility, refers to the degree by which the embedded message doesn't introduce visible distortions to the cover image. The third criterion we included in our evaluation is the robustness [16]. That is, it is essential for a watermarking algorithm to be capable of resisting common image processing manipulations that might occur via an attack. JPEG would be a good example for such an attack. Other types of attacks include noise impulses and image filtering attacks.



(a) Test image

(b) secret image

Figure 3: Images used for testing the performance of the proposed algorithm

Table 1: Comparison of Invisibility performance between different Wavelet Families at fixed embedding strength

Wavelet Family	*Level One (α = 0.05)*		*Level Two (α = 0.1)*		*Level Three (α = 0.2)*	
	WPSNR (dB)	***Similarity***	***WPSNR (dB)***	***Similarity***	***WPSNR (dB)***	***Similarity***
Haar	40.129	100.00%	41.464	100%	41.334	100%
Daubechies	40.653	99.87%	40.997	99.59%	41.221	98.99%
BiorSplines	40.635	99.9%	42.321	99.67%	43.055	99.09%
ReverseBior	40.908	99.67%	40.798	99.04%	41.820	98.14%
Symlets	40.78	99.68%	41.17	99.10%	41.799	98.32%
Coiflets	40.99	99.51%	41.328	98.70%	43.48	96.72%

Unless stated otherwise, the following sets of experiments were carried out using a (370x512) Renoir painting "*A Girl with a Watering Can*"-1876 as a test image. Furthermore, for the sake of clarity and convenience in the discussion of results, we choose to embed an image message. The secret image is a (126x133) grayscale logo of Ain shams University (ASU). The two images are shown in figure 3.

4.1 Hiding Capacity

The *RWBC* algorithm can hide only one bit per coefficient in the DWT approximation sub-band decomposed at level L. Hence, its data payload can be expressed as follows where *M* and *N* represent the image dimensions in pixels:

$$RWBC\ Payload = \frac{3\left(MN/4L\right)}{MN} = 0.75/L \quad bpp \qquad (9)$$

4.2 Invisibility Analysis

Figure 4 depicts the invisibility performance of the proposed algorithm measured in WPSNR, using the Haar transform while **α** is taking values ranging from 0.02 to 0.3. The experiments were carried out at three different levels of decomposition. It is clear that the larger the value of **α**, the more distorted the watermarked image can be. However, very low values of **α** can cause errors in the estimation of the embedded bit and hence the watermark can't be extracted correctly. This sensitivity would increase with certain types of media such as text, where an erroneous bit can change the retrieved character and hence scramble the whole textual content. So, one should compromise between invisibility and quality of recovery. Therefore, after a large number of experiments on different test images, we found that in order to maintain a good imperceptibility, it is recommended to keep **α** not higher than 0.05 at the first level of decomposition. This value almost doubles when moving to higher levels of decomposition. That's it, at level two, **α** can be up to 0.1 and up to 0.2 in level three.

Although the above experiments were carried out using *Haar* transform, they were repeated with different wavelet families. The results confirmed with the previous profile for each wavelet family separately. To spot out the differences, the performance of the proposed method was tested using various wavelet families at the recommended values of ***α.*** The results are listed in table1. In this table, we highlight the differences not only in imperceptibility, but also in the similarity of the extracting images without any attacks. It is noticed that although the *haar* transform provides a slightly lower imperceptibility, it provides the best retrieval quality of the embedded image.

4.3 Robustness Against JPEG Lossy 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 recommended values of ***α.*** Figure 5 shows the extracted results from JPEG-compressed versions of the watermarked images at different compression ratios. The results showed that the quality of the extracted watermark image is still in a good situation, even under the high compression ratio. Obviously, the higher the level of wavelet decomposition the more robust the algorithm against such an attack. Specially, at three levels of decomposition, the extracted image and the original one are of high correlation. In the proposed method, the error rate of the extracted messages did not exceed 0.3% even under the situation of compression ratio 50%.

Once more, the *Haar* wavelet outperforms the other wavelets in terms of robustness. Figure 6 shows that at the third level of decomposition, the *Haar* wavelet kept a steady performance allowing almost perfect recovery of the embedded image even at very high compression ratios. *Daubechies*, *Symlets*, and *ReverseBior* wavelelts showed a relatively similar performance. However, it is not recommended to employ either *BiorSplines* or *Coiflets* wavelets.

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. These attacks include image filtering and noise addition. For convolution filtering: image blurring with 3x3 Gaussian low-pass filtering, sharpening with low-pass filtering and median filtering. With respect to the random-noise adding attack, the watermarked images are attachked with random noise of mean=0, variance=0.05 and pepper & salt noise of density=0.05. Table 2 both shows the extracted watermark images and the WPSNR of the wateramrked images after each attack. The WPSNR gives an indication of the corruption caused by the attack. Usually, when the WPSNR value is lower than 40, the attack becomes obviously visible and hence, the probability of message corruption becomes very high. The results demonstrate that the proposed scheme is robust enough against all of these attacks even with high watermarked image corruption.

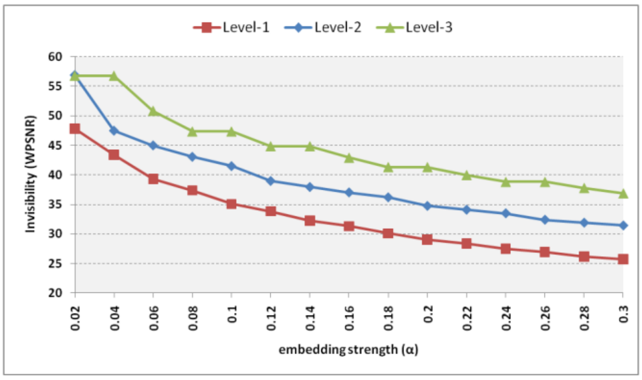


Figure 4: Invisibility Performance of proposed algorithm using multi-level Haar with varying (α)

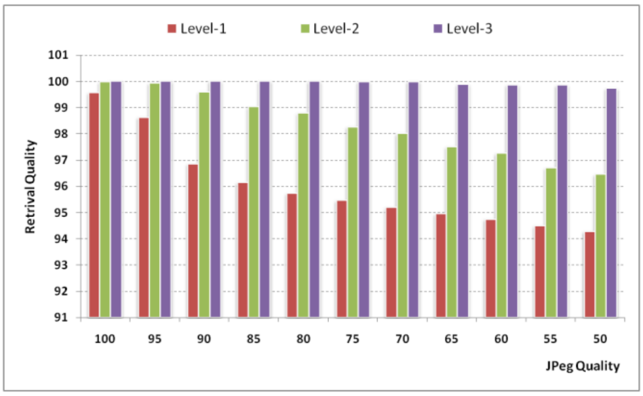


Figure 5: Performance of proposed algorithm against JPEG compression using multi-level Haar wavelet

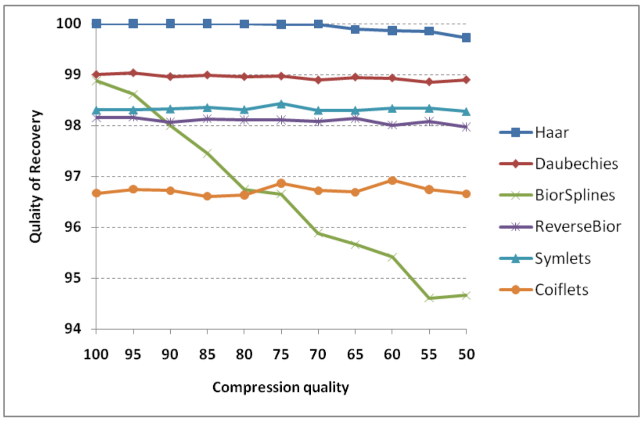


Figure 6: Comparison of Robustness against JPEG compression between different Wavelet Families at three-level wavelet decomposition with fixed embedding

Table 2: Extracted watermark images and their similarity measures under different image attacks

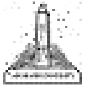
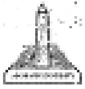
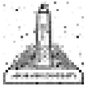
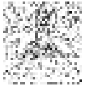
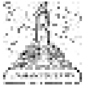
Image operation	Blur	Sharpen	Median Filter	Random Noise	Pepper & salt noise
WPSNR after attack	41.29 dB	35.06 dB	38.02 dB	31.95 dB	35.63 dB
Extracted watermark					
Similarity	99.6936	99.7868	99.6161	95.2474	98.2521

Table 3: Comparison of performance with other transform-domain methods

Method	*Type of Transform*	*PSNR (dB)*	*Payload (bit/pixel)*	*Robust?*
Chang et al. 2007 [6]	DCT	30.34	0.14	No
Lin et al. 2010 [7]	DCT	35.28	0.344	No
Tolba et al. 2005 [9]	IWT (**N=1**)	58.4032	3	No
Lee et al. 2007 [17]	IWT	44	0.6	No
Cheddad et al. 2009 [12]	DWT, 1st level	49.89	0.25	yes
Wua et al. 2010 [12]	RDWT	45.33	1	yes
Proposed	DWT, 2nd level	44.54	0.375	yes

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 3 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. Three 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, which provided larger payload though. Finally, when compared to [12], the proposed algorithm couldn't outperform its performance in neither payload nor imperceptibility. However, the proposed algorithm achieved better robustness as will be shown shortly in the following set of experiments.

To verify the robustness of our scheme compared with **Wu et al. 2010 [12],** different attacking operations are conducted to the standard 512x512 "Lena" image. Table 4 shows the comparison results based on different JPEG-loss compression ratios. Further attacking operations; such as noise addition, low-pass filtering, and median filtering, were tested as well. The outcomes are listed in table 5. The results showed that the proposed algorithm provided better robustness against Jpeg compression for compression ratios less than 50%. However, with higher compression ratios, *Wu et al's* scheme provided a slightly better retrieval rate. On the other hand, the proposed algorithm provided much better robustness against image processing operations, as indicated by the similarity values of listed in table 5.

Table 4: Comparison of robustness against Jpeg Compression with another Wavelet-based method

Jpeg Quality	Proposed	Wu et al. 2010
95%	100	99.99
85%	99.99	99.93
75%	99.86	99.63
65%	99.38	99.19
55%	98.77	98.52
45%	97.91	98.45
35%	96.03	98.74
25%	90.52	97.68

Table 5: Comparison of robustness against Image operations with another Wavelet-based method

Attacking operation	Proposed	Wu et al. 2010
Gaussian low-pass filter (3x3)	99.9999	99.97
high-pass filter (3x3)	96.9214	94.16
5x5 Median filter	99.227	98.39
Random Noise (*mean=0, var= 0.05*)	79.7271	53.87
Pepper & salt noise (*density = 0.05*)	89.8831	88.67

6. CONCLUSIONS

Watermarking is gaining more attention as it conceals the very existing of copyright information and hence protects the intellectual property from illegal usage. In this paper, we proposed a robust and secure image watermarking algorithm that embeds binary watermark in the multi-level wavelet transform of colored images. The algorithm is non-blind since the original image is needed to correctly retrieve the embedded watermark and hence can be used for authentication of ownership. The proposed scheme provides very high payloads and imperceptibility when compared to similar transform-domain techniques. Furthermore, experimental results showed that the proposed algorithm can achieve excellent robustness against attacks such as compression, image filtering, as well as noise addition. This makes the algorithm.

7. REFERENCES

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

[2] R. Anderson, R. Needham, A. Shamir, "The Steganographic File System", *In Proc. the International Information hiding Workshop*, 1998, pp. 43-60.

[3] Considerations in the design of stegtunnel, http://www.synacklabs.net/projects/stegtunnel/

[4] K. Rama , K. Thilagam , S. Manju Priya, A.Jeevarathinam, K .Lakshmi. "Survey and Analysis Of 3D Steganography". *International Journal of Engineering Science and Technology (IJEST)*, Vol. 3(1), pp.638-643, Jan 2011.

[5] H. Dominik, P. Martin, B. Angelika. "DNA watermarks in non-coding regulatory sequences". *BMC Res Notes,* 2: 125, 2009.

[6] Chang, C.C., Lin, C.C., Tseng, C.S. & Tai, W.L., "Reversible hiding in DCT-based compressed images". *Information Sciences*, 177(13), pp. 2768-86, 2007.

[7] Chia-Chen Lin, Pei-Feng Shiu, "High Capacity Data Hiding Scheme for DCT-based Images", *Journal of Information Hiding and Multimedia Signal Processing, Vol.* 1(3), p.p. 220-240, July 2010.

[8] A.Cheddad, J.Condell, K.Curran, P.Mc Kevitt, "A skin tone detection algorithm for an adaptive approach to steganography". *Signal Processing*, Vol. 89(12), pp.2465-78, 2009.

[9] M. F. Tolba, M. Ghonemy, I. Taha, A. Khalifa ,High Capacity Image Steganography using Wavelet-Based Fusion, *in proceedings of The Ninth IEEE Symposium On Computers And Communications (ISCC'2004)*, Alex-Egypt, June 2004, p.p. 430-435.

[10] X. You; L. Du; Y. Cheung; Q. Chen, "A Blind Watermarking Scheme Using New Non-Tensor Product Wavelet Filter Banks". *IEEE Transactions On Image Processing*, Vol. 19(12), pp. 3271 – 3284, 2010.

[11] F. Kammoun, A. Khalfallah, M. Bouhlel, "New scheme of digital watermarking using an adaptive embedding strength applied on multiresolution filed by 9/7 wavelet". *the International Journal of Imaging Systems and Technology*, Vol.16(6), pp. 249–257, 2006.

[12] C.C. Wua, Y. Sub, T. Tuc, C. Changa, S. Li, "Saturation Adjustment Scheme of Blind Color Watermarking for Secret Text Hiding". *Journal Of Multimedia*, Vol. 5, No. 3, P.P.248-258, June 2010.

[13] S. C. Tamane, R. R. Manza and R. R. Deshmukh, B. Ambedkar, "Digital Watermarking using Image Fusion Method". *International Journal of Recent Trends in Engineering*, Vol. 1, No. 2, pp.113-116, May 2009.

[14] S. Tripathi, N. Ramesh, A. Bernito, K.J. Neeraj, "A DWT based Dual Image Watermarking Technique for Authenticity and Watermark Protection". *Signal & Image Processing : An International Journal(SIPIJ)*, Vol.1, No.2, pp.33-45, December 2010.

[15] K. Navas, M. Sasikumar, "Image Fidelity Metrics: Future Directions", *IETE Technical Review*, Vol. 28(1), pp. 50-56, 2011,.

[16] S. Katzenbeisser,. "Principles of steganography". In *Information hiding techniques for steganography and digital watermarking. Norwood*: Katzenbeisser, S. & Petitcolas, F.A.P. Ed. Artech House, INC, 2000.

[17] Lee, S., Yoo, C.D. & Kalker, T., Reversible image watermarking based on integer-to-integer wavelet transform. IEEE Transactions on Information Forensics and Security, 2007, 2(3), pp.321-30.