Information Hiding Based on Discrete Time Wavelet Transform and Huffman Coding

Ammar Abdul-Amer Rashed

Received on: 29/9/2010
Accepted on: 5/1/2011

Abstract

The approach of This paper presentation a companied technique for hiding secret messages (text) based on wavelet transform applying in cover image (a gray level image 8bit) then Huffman encoding is also executed on the secret messages,to increase the robustness of hiding system by inserting the embedded secret messages in the low frequency components of the cover image after applying wavelet transform followed by a sorting process and the coefficients of secret messages after applying Huffman encoding and using binary to multilevel to reading the string of message reducing by multiplying in attenuation factor before adding them with those of the cover image.

The experimental results show that the algorithm has a high capacity and a good invisibility, Moreover PSNR of stego image shows the better results the PSNR above 40 dB, the proposal system was activated according to attacker noise is addition and JPEG compression application are used with out detection the secret message.

Keywords: Information hiding, wavelet transform, Huffman coding.

أخفاء المعلومات بالاعتماد على تحويل الموجه(DWT) وترميز هوفمان

الخلاصة

محصله هذا البحث تقنية مؤلفة لإخفاء (رسائل سرية / النص) في غطاء الصور(gray level image 8bit) على أساس تحويل الموجه المطبقة على صورة الغلاف ثم تم تنفيذ ترميز هوفمان على رسائل سرية ولزيادة متانة الإخفاء وذلك من خلال إدخال الرسائل السرية في المكونات ذات التردد المنخفض للغلاف الصوري المطبق عليها تحويل الموجه تليها عملية الفرز وكذلك تم تضعيف معاملات الرسائل السرية بقدر معين بعد تطبيق (Huffman coding) و(reading the binary string) وذلك بضربها بمعامل التقليل (attenuation factor) ، النتائج التجريبية بينت أن الخوارزمية لديه قدرة عالية وجيدة الخفي. و PSNR الناتجة للصورة stego image فوق 40 ديسبل وخذ بنظر الاعتبار أن يكون المهاجم فعال بحيث تم إضافة ضجيج و تطبيق ضغط (JPEG) على الصورة الناتجة stego image دون الكشف عن الرسالة المخفية.

1- Introduction

The development of the technology of computer software and hardware, and digital media is getting more and more widely used and is playing an important role in such fields like education, scientific research, amusement, etc. At the same time with the rapid development of Internet these digital media can be copied and transmitted in a low cost and high speed. Under such a circumstance, some pirates use these features to spoil the legal interests of manufacturers and users so as to

* Computer Engineering & Information Technology Department, University of Technology/Baghdad

https://doi.org/10.30684/etj.29.2.9
2412-0758/University of Technology-Iraq, Baghdad, Iraq

obtain their individual interests, so copyright protection about digital media is becoming urgent to be solved. While taking legal and administrative measures, we should also provide some technical protection based on the features of digital media [1].

The information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly[2,3].

There are two types of data hiding the first one is, steganography and the second is digital watermarking [4].

Steganography is a word derived from Greek meaning "covered writing" is the hiding of a secret message inside another message so that no one can detect or decode the secret message. Steganography is used in espionage both corporate and in the intelligence industry, for Example the entertainment industry for copyright purposes, and there is Speculation that terrorists use it for some means of communication as well [5].

Digital Watermark is the process of embedding a signal, called the watermark, into another signal, called the host or cover, robustly and at the same time imperceptibly. The host signal can either be an image, audio, video or a text document (for example, program source code) [6].

The wavelet transform has become a useful computational tool for a variety of signal and image processing applications. For example, the wavelet transform is useful for the compression of digital image files; smaller files are important for storing images using less memory and for transmitting images faster and more reliably. The FBI uses wavelet transforms for compressing digitally scanned fingerprint images. NASA's Mars Rovers used wavelet transforms for compressing images acquired by their 18 cameras. The wavelet-based algorithm implemented in software onboard the Mars Rovers is designed to meet the special requirements of deep-space communication. In addition, JPEG2K (the newer JPEG image file format) is based on wavelet transforms. Wavelet transforms are also useful for `cleaning' signals and images (reducing unwanted noise and blurring). Some algorithms for processing astronomical images, for example, are based on wavelet and wavelet-like transforms [7].

Wavelets were developed independently in the field of mathematics, quantum physics, electrical engineering, and seismic geology. Interchanges between these fields during the last years have led to new wavelet applications such as image compression, turbulence, human vision, radar, and earthquake prediction [8, 9].

The Huffman coding uses a variable length code for each of the elements within the information. This normally involves analyzing the information to determine the probability of elements within the information. The most probable elements are coded with a few bits and the least probable coded with a greater number of bits [10, 11, 12].

1.1 Related Work

A general survey of information hiding is given as in [13], in [14] a created robust image hiding wavelet-base image hiding methods. the

Image watermarking in some years ago using wavelet transform to embedding watermarking in still image BMP true color [15].

2-Implementation of Proposed system

The proposed of information hiding algorithm has two parts as the following:-

2-1 The Embedding Algorithm:

The details of the embedding algorithm steps as shown in Figure (1) as the follows:

Step1:- Select the Cover-Image

Applying the full tree two-dimensional wavelet packets to the cover image, resulting in sub bands that contain both the frequency and spatial information. Since most of the natural images' energy concentrates in the low frequency bands, so in general, the high energy sub bands reflect their low frequency contents and vice versa [11]. In other words, one can pinpoint the low frequency subbands in term of calculating their energies.

Step2:- The sorting Process:

The sorting Process is applied to the low frequency components of the cover image depending to the energy of each cover image subband, those subbands are sorted in a descending manner.

Step3:- Enter the Message (secret messages/text):-

Perform the Huffman encoding to secret messages.

Step4:- Read the string binary

In this step reading binary for three cases or three levels using the following table (1) to reading the staring binary to decimal.

Step5:- Select the attenuation factor (secret key) between (0.1-0.9)

Multiplying this mapped string by attenuation factor (α). And adding to the low frequency components of the cover image. The value of attenuation factor (α) is saved automatically in the Info-file, in order to use the same value in the extraction stage. This factor has an important role in the embedding stage, as its value increase, more robustness will be obtained but less imperceptibility (less PSNR), so that atradeoff should be made between these parameters in order to obtain the best results.

Step6:- The Re-sorting Process

The order of the resulting sub bands can be returned to the same of the cover image by resorting them.

Step7:- Inverse Wavelet Packet Transform.

Appling the Inverse Wavelet Packet Transform to the cover image after Re-sorting process.

2.2 The Extracting Algorithm:

The details of the embedding algorithm steps as shown in Figure (1) as the follows:

Step1:- Select the Stego-Image. Applying the full tree two-dimensional wavelet packets to stego image. Its subbands are produced. These subbands contain the cover image subbands and secret message .

Step2:- Appling the step2 (the sorting process) from the embedding algorithm.

Step3:- Applying the full tree two-dimensional wavelet packets to cover image, Its subbands are produced.

Step4:- Appling the step2 (the sorting process) from the embedding algorithm.

Step5:- Subtracting the low frequency components between the stego image and cover image, and then the resulting values will be multiplying by the reciprocal of the attenuation factor (α).

Step6:- Sorting the redundancy confection in the low frequency components in step 5 and reconstructing the embedding encoding message.

Step7:- Round to nearest binary value.

For example If the resulting value of step 6 is greater than zero then a message bit is "1", on the other hand if the resulting value of step 6 is less than zero then a message bit is "0 after covert to decimal.

Step8:- Applying the step4 from the embedding algorithm but (reading decimal to binary).

Step8:- Decoding the Embedding message using the Huffman decoding.

3-Simulation Results:

In this paper some experiments are carried out to prove the efficiency of the proposed algorithm and gray scale images of size 512 × 512 are used as the cover-image to form the stego-image shown in Figure 2, and calculated (MSE, PSNR for Multilevel decomposition , binary to multilevel, the noise attack and the compression attack).

3-1 PSNR (Peak Signal to Noise Ratio):

One of the standard objective measurements is the PSNR, which will be adopted in this test.

$$PSNR = 10 * \log(255^2 / \text{MSE}) \quad \ldots(1)$$

Where

$$\text{MSE} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (f(x,y) - g(x,y)) \; / N^2$$

Where f(x,y) and g(x,y) means the pixel value at the at position (x, y) in the cover-image and the corresponding stego-image respectively. The PSNR is expressed in dB's. The larger PSNR indicates the higher the image quality i.e. there is only little difference between the cover-image and the stego-image. On the other hand, a smaller PSNR means there is huge distortion between the cover-image and the stego image [16].

And also measured

$$P_e = \frac{N_e}{N_t} \times 100 \ \% \qquad (2)$$

Where:

Nt = Total Message Length in Bits.

Ne = Total number of erroneous Bite of the Extracted Message.

In the table (2, 3, 4) shown the PSNR's (dB) for stego image and (Variableα), and binary to multilevel.

4-The Robustness of the Proposed System:

The Robustness is a practical requirement for a hiding system. A system is called robust if the embedded information cannot be altered without making drastic changes to stage- image [17].The robustness of the proposed system will be tested against two well-known types of attacks, noise, and compression attacks.

4-1 The Noise Attack

The improve the stego image imperceptibility, the embedded message is attenuated during the embedding process, so that it becomes more sensitive to the external distortion during the transmission or even introduced by an attacker. To see how much this image is sensitive, noise Gaussian Noise (AWGN) are used and added to the stego image with different variances shows the results in table 5.

4-2 The Compression Attack

Another test is applied to the proposed stegosystem to show its robustness against the compression attack. The Joint Photographic Experts Group (denoted by JPEG) [12] compression which based on cosine transform is used here because it is a standard lossy compression algorithm that uses many parameters allowing users to adjust the amount of the data lost (and thus also the compression ratios) over a wide range ,JPEG 2000 which is new standard scheme based on wavelet transform is not used here because the same principles of the JPEG compression is used in this scheme which reduces the data by eliminating its high frequencies followed by entropy coder, the compression ratios that are used in this work are 5,10 & 15 shows the results in table (6).

5-The Capacity Of the proposed system:

The capacity of the proposed of information hiding algorithm different according to the applied or chose the level in (binary to multilevel table in step 4 embedding algorithm) as following:

1- Hiding 1bit/pixel in low frequency components of the cover image the size of message is 196608 bit .

2- Hiding 2bit/pixel in low frequency components of the cover image the size of message is 393216 bit .

3- Hiding 3bit/pixel in low frequency components of the cover image the size of message is 589824 bit.

6-Conclusions:

In This proposal system has a high security because the secret message is embedded in special domain using the Transform Domain Techniques two-dimensional wavelet packets for multilevel decomposition in cover image and the Huffman encoding applied in message.

The capacity of embedded message is increased due to use binary to multilevel and Huffman encoding to reading the secret message but the PSNR is decreased when over the JPEG compression ratio is increased, the system must increase α therefore reduce the PSNR of stego image and the noise attack is not essentially affected in the embed message.

Refferences

[1] Liwei Chen clwswust, and Mingfu Li(An Effective Blind Watermark Algorithm Based on DCT), Proceedings of the 7th World Congress on Intelligent Control and Automation June 25 - 27, 2008, Chongqing.

[2] Pierre Moulin, Fellow, IEEE, and Joseph A. O’Sullivan, Fellow, (Information-Theoretic Analysis of Information Hiding), IEEE, IEEE Transactions On Information Theory, Vol. 49, No. 3, March 2003.

[3] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding-A Survey", proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 87(7): 1062-1078, July 1999.

[4] S. Katzenbeisser and F .A .P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, London 2000.

[5] T. Armstrong, K. Yetsko, "Steganography", CS-6293 Research Paper, Instructor: Dr. Andy Ju An Wang, 2004.

[6] A. Sequeira "Enhanced Watermark Detection ",M. Sc., thesis, University of Toronto, Canada, 2003.

[7] Lvan W. Selesnick . Polytechnic University Brooklyn, NY (Wavelet Transforms - A Quick Study), September 27, 2007.

[8] M. Vetterli and J. Kovacevic, "Wavelets and Subbands Coding", Englewood Cliffs, New Jersey: Prentice Hall, 1995.

[9] K. R. Castleman, "Digital Image Processing", Prentice Hall 1998.

[10] W. Buchanan :"Advanced Data Communications And Networks", senior Lecturer of EECE Napier University Edinburgh UK ,1997.

[11] Salomon D. "Data Compression the Complete Reference" 4Ed.springer Verlag.New York,2005.

[12] Lim H.Y.P., Interactive Data Compression internet teaching Web based teaching aid for data compression, School of Electronic and Electrical Engineering, University of Birmingham,1998.

[13] N. F. Johnson and S. Katzenbeisser, A survey of steganographic techniques., in S. Katzenbeisser and F.Peticolas (Eds.): Information Hiding, pp.43-78. Artech House, Norwood, MA, 2000.

[14] Chih-Yang Lin And Yu-Tai Ching, A robust image hiding method using wavelet technique ,journal of information hiding science and engineering 22,163-174(2006).

[15] A.Nag',S.Biswas *Dr. Jane J.Stephan . Image watermarking using wavelet transform ,Iraq commission for computer and informatics ,information institute for postgraduate studies/Baghdad 2005.

[16]A.Nag',S.Biswas*,D.Sarkar*,P.P . Sarkar* (A novel technique for image staganography based on Block-DCT and Huffman Encoding ,International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010.

[17] Stefan Katzenbeisser, Fabien A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", ArtechHouse, London, 2000.

Table (1) reading the staring binary:

Two level read binary 1-bit		Four level read binary 2-bit		Eight level read binary 3-bit			
Binary sequence	Level represent	Binary sequence	Level represent	Binary sequence	Level represent	Binary sequence	Level represent
1	+1	11	+3	010	+7	100	-1
0	-1	01	+1	011	+5	101	-3
		00	-1	001	+3	111	-5
		10	-3	000	+1	110	-7

Table (2) PSNR's (dB) for stego image and (Variableα), and binary and reading the binary with 2- level.

Cover image name= Babban (512x512), Size message=196608 bit				
Attenuation (Factorα).	WP three Levels Decomposition		WP four Levels Decomposition	
	PSNR	Error in message%	PSNR	Error in message%
0.9	20.5	20.5	22.6	22.8
0.7	25.3	16	28.35	13
0.3	30.4	4.5	31.5	6
0.2	36.5	0	38.1	3.3
0.1	42.1	3	44	0
Optimum Parameters	PSNR=36.5 αopt.=0.2		PSNR=44 αopt.=0.1	

Table (3) PSNR's (dB) for stego image and (Variableα), and reading the binary with 4- level

Cover image name= Lamees, (512x512), Size message=393216 bit				
Attenuation (Factorα).	WP three Levels Decomposition		WP four Levels Decomposition	
	PSNR	Error in message%	PSNR	Error in message%
0.9	20.5	33	22	32
0.5	25.7	18	28.1	18
0.3	27.5	10	29.5	8
0.2	39	5	40.5	0
0. 015	40.3	0	42	11
Optimum Parameters	PSNR=40.3 αopt.=0.015		PSNR=40.5 αopt.=0.2	

Table (4) PSNR's (dB) for stego image and (Variableα), and reading the binary with 8- level.

Cover image name= Lamees, (512x512), Size message=589824 bit				
Attenuation (Factorα).	WP three Levels Decomposition		WP four Levels Decomposition	
	PSNR	Error in message%	PSNR	Error in message%
0.8	19	29	20	27
0.6	23.3	18.8	26.8	18
0.4	27	15	30	9
0.2	38.2	0	38.7	5
0.125	40	5	40.5	0
Optimum Parameters	PSNR=38.2 αopt.=0.2		PSNR=40.5 αopt.=0.125	

Table (5) the optimum parameters for the reconstructed stego images for AWGN Test.

Stego image name= Babban (512x512), after embedded Size message=196608 bit					
Variance	Attenuation (Factorα). Optimum Parameters	WP three Levels Decomposition		WP four Levels Decomposition	
		PSNR	Error in message%	PSNR	Error in message%
50	0.175	30	0	38	0
100	0.273	29	0	30	0
150	0.356	28.6	0	28.5	0

Table (6) the optimum parameters for JPEG compression tests.

Stego image name= Babban (512x512), after embedded Size message=196608 bit					
Comp. ratio	Attenuation (Factorα). Optimum Parameters	WP three Levels Decomposition		WP four Levels Decomposition	
		PSNR	Error in message%	PSNR	Error in message%
5	0.285	30	0	35	0
10	0.42	26	0	30	0
15	0.51	25	0	27	0

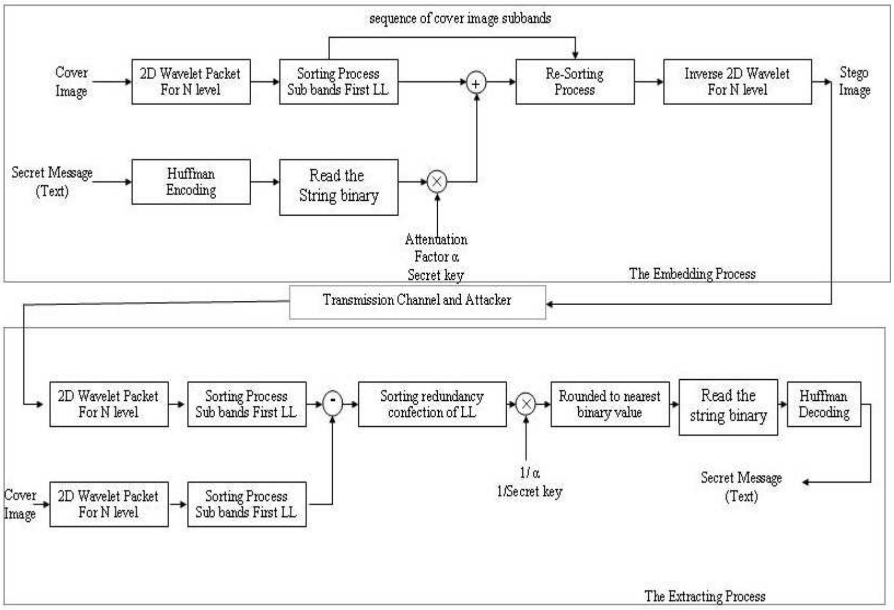

Fig (1) The Proposed Information hiding

Lamees 512 x 512 **Babban 512 x 512**

Figure (2) the cover image