International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 06, Issue 05, May 2017, ISSN: 2278 -7798

WATERMARKING ALGORITHM BASED ON DISCRETE WAVELET TRANSFORM USING TWO TYPES OF IMAGES

Asst. Lect. Heba Abdul-Jaleel Alasadi

Abstract— In the recent years, the fast growth of Internet, wireless networks and the revolution of digital multimedia technology have brought significant changes in our lives. It has made it possible to transmit and share multimedia date fast and easily. However, these developments have created problems of a copyright protection, security and authentication of the original data. The digital watermarking is one of the popular techniques proposed to protect the copyright and to prove the ownership of digital data. In this paper; the proposed algorithm is built under MATLAB environment and it is tested using two different images. The experimental results stated that the proposed algorithm work well for both types of images and get maximum advantages of this transform in watermarking to extract the hiding image efficiently.

Index Terms—watermarking, wavelet, transform, algorithm

1) INTRODUCTION

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself [1]. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Digital watermarking is the practice of embedding a secret information into the original data imperceptibly [2]. The watermark is inserted in such a Manner that it should be resistant to all types of intentional or unintentional attacks as long as the perceptual quality of the original data is at an acceptable height. To prove the ownership a reverse process called watermark detection is used [3] as shown in figure (1). In watermark detection process the embedded watermark is extracted from the watermarked data to prove the ownership [4]. The processor watermarking brings some distortion to the cover media. This intentional distortion is called marks, and all the marks are combined to form the watermark.The marks are inserted in such a way so that they have an insignificant impact on the usefulness of the cover media and are placed in manner so that a malicious attacker cannot demolish the remarks without making the data considerably less useful [5].

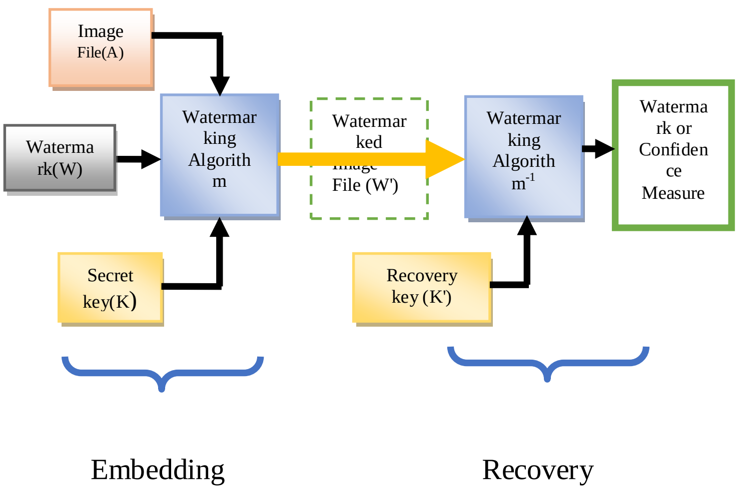


Figure (1): Basic watermarking system

2) WAVELETS

A wave is a periodic oscillating disturbance that propagates through space and time, usually with transference of energy [6]. The word wavelet literally means “little wave” and is attributed to Morlet and Grossmann in the early 1980s [6 and 7]. They used the word onde- lette; the French word was Anglicized by translating “onde” into “wave”, giving “wavelet”. The “-lette“ or “-let“ suffix generally means petite [7]. The wavelet is called a “let”, or little, because the wavelet function is of finite length [8].There are two types of the wavelet transforms. These types may differ according to the application. For example, some wavelet transforms act in manner which divides a signal into those components which are significant in time and space, and those that contribute less. This feature enables wavelets tube very useful in applications such as noise removal, edge detection and data compression [8 and 9].The other type is the Discrete Wavelet Transform (DWT) which is used in this paper. The main aim of the using DWT is that to decompose the discrete time signal into basis functions to give a good analytic view of the analyzed signal. However, these basis function are called the wavelets [9]. The behavior of the DWT is governed by the choice of the filters [10]. The DWT decomposes a signal into the coarse approximation and detailed information. It employs two sets of functions, called scaling functions and wavelet functions, which are associated with low pass h[n] and high-pass g[n] filters, respectively. The decomposition process into different frequency bands is obtained by the filter banks composed of the successive high-pass and low-pass filters respectively [10]. At each level of the decomposition, the signal is split into high frequency and low frequency components, and the low-frequency components can be further decomposed until the desired resolution is reached [11]. The natural way to discretize the scaling variable s is in a logarithmic manner $\left(s = s_0^{-j}\right)$ and to use Nyquist sampling rule, based on the spectrum of function *x(t)*, to discretize τ at any given scale $\left(\tau = k\, s_0^{-j}\, T\right)$. The resultant wavelet functions are then as follows [12]:

$$\Psi_{j,k}(t) = s_0^{j/2}\ \Psi\left(s_0^j t - k\tau_0\right) \tag{1}$$

Generally $s_0 = 2$, so the computation is done octave by octave. So the mother wavelet, represented by $\Psi(t)$, yields following two-dimensional parameterization of $\Psi_{j,k}(t)$.

$$\Psi_{j,k}(t) = 2^{j/2}\,\Psi\left(2^j t - k\right) \tag{2}$$

The $2^{j/2}$ factor in equation (2) normalizes each wavelet to maintain a constant norm independent of scale j. In this case, the discretizing period in τ is normalized to one and is assumed that it is the same as the sampling period of the discrete signal $\left(\tau = k\, 2^{-j}\right)$. The lower resolution function, $\Phi(t)$, can be expressed by a weighted sum of shifted version of the same scaling function at the next higher resolution, $\Phi(2t)$, as follows[13]:

$$\Phi(t) = \sum_k h(k)\sqrt{2}\ \Phi(2t-k) \tag{3}$$

The set of coefficients $h(k)$ being the scaling function coefficients and $\sqrt{2}$ maintain the norm of the scaling function with scale of two [12 and 13]. The important features of a signal can better be described or parameterized, not by using $\Phi_{j,k}(t)$ and increasing j to increase the size of the subspace spanned by the scaling functions, but by defining a slightly different set of functions $\Psi_{j,k}(t)$ that span the differences between the spaces spanned by the various scales of the scaling function. So similarly to equation (3), $\Psi(t)$ will be:

$$\Psi(t) = \sum_k g(k)\sqrt{2}\ \Phi(2t-k) \tag{4}$$

The set of coefficients $g(k)$'s is called the wavelet function coefficients or the wavelet filter. It is shown that the wavelet coefficients are required by orthogonality to be related to the scaling function coefficients by [13]:

$$g(k) = (-1)^k h(1-k) \tag{5}$$

The operation of 1-level discrete wavelet transform decomposition is to separate high pass and low pass components of x[n]. Thus, process involves passing the time-domain signal *x*[*n*] through a high pass filter *g0*[*n*] and down sampling the signal obtained yields detailed coefficients (D). And, passing *x*[*n*] through low pass filters *h0* [*n*]and down sampling generated approximate coefficients (A)[14]. The working principle is shown in Figure (2).

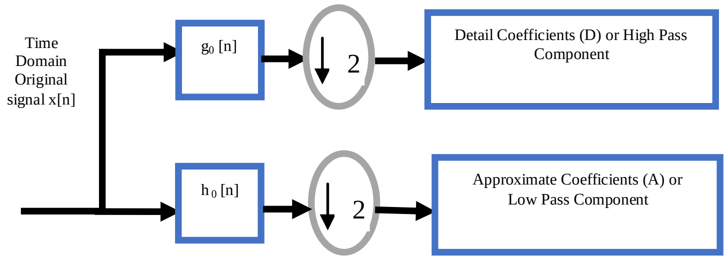


Figure (2): Single level analysis the signal in DWT.

3) THE PROPOSED WATERMARKING ALGORITHM IN IMAGE USING DWT

In this section, we discuss some motivating factors in the design of our approach to image watermarking scheme. The proposed system consist of two main parts: Embedding algorithm and extraction algorithm as follows.

3.1- EMBEDDING ALGORITHM

The block diagram of the embedding algorithm is shown in Figure (3)

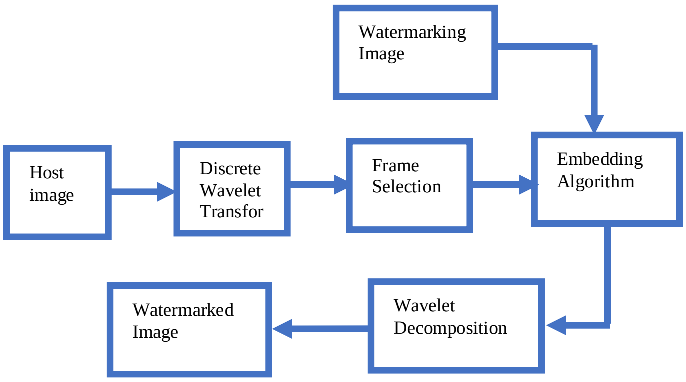


Figure (3): Embedding procedure block diagram

The embedding process can be described in the following steps:

a) Read the original image of size N*N which is 256×256 and convert it to gray.

b) Read the watermarking image and convert it to gray-level of size 64*64.

c) Apply the DWT on each color of image to extract the wavelet coefficients which are the approximation coefficients matrix (ca) & details coefficients matrices (cd).

d) Select the detail coefficients of the wavelet transforms and embed the encrypted data.

e) Finally, Apply the IDWT to reconstruct the original image which is called watermarked image.

3.2- EXTRACTION PROCEDURE BLOCK DIAGRAM

The block diagram of the Extraction algorithm are shown in Figure (4)

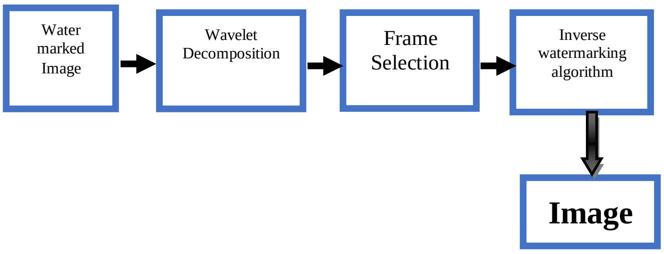


Figure (4): Extraction procedure block diagram.

The extraction process can be described in the following steps:

a) Read the watermarked color image of size N*N which is 256×256 and convert it to gray-level image.

b) Apply the discrete wavelet transform on it to extract the frame of the watermarked image.

c) Select the detail coefficients of the wavelet transforms and take the inverse encryption to extract the gray image and resize it to 64*64.

4) THE EXPERIMENT SETUP, RESULTS AND DISCUSSION

For testing the performance of this algorithm, the experiments is simulated with the software MATLAB. In the following experiments, the colored -level image with size of (256 ×256) pixels is used as host image to embed watermark which is gray-level image with size of (64*64) pixels. The proposed algorithm is tested once with JPG images, and then with PNG images types. The original host images, watermarked images that used in this paper are shown in the figures below:

a) Host image b) Watermarking image c) Extracted image

Figure (4.1) The first experiment for PNG images

a) Host image b) Watermarking image c) Extracted image

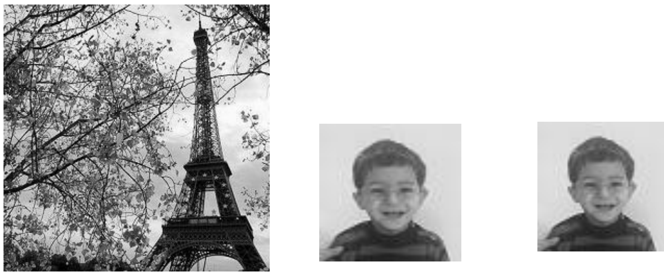
Figure (4.2) The first experiment for JPG images

a) Host image b) Watermarking image c) Extracted image

Figure (5.1) The second experiment for PNG images

a) Host image b) Watermarking image c) Extracted image

Figure (5.2) The second experiment for JPG images



a) Host image b) Watermarking image c) Extracted image

Figure (6.1) The third experiment for PNG images

a) Host image b) Watermarking image c) Extracted image

Figure (6.2) The third experiment for JPG images

The performance of the proposed algorithm is tested once with JPG image, and then with PNG image types as shown in table (1) and (2).

Results images type " PNG"

The subject	First Experiment		Second Experiment		Thread Experiment	
	Hosting	Watermarking	Hosting	Watermarking	Hosting	Watermarking
PSNR (dB)	8080.223	8080.222864	11795	11795.23634	7676.9	6954.409695
RMS (bits)	0.631171	0.63117071	0.4324	0.432377941	0.6643	0.664326694

Table (1) The results of experiments of the type (png)

Results images type "jpg"

The subject	First Experiment		Second Experiment		Thread Experiment	
	Hosting	Watermarking	Hosting	Watermarking	Hosting	Watermarking
PSNR (dB)	619.6667	619.6667263	1258	1258.011316	540.86	500.23877
RMS (bits)	8.230231	8.230230515	4.054	4.054017587	9.3555	9.355532359

Table (2) The results of experiments of the type (jpg)

In this section the effect of embedding algorithm on the cover image is discussed in terms of perceptual similarity between the original image and watermarked image using PSNR, and the RMS values as shown in table (1) and (2), as the equations below:

$$SNR = 10\log_{10}\left(\frac{\sum_{n=1}^{N} x^2(n)}{\sum_{n=1}^{N}(x(n)-x'(n))^2}\right) \quad (6)$$

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[x'(i,j) - x'(i,j)]^2 \quad (7)$$

$$RMS = \sqrt{[MSE]^2} \quad (8)$$

The proposed technique uses the wavelet transformation domains to embed the data so as to exploit the advantages of wavelet Transform being resistant to frequency attacks. We test this algorithm on the cover image in two times: once with the PNG image and last with the JPG image file types. The proposed watermarking algorithm works well. According to table (1) and (2).and by comparing the results in it, we get the max. PSNR for the two images (cover image and embedded image) in each type of image attention. As we comparing these result between the PNG and JPG we find there is an unexpected problem which has happened when using an image of JPG type. There is a difference between the matrices when read the data of image and writing it because JPG is a lossy image compression format, and when saving the image in this type some of information is lost, and the best result when we use the PNG image file types because PNG type is lossless compression mean that don't loss the information in the transmitting and receiving the data of image or in printing. So to get the advantages of wavelet transform to hide the information and to prevent the loss of it when we save the image in PNG format instead of JPG format.

5) CONCLUSION

This paper introduces a digital watermark algorithm based on discrete wavelet Transform (DWT) to embed the data in the high frequency component wavelet transformation domain so as to exploit the advantages of it being resistant to frequency attacks. We test this algorithm on the cover image in two times: once with the PNG image and last with the JPG image file types. As we comparing the results between the PNG and JPG, we see that the wavelet transform work well for both types of images but we can get maximum advantages of this transform in watermarking and extract the hiding information efficiently without any distortion or loss in it, when we used the PNG format of image.

REFERENCES

1- Kaur, Amarjeet, Arti Goel, and Hitender Gupta. "Digital watermarking in neural networks models." Engineering and Computational Sciences (RAECS), 2014 Recent Advances in. IEEE, 2014.

2- Swanson, Mitchell D., Mei Kobayashi, and Ahmed H. Tewfik. "Multimedia data-embedding and watermarking technologies." Proceedings of the IEEE 86.6 (1998): 1064-1087.

3- Sencar, Husrev T., and Nasir Memon. "Watermarking and ownership problem: a revisit." Proceedings of the 5th ACM workshop on Digital rights management. ACM, 2005.

4- Neelima, K. Bramara, and T. Saravanan. "Sample Image Watermarking Study." Indian Journal of Science and Technology 8.31 (2015).

5- Haouzia, Adil, and Rita Noumeir. "Methods for image authentication: a survey." Multimedia tools and applications 39.1 (2008): 1-46.

6- Serway, Raymond, and John Jewett. Physics for scientists and engineers with modern physics. Nelson Education, 2013.

7- Brannock, Evelyn, Michael Weeks, and Robert W. Harrison. "The effect of wavelet families on watermarking." (2009).

8- Polikar, Robi. "The wavelet tutorial." (1996).

9- Nesvijski, Edouard, and M. Marasteanu. "Wavelet transform and its applications to acoustic emission analysis of asphalt cold cracking." E J. NDT12: 1-13 (2007).

10- Shensa, M. J. Discrete Wavelet Transforms: The Relationship of the á trous and Mallat algorithms. NAVAL OCEAN SYSTEMS CENTER SAN DIEGO CA, 1991.

11- Kumar, Mr Arun, Miss Sarita Chokhandre, and Anup Mishra. "Discrete wavelet transform based signal stegnography & encryption." International Journal of Engineering Science and Technology (IJEST) 4.5 (2012): 2417-2420.

12- K. Guo, D. Labate, W.Q. Lim, G. Weiss, and E. Wilson, "Wavelets with Composite Dilations and their MRA properties", Applied and Computational Harmonic Analysis, vol. 20, No.2, pp. 202-236,2006.

13- M. Misiti, Y. Misiti, G. Oppenheim. "Wavbox 4: A software toolbox for wavelet transforms and adaptive wavelet packet decompositions", Wavelets and statistics, Springer New York,vol.7, No.113, pp. 361-375, 1995

14- Valens, Clemens. "A really friendly guide to wavelets." ed. Clemens Valens(1999).

Ass. Lec.: Heba Abdul Jaleel Al-Asadi, Bachelor of Electrical Engineering from Kufa University / Faculty of Engineering / Electrical Engineering Department / Iraq in 2010. And holds a master's degree in electronic engineering and communications from the University of Babylon / Faculty of Engineering / Department of Electrical Engineering / Iraq in 2014. Assistant Lecturer at Islamic University College - Iraq