TJES
ISSN: 1813-162X
Tikrit Journal of Engineering Sciences
available online at: http://www.tj-es.com

Secured Watermarking Image Using Spread Spectrum

Abdulkareem Mohammed Salih
Al-Dour Technical Institute, Salahaldeen, Iraq
E-mail: abdulkreem86@gmail.com

Abstract

Due to the increased development in technique of data transfer over internet and transmission media, the access and copy to these data in unathentical manner became a big challenge in the transmission media. This challenge led to make effort in digital multimedia security.

In this paper a new algorithm is proposed to protect image from unauthentication access using watermarking. The watermarking algorithm hide the mark image in frequency domain using Discrete Cosine Transform and extract it at the receiver from the transmitted image without need for origin image. The basic principle of the algorithm is depend on spread spectrum communications. The spread spectrum depend on transmit a narrow band signal over a much larger bandwidth where that the signal energy is undetectable. Similarly, the watermark image bits are spread by a large factor called chip-rate so that it is imperceptible and arrange in cover image in away where if the half of the watermarked image is cropped, the watermark image is not affected. The proposed algorithm efficiency is measured by using many of measurement factors such as Peak Signal to Noise Ratio PSNR and Normalized Correlation Coefficient NC, the watermark robustness and feasibility are measured by using many types of attacks.

Keywords: Watermarking, Spread Spectrum, Robustness. Security.

العلامة المائية السرية للصور باستخدام انتشار الطيف

الخلاصة

نتيجة للتطورات الحاصلة في تقنيات نقل المعلومات والبيانات عبر الأوساط المتعددة وعلى شبكة الانترنيت أصبح الوصول ونسخ هذه المعلومات والبيانات بأسلوب غير مخول تحدي كبير في وسائط النقل وهذا التحدي أدى الى تظافر الجهود لتطور أمنية الوسائط الرقمية.

في هذا البحث تم اقتراح خوارزمية جديدة لحماية الصور من الوصول غير الشرعي باستخدام العلامة المائية. العلامة المائية هي إخفاء العلامة في حيز التردد باستخدام دالة تحويل الجيب تمام المتقطع واستخلاص العلامة في جهة الاستقبال من الصورة المرسلة دون الحاجة للصورة الأصلية. المبدأ الأساسي للخوارزمية يعتمد على نظرية انتشار الطيف في الاتصالات. في نظرية انتشار الطيف في الاتصالات الإشارة ذات الحزمة الضيقة من التردد ترسل في حيز واسع من التردد بحيث الطاقة الموجودة في الإشارة المرسلة تكون غير مكشوفة، وبطريقة مشابهة النقاط الصورية للعلامة المائية تتوسع بمعامل تكبير يسمى (chip-rate) بذلك تكون غير مكتشفة وتكون مرتبة في الصورة الغطاء بطريقة بحيث أذا تم قطع نصف الصورة المضمنة للعلامة فأن العلامة لا تتأثر. تم قياس كفاءة هذه الخوارزمية بحساب قيم Peak Signal –to-Noise Ratio PSNR ومعامل الارتباط Normalized Correlation Coefficient NC وكذلك استخدام مجموعة من الهجمات لقياس مرونة وصلابة العلامة المائية.

الكلمات الدالة : العلامة المائية، انتشار الطيف، الوثوقية ، السرية.

Symbols

Cr=Chip rates
PSNR= Peak Signal to Noise Ratio
NC=Normal Correlation Coefficient

Introduction

Digital Watermarking can be defined as the process of embedding invisible signal in an image in such a way that intruder is unable to trace the signal to enhance Copyright Protection[1]. Watermarking is a method for encoding visible or invisible watermark image into multimedia data applications. Where the visible watermark is clearly detectable, and it is perceptible to a human observer. Visible watermarking is used to prevent unauthorized access to an image .While the invisible watermarking is used to identify the owner or the origin of the host image[2]. The property of easy in implementation in spatial domain watermarking is obvious from a computational point of view, at the expensive of the resist of numerous attacks. Therefore, to have more promising techniques, researches were directed towards using watermarking in the transform domain, where the watermark is added to the transform coefficients of image instead of image intensities. Then to get the watermarked image, one should perform the transform inversely[3]. The watermarking scheme based on the frequency domains can be further classified into the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) domain methods. The watermark is embedded in transformed coefficients of the image therefore the watermark is invisible and more robust for some image processing operations[4]. Steganographic systems are information hiding science which embed hidden information into a cover content so that it is not noticeable, and watermarking can be considered to be a part of these systems. There are three aspects of information hiding systems contend with each other: capacity, security and robustness. These aspects are used to measure system quality.

Capacity indicate to how many of information that can be hidden and then recovered, security to ability of prevent anyone to discover hidden information and make it imperceptible, and robustness to be invariant to the attacks and stay detectable after attacks are applied. In watermarking, the robustness factor is preferable where should be impossible to remove the watermark without severe quality degradation of the cover content[5]. There are numerous techniques for digital watermarking, Early watermarking schemes worked in the spatial domain, where the watermark is added by modifying pixel values of the host image as in[6]. Perwej[7] focused in his paper on the modification of the least significant bit (LSB) of an image based on the substitution method to encrypt the message in the watermark image file. The transform domain based watermarking techniques are applied and by using Discrete Cosine Transform (DCT) as is the one suggested in[5] . Another type of the transform domain is used based wavelet transform which provide the property of multi-Resolution analysis, many of researcher focus on this property as was mentioned by Dinghui[8]. Some of papers are merge more of transform, where these papers joined between DCT and DWT (Digital Wavelet Transform) which take advantage of the two frequency domains[9].

The main objective of this paper is to present the hiding watermark in cover image using spread spectrum with frequency hopping since much than one frequency are used to embed the watermark in DCT blocks and two secret keys are used for get more security, then the watermark image is extracted at the receiver without need for origin image . The rest of this paper is organized as follows: In section 2 Spread Spectrum Technique For Watermarking explained. Section 3 discusses the Watermark Embedding and Watermark Extraction respectively. Error and Correction Ratio are explained in section 4. In section 5 Simulation Results are discussed. Finally, section 6 concludes the paper.

Spread Spectrum Technique for Watermarking

In general, in the spread spectrum communication technique, the signal reside a bandwidth in excess of the minimum necessary to send the information where the signal energy present in any single frequency is undetectable[10]. The image transformed in

frequency domain can be viewed as the communication channel, and the watermark is considered as a signal that is transmitted through this channel. The noise implemented in the attacks and unintentional signal distortions[11]. This method is used for watermark image insertion and extraction with different frequencies for embeds watermark pixels, this process gives a robustness and security for algorithm.

The Proposed Algorithm

The proposed algorithm consists of two stages. The first stage is watermark embedded which embedded the watermark image in the cover image to contain watermarked image. While the second stage is extracting stage that include extract the watermark from the watermarked image.

Proposed Watermark Embedding

The embedding side in watermarking consist of many stages that sequent as shown:

1- To make some of necessary steps before embedded the watermark image into the cover image, a preprocessing unit is used. In this unit where the sequence of information bits that has to be embedded into the image which referred as the $a_i \in \{-1,1\}$. This sequence is spread by using large factor through the chip-rate (cr), and the spread sequence bi is obtained:

$$b_{(2i+k)}=a_i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Where k={1,2} and i is the index for watermark image pixel value. In this way two copy of watermark image will embedded in the cover image.

2- To give the spread sequence (bi) random form ,It is modulated by using a pseudo noise sequence (pi) to generate the new sequence (Gi),

$$G_i = b_i . p_i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Where $p_i \in \{-1,1\}$, i =1, 2, …, N. The pseudo noise sequence can be generated by random number generator and this generator depend on a secret key (key1) that give the proposed algorithm more security form since nobody can extract the bi signal from the (Gi) at unless used the secret key at extracting side and this key is a number used as input to pseudo function where the output of pseudo function changed and depend on this number. The produced sequence (G_i) is scaled by a scalar α to increase the amplitude as in the equation:

$$W_i = \alpha.G_i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Where W_i is the spread spectrum watermark.

3- After convert the cover image to frequency domain using DCT that is deal with frequencies and a frequency hopping used to choose the frequencies that will embed the sequences of watermark with a second secret key (key2) that used for select frequency hopping as in Equation (4):

$$Ri = Wi \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Where Ri is the modified DCT coefficients and more than one frequency position are used to give algorithm more robustness. At last inverse DCT applied to obtain watermarked image. Figure (1) shows the process of watermark embedded. The flow chart in Figure (2) explains the steps of watermark embedded.

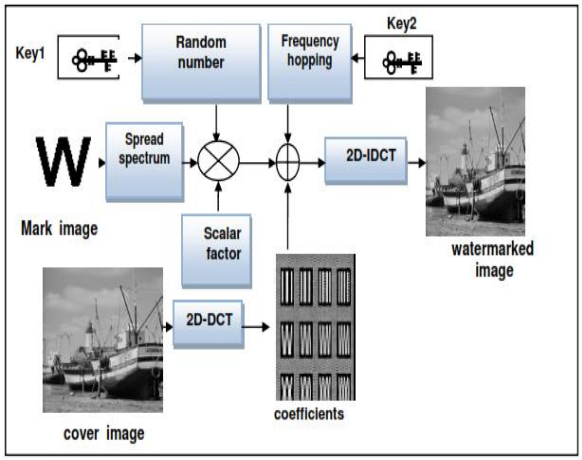


Fig. 1. Watermark Embedded Process

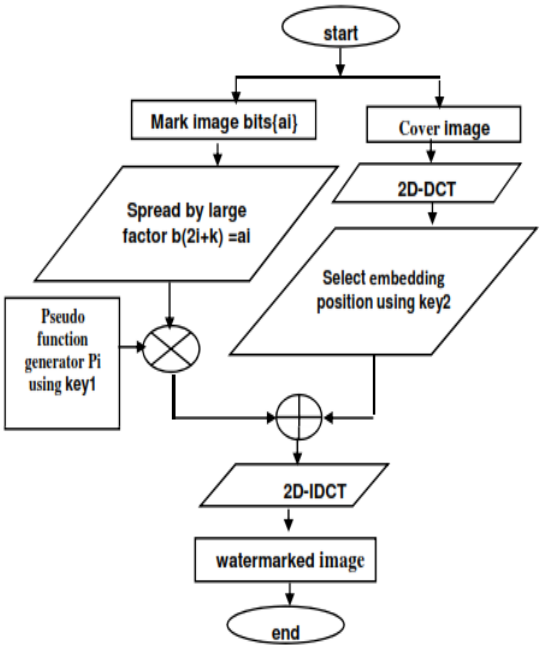


Fig. 2. Flow Chart Explain The Steps Of Watermark Embedded

Secret keys

Two secret keys are used and this keys given the algorithm security. The first key is a number used as input to pseudo function generator while the second key is used to select in any location the mark pixel embedded. These keys should be known by receiver to be able to extract the mark.

Proposed Watermark Extraction

As shown in Figure (3), backward steps are used to recover mark image as explain:

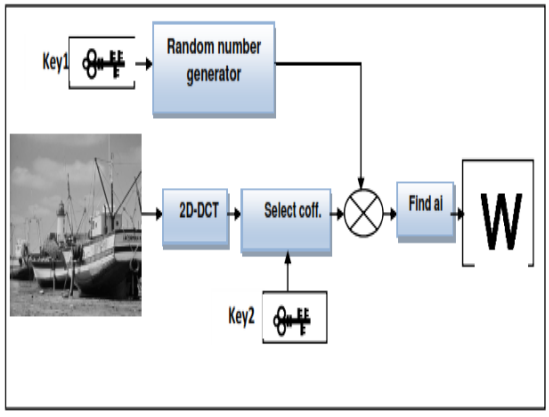


Fig. 3. Watermark Extraction Process

1- Convert the cover image to Frequency domain using the DCT transforms.
2- Select the same coefficients in the embedded process which used to select the position of frequency hopping (key2).
3- This spread spectrum signal is then demodulated with the pseudo-noise signal P_i that is the same as the one used for embedding to obtain bi by using the same number (key1).
4- Find ai which is :

$$ai = b_{2i} + b_{2i+1} \quad \text{.....(5)}$$

Where $(b_{2i} + b_{2i+1})$ are same pixels value and if any of them is destroy by noise the other pixel will keep the same value for watermark image. Then the value of the ai is threshold to '1' or '0' as shown in the flow chart in Figure (4).

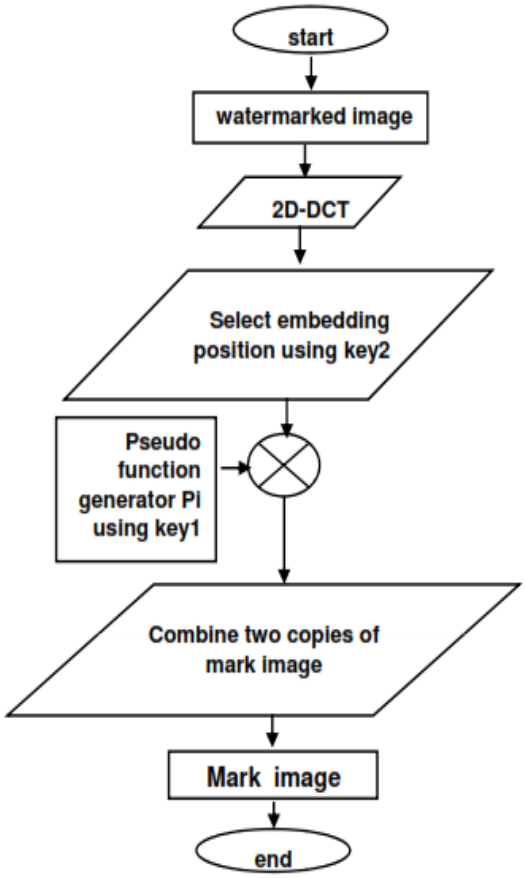


Fig. 4. Flow Chart of Watermark Extraction Process

Error and Correction Ratio

The error ratio between the origin image and the cover image can be calculated by finding the value of Peak Signal to Noise Ratio PSNR[1], as shown:

$$PSNR=10\log_{10} 255^2/RMSE \quad \ldots\ldots\ldots\ldots\ldots\ldots(6)$$

Where the RMSE is root mean square error and equal to :

$$RMSE=\frac{1}{MN}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j)-f(i,j)]^2} \quad \ldots(7)$$

M and N are image dimensions (number of pixels) (M=N). The extracted watermark must be similar to the origin watermark, and the correlation ratio can be calculated by finding the Normalized correlation coefficient NC as in Equation (8):

$$NC=\sum_{i=1}^{M}\sum_{j=1}^{N}w(i,j)w^*(i,j) \;/\; \sum_{i=1}^{M}\sum_{j=1}^{N}w(i,j)^2 \quad \ldots(8)$$

Where w(i,j) and w*(i,j) represent the origin and extracted watermark respectively. The value of NC equal to 1 as maximum value[6][12]**.**

Simulation Results

Three gray images are used for test the algorithm, Boat , Harbour and Lena image which are size of (512x512) pixels used as cover images. Whereas two binary images size (64x64) pixels are used as watermark image. PSNR are calculated for these images as shown in Table (1). Also the NC is calculated for extracted watermark and it was equal to (1).

A watermarked object may be changed or modified by hackers or through transmission media so the watermarking system should still be able to detect and extract the watermark. Watermarked image is subject to various signal processing operations, or attacks, and the watermark detected without using the original image in all of the distortions and attacks as shown in Tables (2) &(3).

Table 1. PSNR for cover images

image	PSNR (db)
Boat 	35.925
Harbour 	35.844
Lena 	35.84

CONCLUSION

This paper presented a watermark algorithm for digital image. The three aspects of information hiding systems capacity, security and robustness are saved or obtained in this algorithm. For the capacity, the size of cover image is (512x512) and size of watermark is ((64x64) x 2) since two copy are embedded, this ratio suitable and no effect on the cover image as shown in value of PSNR. Security to ability of anybody to detect hidden information is improved using two secret keys, first key is a number used as input to pseudo function generator and second is used to select position or index of frequency to embed the mark. Where without these keys nobody can detect the hidden information. Finally the robustness to the resistance to modifications of the cover content before hidden information is destroyed are applied by using more than one technique, where a frequency hopping is used by using much than one frequency to embed the watermark to resistance the effect of filter that destroy the frequencies such as Low Pass Filter or Mean Filter where low and high frequencies are used to embed watermark image, and for resistance the effect of other types of attack such as cut part from image, by using spread spectrum there are two copy of watermark image and everyone is embed in form opposite to other, the first copy

starting embedding from pixel (0,0) to pixel (511,511) and the other copy is embed from pixel (511,511) to pixel (0,0) since if the half part of image is cropped there will be another part contain the pixels of watermark image and no effect on the watermark image as shown in Table (2) and Table (3) respectively. In Table (2) same mark used in different cover images while in Table (3) different mark used in same cover image.

Table 2. NC for extracted watermark image(same mark)

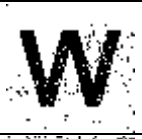
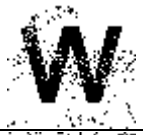
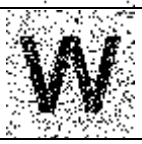
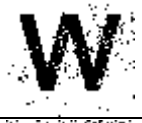
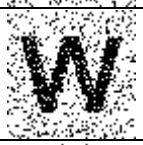
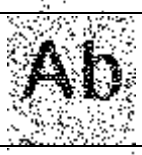
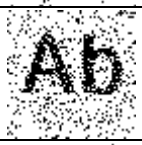
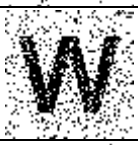
Attacks	Boat image		Harbour image	
	NC	Extracted Watermark image	NC	Extracted Watermark image
Without attack	1		1	
Cut part from image	1		0.999	
LPF	0.9772		0.9624	
Salt and Peppers	0.8999		0.9066	
Mean Filter	0.9797		0.9358	
Gaussian Filter	0.9129		0.9132	
Wiener Filter	0.995		0.9836	

Table 3. NC for extracted watermark image(different mark)

Attacks	Lena image(with mark ab)		Lena image(with mark w)	
	NC	Extracted Watermark image	NC	Extracted Watermark image
Without attack	1		1	
Cut part from image	1		0.999	
LPF	0.9726		0.9620	
Salt and Peppers	0.9142		0.9062	
Mean Filter	0.9759		0.9350	
Gaussian Filter	0.920		0.9130	
Wiener Filter	0.992		0.9831	

References

1- Sharma, C. and Prashar, D. "DWT Based Robust Technique of Watermarking Applied on Digital Images", International Journal of Image, Graphics and Signal Processing (IJIGSP) ISSN: 2074-9074, Vol.2, Issue-2, May 2012.

2- Mohanty, S. P., "Watermarking of Digital Images", M.Sc. Thesis, Department of Electrical Engineering Indian Institute of Science Bangalore-560 012, India January, 1999.

3- Hajjara, S**.,** Abdallah, M. and Hudaib, A., "Digital Image Watermarking Using Localized Biorthogonal Wavelets" European Journal of Scientific Research ISSN 1450-216X Vol.26 ,No.4, pp.594-608, 2009.

4- Mohananthini, N. and Yamuna, G., "Robust Image Watermarking Scheme Based Multiresolution Analysis ", World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 163-168, 2012.

5- Zlomek, M., "Video Watermarking", M.Sc. Thesis, Charles University in Prague Faculty of Mathematics and Physics.2007.

6- Prasad Maity, S. and Kumar Kundu, M., "Robust and Blind Spatial Watermarking in Digital Image", ICVGIP 2002.

7- Perwej, Y. , Parwej, F. and Perwej, A., "An Adaptive Watermarking Technique for the Copyright of Digital Images and Digital Image Protection ", The International Journal of Multimedia & Its Applications (IJMA) Vol.4, No.2, April 2012.

8- Dinghui, Z., Haixia, D. and Chao, Z., "Researches on Digital Image Watermarking", The Eighth International Conference on Electronic Measurement and Instruments ICEMI', 2007.

9- Amirgholipour, S. K. and Naghsh-Nilchi, A. R., "Robust Digital Image Watermarking Based on Joint DWT-DCT", International Journal of Digital Content Technology and its Applications Vol. 3, No. 2, June 2009.

10- George, M., Chouinard, J. and Georganas, N., " Spread Spectrum Spatial and Spectral Watermarking for Images and Video", School of Information Technology and Engineering, University of Ottawa 161 Louis-Pasteur, Ottawa, Ontario, Canada K1N 6N5,1999.

11- Gunjal, B. L. and Gunjal, R. R.," An Overview of Transform Domain Robust Digital Image Watermarking Algorithms", Journal of Emerging Trends in Computing and Information Sciences Vol. 2, No. 1, ISSN 2079-8407, 2010.

12- Zubair, A. R., Fakolujo, O. A. and Rajan, P. K., " Digital Watermarking Of Still Images With Color Digital Watermarks", IEEE 978-1-4244-3861, 2009.