

## Secure and Non-Blind Watermarking Scheme for Color Images Based on DWT

G.S.El-Taweel, H.M. Onsi, M.Samy, M.G. Darwish

Faculty of computer and information, Cairo University, Giza, Egypt

[ghada\\_el11@hotmail.com](mailto:ghada_el11@hotmail.com)

### Abstract

This paper represents secure watermarking scheme for color images, providing robustness against a set of attacks. Firstly, the image is transformed using an appropriate color transformation. Next each of color channels is transformed through Discrete Wavelet Transform (DWT) and then the Discrete Hadamard Transform (DHT) is applied. By this cascaded transformation, we are in a position to select the most appropriate coefficients, which are close to the low and middle frequencies and uncorrelated in nature. Higher level of security is achieved by introducing encryption among the selected transformed coefficients using a private encryption key. Secondly, we propose non-blind detection scheme. Original image is mandatory, which is based on other widely known watermark detection techniques, but has some modifications. The results are two-stages, multi-resolution watermark decoder that allows efficient identification of the embedded watermarking key without prior notice. The scheme is tested against a variety of legitimate and illicit image processing operations including compression, uniform and Gaussian noise addition, median filtering, cropping and Stir Mark Benchmark. The results presented in this paper are quite convincing and truly demonstrate the robustness of our watermarking method to fundamental image processing operations.

**Keyword** *Image Watermarking, Hadamard, Multi resolution, Non-blind detection.*

### 1. Introduction

The rapid expansion of the Internet and the overall development of digital technologies in the past years have sharply increased the availability of digital media. Digital contents can be reproduced without loss of quality, but they may also be easily modified, and

sometimes imperceptibly. In many contexts, any alteration of image, video and audio must be detected. Therefore, some work needs to be done to develop security systems to protect the content of digital data. Watermarking is accepted as a plausible candidate such an application as it allows for the invisible insertion of information in a host by its imperceptible modification. The most important characteristic of Watermarking is its imperceptibility and robustness. Digital Watermark is a short sequence of information which consists of owner's identify or copyright information added in a way that it is difficult to erase.

Image Watermarking techniques proposed so far can be divided into two categories according to the processing domain of the host image that the Watermark is embedded in. One is to modify the intensity values of the luminance in the spatial domain [2-3]. The other is to change the image coefficients in the frequency domain [4-6]. The frequency domain approaches are the most successful for Image Watermarking. The DCT (Discrete Cosine Transform), the DWT (Discrete Wavelet Transform), the DFT (Discrete Fourier transform) and the DHT (Discrete Hadamard Transform) are employed in most of the Watermarking techniques. Jung and Mitra have introduced the sub band-DCT [10]. It is a method that involves both the DWT and the DCT. [7-9]. In the present work we use the DHT instead of the DCT thus achieving better robustness for Watermarking.

This paper is organized as follows proposed watermarking scheme is presented in section 2. The results of the conducted experiments are illustrated in section 3 and conclusions are in section 4.

### 2. Proposed Watermarking Scheme

In Watermarking system design, the first step to be considered is the embedding of the watermark. Traditionally the watermark should not be placed in perceptually insignificant regions of the image (spatial) or its frequency spectra [7]. The reason is that many signal and



geometrical processes affect these components. A watermark placed in the high frequency spectrum of an image can be easily destroyed with little degradation by direct or indirect low-pass filtering. On the other hand the low-pass components of an image should not be altered for two reasons. First as most of the image energy is concentrated in the low frequency components, any appreciable change may cause fidelity loss. Secondly, the energy of these low frequency components could be considered as noise and thus subtracted, in the case that the original image is available (non-blind watermarking). But in the absence of the original image (blind watermarking), the image noise creates great concern during the detection phase. One of the solutions to this problem is to apply matched filtering before correlation. This decreases the contribution of the original to the correlation [14], or to select low to middle level of coefficients. In our scheme each component of color space is considered as an independent communication channel and the Watermark as a narrow band signal, communicated over larger bandwidth signals. In the present scheme, the watermark sequence consists of real numbers generated by a pseudo random number generator with private key K2. Each value  $w_i$  is drawn from a normal distribution with  $N(0,1)$  i.e. with zero mean and variance equal to one. Pseudo Random generator makes the watermark difficult for an attacker to estimate it from marked media and even if the attacker can estimate some segments of the watermark, it is not possible to determine the rest of the watermark.

## 2.1 Watermark Embedding

In the proposed approach, the embedded watermark must be invisible to human eyes and robust to most image processing operations, first we transform the color image by YUV color transformations, thus decreasing the correlation among the three channels. Each channel is considered as an independent image, candidate for Watermarking. Lowest and medium frequency are selected for further processing. The next step is to de-correlate the components of the frequency band. The DHT is applied for this purpose. The next operation is to add a Pseudo-Random sequence N. In fact a Gaussian distribution is used with mean zero and variance one, to the coefficients of the medium and low frequency bands. The normal distribution is used because it has been proven quite robust to attack. The following formula is used for insertion:

$$\tilde{Y}[m,n] = Y[m,n] + \alpha \text{abs}(Y[m,n], W[m,n]) \quad (1)$$

Where  $y$  is a transform coefficient,  $\hat{y}$  is the corresponding watermarked coefficient and  $w_k$  is the watermark element, the parameter  $\alpha$  is to control the level of watermark. Then the inverse of Hadamard transform is computed and finally the 2D inverse wavelet transform of  $Y$  is computed to form the watermarked image

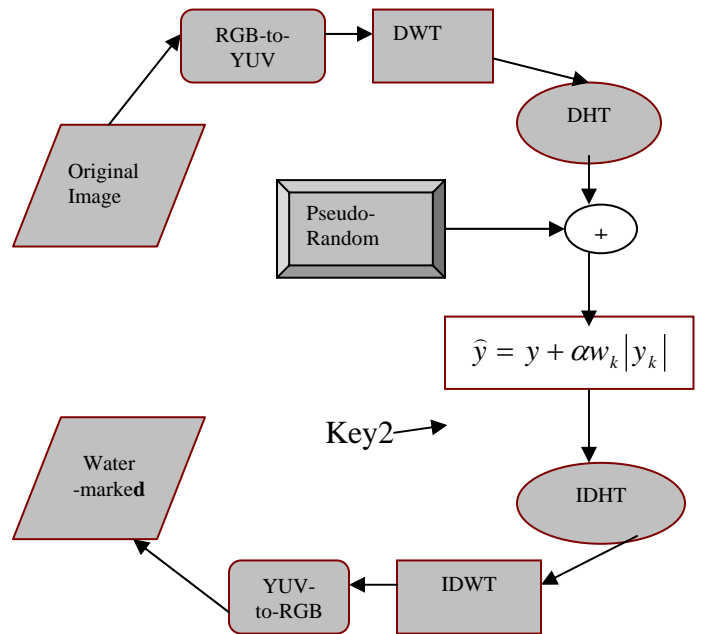


Fig.1 Watermark-Embedding Flowchart

## 2.2 Watermark Decoder

A decoder is used to extract the watermarked information from the received image. Upon reception of the supposedly watermarked image. Firstly, the watermarked and the original image are decomposed each of them into three channels with the same color transform applied during the embedding. Then the algorithm isolates the signature included in this image by comparing the DWT coefficients of the watermarked image with those of the original (non-watermarked) one. We have assumed the specific watermarking key is part of a bank of known key (e.g. a database of copyright owners). Using a method closely related to the one introduced by Cox et al [2] but mainly derived from the paper by Inoue et al [10], we compared the found signature with the ones of the bank by correlating them. Then, as decision is made on the threshold method from [10]. The threshold allows the identification of one and only one possible key that could be the one found in the received image. The threshold computation is based on the value of the wavelet coefficient of the original image and can be written as follow:

$$T = \frac{\alpha}{2NM} \sum_{n=1}^N \sum_{m=1}^M |Y[m,n]| \quad (2)$$

The result of each correlation is compared with that threshold to detect one matching key that will then be used in the second detection stage. The following operation consists of taking the identified key to put in contrast with the found signature by computing the cross



correlation at the first resolution level. The watermarked is detected if there is a peak in the cross correlation corresponding to a positive identification. If there is no central peak, the decoder adds the second resolution level to the computation aiming at finding for a peak. Once again, if there is a peak, the watermark is called detected and if not, we go to the third resolution... and so on until we reach the ninth resolution limit.

The main advantage of our technique is that while allowing good detection, even in the presence of corruption, first, by using the first step, *i.e.* the comparison with a bank of keys, the watermark can be identified without prior knowledge of it. This is a main advantage over the technique proposed by Xia *et al.* since we do not need to consider only one watermark possibly present in the received image. Then the second step aims at ensuring the maximum exactitude in the detection of the owner identification key. It is thus an interesting complement to methods like the ones in [2] and [10] proposed earlier. All that has been said means that the first stage asks: "Is there any key that could be the one we are looking for?" and the second one then asks: "Is this identified key close enough to the one extracted from the received image?". The results presented later on should convince the reader of the performance of our decoder.

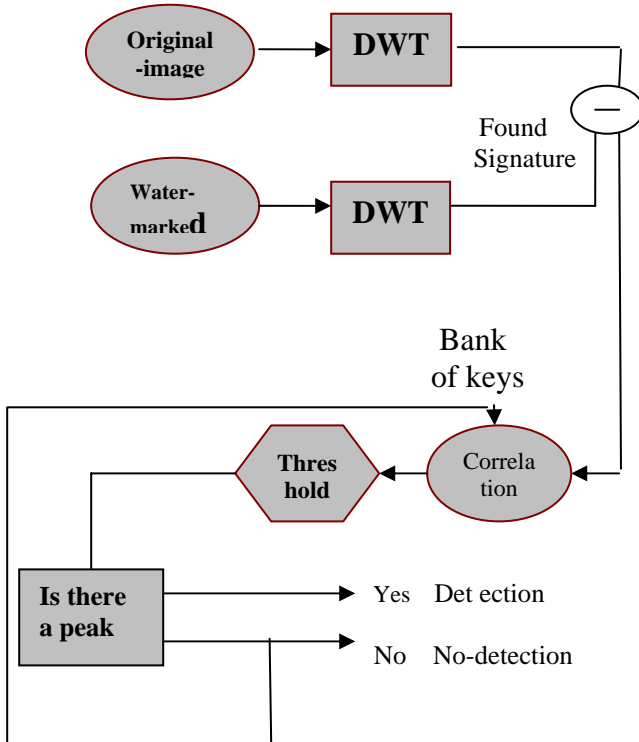


Fig.2 Watermark-Detection Flow-chart

### 3. Experimental results

To evaluate the performance of the proposed watermarking scheme experiments were conducted using

the Lena and paper (256x 256) images and the results were compared with ox's and Shoemaker methods.

### 3.1 Robustness Test

We have focused on the result of attacks due to widely spread image processing operations and geometric distortion operations including uniform-noise,compression, gaussian-noise,filtering (Low-pass,average), cropping. By doing so, we wanted to make sure that our system could be used in the transmission of images. We present some of the results obtained for those different images and attacks in order to summarize the contribution of our paper.

#### 3.1.1 Results of the Scheme:

If there is no central peak, the decoder adds the second resolution level to the computation aiming at finding for a peak. Once again, if there is a peak, the watermark is called detected and if not, we go to the third resolution... and so on until we reach the ninth resolution limit.

The main advantage of our technique is that while allowing good detection, even in the presence of corruption, first, by using the first step, *i.e.* the comparison with a bank of keys, the watermark can be identified without prior knowledge of it. This is a main advantage over the technique proposed by Xia *et al.* since we do not need to consider only one watermark possibly present in the received image. Then the second step aims at ensuring the maximum exactitude in the detection of the owner identification key. It is thus an interesting complement to methods like the ones in [2] and [10] proposed earlier. All that has been said means that the first stage asks: "Is there any key that could be the one we are looking for?" and the second one then asks: "Is this identified key close enough to the one extracted from the received image?". The results presented later on should convince the reader of the performance of our decoder.



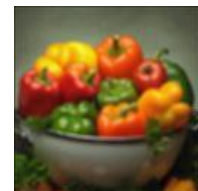
(a)Original Peppers



(b) Peppers-watermarked



(c)Difference



(d) Average filtering



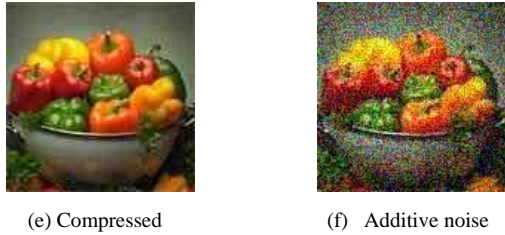


Figure 3 (a) original Pepper image which is the second test image,(b) the corresponding watermarked image ,(c) is the difference between (a) and (b)., (d) is the Average Filtering, (e) is the Compressed watermarked image, and (f) is the Additive-Noise of watermarked image.

### 3.1.2 Evaluation of the Scheme (Lena Image)

The first step involve in the production of results was to create a watermarked image from the original one. It can be seen in the following figure, the two images are quite similar.



Figure 4. a) Original image; b) Watermarked Lena image; c) difference between original and watermarked images

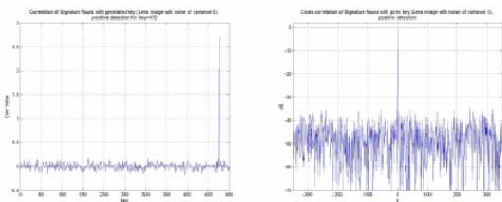


Figure 5 Two stage detection for the uncorrupted Lena image

Then, we have used the uncorrupted watermarked image for detection in order to obtain some reference results. In the first case, for the correlation with the bank of keys, we try to determine if there is any key similar to the one found in the image by looking for a major peak in the correlation value, which is above the predetermined threshold. Then, in the second stage, the cross correlation computation, we verify if the central peak is at least 8 dB above (i.e. six times as important) the second largest peak. If so, the key identified in stage one is acknowledged as being the one we are looking for. Based on those observations, the results are quite explicit; the first stage identifies key 476 as a possible match, while the second stage confirms it.

The second step of the utilization of the Lena image was designed to investigate the impact of noise in watermark detection. We have added additive white Gaussian noise of variance 25 to the previously shown watermarked Lena image. Then, we have used the implemented decoder to identify the present identification key.

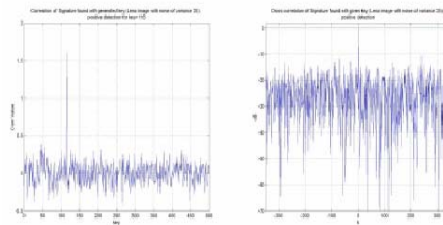


Figure 6 Two stage detection for the noisy Lena image

Even though the received image is perceptually corrupted, the first stage of the decoder is still able to select a key (here 116)7 as a possible match with the found one. The central peak obtained in the second stage is important enough to conclude that the identified key is the one we are looking for. It means that our decoder is able to detect, upon the reception of the data. Consequently, the robustness requirement is met.

To conclude this sub-section, we must point out the fact that robustness testing is a really important part of the design of watermarking scheme and a lot of efforts have to be made in order to standardize this process. In fact, as stated by Petitcolas [5], the absence of a widely accepted testing procedure is probably one of the major factors preventing a faster spread of the utilization of digital watermark. It is agreed that common testing benchmarks (not only for robustness) are needed in order to make sure that specific watermarking schemes fulfill the requirements needed for a certain application. This is certainly also needed to guarantee a secure and efficient use of the powerful tools of digital watermarking technologies. Finally, it is thought that such a scheme, which might standardize the different systems, would eventually speed up the acceptance of its utilization in different key applications.

### 3.2 Quality Measures

We have also used the quality measures PSNR “Peak Signal to Noise Ratio” and CQ “Quality Correlation” to test the performance of the proposed algorithm which is compared with other known techniques like Cox’s and



Shoemaker methods. In Table1-2, by comparing the PSNR of the distorted watermarked images of our scheme with other techniques, we have found that our scheme is better and more efficient than others are. In addition, we found that PSNR of the watermarked image to the original image of the proposed scheme is higher than other methods

Table 1:

Evaluation of the proposed algorithm against different Image processing distortions applying YUV color Transform

Test Lena Image	PSNR (db) of Water-marked Image	PSNR (db) after JPEG	PSNR (db) after Median Filter
Proposed-Scheme	51.0155	54.2251	20.998
Cox's - Scheme	49.8162	53.001	21.001
Shoemaker-Scheme	27.4622	53.4624	20.780

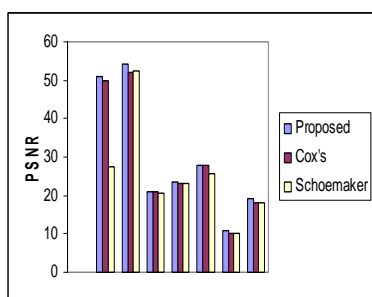


Figure 7. the PSNR of the proposed scheme and other techniques.

#### 4. Conclusion

In this paper, we have presented a multi-resolution watermarking method based on Haar- wavelet transform. We have seen how it is possible to embed some information within the middle and low frequency bands of the cascade transformation in an unperceivable way for the HVS but detectable by our two-stage decoder, thus providing copyright protection capabilities. We have then demonstrated that our system is fully robust to basic image processing operations such as noise addition "Gaussian or uniform", compression, half toning and different kind of filtering. By using different quality measures, we have proven that our proposed scheme is more efficient than other techniques like here by Cox's and Shoemaker. Furthermore, with the choice of different embedding parameters, we have seen that a tradeoff between robustness and transparency can be achieved. This flexibility, since it allows adaptation of the system to a

particular application is certainly a great advantage of our technique and would make it a potential candidate for more advanced watermarking schemes.

#### 5. Reference

- [1] Xiang-Gen Xia, C.G. Boncelet and G.R. Arce, A Multiresolution Watermark for digital images, *Proc. of International Conference on Image Processing*, vol. 3, pp.548-51, 1997.
- [2] M.Kutter, F Jordan, and F. Bossen, "Digital signature of Color Images Using Amplitude Modulation," in *Proc. SPIE Electronic Imaging 97, Storage and Retrieval for Image and Video Databases V*, pp. 518-526, San Jose,CA, Feb, 1997.
- [3] A. Nikolaidis, I. Pitas, "A Region-Based Technique For Chaotic Image Watermarking," *EUSIPCO 2000*, vol. II, Tampere, Finland, Sept. 4-8, 2000.
- [4] I.Cox, J.Kilian, F.Thomson Leigton and T.Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Trans. On Image Processing*, vol.6, no.12, Dec. 1997.
- [5] Fotopoulos,V., Krommydas,S. and Skodras,A.N., "Gabor Transform Domain Watermarking", *Proc. IEEE Int. Conf. on Image Processing (ICIP 2001)*, Thessaloniki, Greece,Oct. 7-10, 2001.
- [6] S.A.M.Gilani and A.N.Skodras, "DLT-Based Digital Image Watermarking", *First IEEE Balkan Conference on Signal Processing, Communications, Circuits and Systems*, Istanbul, Turkey, June 2-3, 2000.
- [7] S.H.Jung, S.K.Mitra, "Subband DCT: Definition, Analysis, and Applications", *IEEE Trans. Circuits and Systems for Video Technology*, vol.6, no3, June 1996.
- [8] G.C. Langelaar, I. Setyawan and R.L. Lagendijk, "Watermarking Digital Image and Video Data; A state of The Art Overview," *IEEE Signal Processing Magazine*, pp. 20-46, Sept. 2003.
- [9] S. J. Sangwine, "Colour in Image Processing", *Electronics & Communication Engineering Journal*, pp. 211-219, Oct. 2000.
- [10] S. Katzenbeisser, and A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking," *Artech House, Inc.*, 2000.
- [11] I. J. Cox, M. L. Miller, J. A. Bloom, "Digital Watermarking", *Academic Press* 2002.
- [12] <http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/index>

