Hybrid Algorithm to Improve Robustness of Image Watermarking

Ammar Fakhri Mahdi
Computer Sciences Department, University of Technology/Baghdad.
Email:ammar_ar2@yahoo.com

Received on: 1/12/2014 & Accepted on: 2/4/2015

Abstract

Watermarking is the process of embedding digital information into any multimedia data such as an image, audio or video file in such a way that intruder cannot be able to trace the signal to protect copyright of intellectual property of owners. In this paper, a new hybrid watermarking algorithm is proposed by using discrete wavelet transform (DWT) and slant let transform (SLT) which are the most robust to attacks rather than least significant bit (LSB) for the protection of digital Images. Embedding watermark is accomplished in still images (JPEG) true color in high frequency sub bands by combining the two transforms. The watermark is applied to many images, and the results showed that the proposed algorithm offers good performance and has good robustness against different types of attacks and it does not effect on the transparency of the cover image.
Keywords: Discrete Wavelet Transform (DWT), Slant Let Transform (SLT), Peak Signal to Noise Ratio (PSNR) and Accuracy Rate (AR).

خوارزمية هجينة لتحسين متانة العلامة المائية للصورة

الخلاصة

العلامة المائية هي عملية اخفاء المعلومات الرقمية في بيانات وسط متعدد كأن يكون ملف صورة، صوت أو فيديو بطريقة ما بحيث لايتمكن المتطفل من تتبع الأشارة بهدف حماية حقوق النشرللمالك. في هذا البحث تم اقتراح خوارزمية جديدة هجينة للعلامه المائية بأستخدام التحويل المويجي المنفصل (DWT) وتحويل المويل (SLT) واللذان يعتبران اكثر قوة في توفير الحماية للصور الرقمية مقارنة بطريقة البت الأدنى أهمية (LSB). تم أخفاء العلامة المائية في الصور الملونة الثابتة (JPEG) في الجزء ذو الترددات العالية من خلال الدمج بين التحويلين. وتم تطبيق العلامة المائية في صور متعددة، وقد اوضحت النتائج بأن الخوارزمية المقترحه ذات اداء وقوه جيده في الأخفاء ومواجهة أنواع مختلفة من الهجوم ولم تؤثر على شفافية الصورة الغطاء.

INTRODUCTION

Digital watermarking also called tamper-proofing or content verification hides a secret and personal message to protect a products copyright; it became a most powerful applicant who can solve the essential problem of legal ownership. Many applications involve copyright protection, authentication and data hiding. Though watermarking is widely soiled to protect copyright of digital content, it is now finding use

https://doi.org/10.30684/etj.33.3B.16
2412-0758/University of Technology-Iraq, Baghdad, Iraq

in other kinds of media like printed materials, texture images, designs, copy machines, scanners and other applications where copyright protection is required. Various watermarking schemes have been advanced, which embed the watermark either in time or in the frequency domain [1, 2].

Digital watermark can be classified as visible or invisible recognition code that is always embedded in the host media. It should be imperceptible, transparent, secure, robust to improve its application in copyright protection, video authentication, fingerprinting, and copy control. As comparing the two domains, time-domain watermarking technique is simpler and its computing speed is higher than frequency-domain watermarking. However, it is not robust against popular image processing operations. Frequency-domain techniques are introduced to increase the robustness of the digital media [3, 4]. When the watermark media is embedding by using special algorithms, the main (host) media is called the watermarked media and will be lightly changed, then is sent to the receiver through the Internet or any other transmission canal. There might be no or little perceptible dissimilarity between the original and the watermarked media [5.[

In this paper, DWT is used and the watermark is embedded in the frequency regions, then the SLT is used in order to achieve perceptual invisibility as well as robustness to attacks. Discrete Wavelet Transform and Slant let Transform

Signal transformation is not modify the content of the information existent in it, is just a different form of representing the signal. Discrete wavelet transform supply a time-frequency representation of the signal and it was advanced in order to get over the short coming of the Short Time Fourier Transform (STFT) which grant a fixed resolution at all frequencies, whereas the discrete wavelet transform uses multi-resolution mechanism by which various frequencies are analyzed with various resolutions [6].

However, in wavelet transform the time domain is transported via low-pass and high-pass filters in order to elicit low and high frequencies individually, then in each time the signal is drawn out when this routine is repeated more than one times. The signal is divided by the DWT into two classes (Approximation and Detail) through signal decomposition for different frequency bands and scales. Only half of the samples in a signal are effective to represent the entire signal. Figure1 shows first-level decomposition image. Wavelet decomposition has significant characteristics so many of the coefficients for the high-frequency parts (LH, HL and HH) are zero or insignificant. Therefore, the important information is in "LL" sub-band [7, 8]

Figure(1): First level decomposition for image [9]

The slant let transform (SLT) is an orthogonal DWT with two zero moments and possesses improved time-localization properties and it has been more effective than the DWT by involving the lengths of the discrete time basis function and their moments as the vehicles since both time-localization and smoothness properties are accomplished. The SLT is based on a filter bank form where different filters are used for each scale. The SLT filter bank can be controlled through various filters that are not products. Filters of shorter length are designed satisfying orthoganality and zero moment conditions from that additional extent of freedom, which obtained by giving up the product form. The Daubechies filter with two-channel is the shortest filter which makes the filter bank orthogonal and has K zero moments. The iterated filters in the case of K=2 zero moments are of lengths 10 and 4 but the SLT filter bank with K=2 zero moments has filtered lengths 8 and 4. Therefore the two-scale SLT filter bank has a filter length which is two samples less than that of a two-scale iterated Daubechies-2 filter bank. Each filter bank has a scale dilation factor of two and provides multi resolution decomposition. The slant let filters are linear, and there is no tree structure for SLT that can be effectively implemented as found in an iterated DWT filter bank. Finally, the frequency domain is more effect than the time domain of apportioning the hidden information through different order bits in a way that is robust [1, 10].

The Proposed Algorithm

In this paper, a new hybrid proposed digital watermarking algorithm is presented, it consist of two stages and there are:

1. Digital watermarking embedding algorithm.
2. Digital watermarking extracting algorithm.

Embedding Watermarking Algorithm

In this stage, a watermark image is embedded in the host image, and this is done pixel by pixel [each pixel in the original image is replaced by pixel of the watermark image]. This process is passed through two steps; first step embedding is accomplished after the original image and the watermark image is transformed using DWT, and in the second step the output from the watermarked image is embedded in another host image after transformed them using SLT. This algorithm is illustrated in algorithm (1):

Algorithm (1): Embedded Watermarking.

Input: Host image, Watermark image and factor controlling (F).

Output: Watermarked image.

Step1: Apply the transform DWT to host image with size (128*128) and to watermark image with size (64*64), obtain 4-subbands (LL, LH, HL and HH).

Step2: Embed the data by replacing the high frequency coefficients of the host image with the coefficients of the watermark image (one pixel per pixel), dividing each coefficient by (F) to normalize the values of coefficient, where (F) is the factor controlling the level of watermarking as in the following equation.

$$C1(i1, j1) = C2(i2, j2)/F \quad \ldots (1)$$

https://doi.org/10.30684/etj.33.3B.16
2412-0758/University of Technology-Iraq, Baghdad, Iraq

Where
(C1) is the coefficient of host image, (i1, j1) are the index of the modified band, (C2) is the coefficient of watermark image, (i2, j2) are the index of the watermark image. The result is the watermarked image with size (128*128).
Step3: Apply the inverse transform IDWT for the modified image to reconstruct the watermarked image.
Step4: Apply the transform SLT to another host image with size (256*256) and to the reconstructed watermarked image with size (128*128), obtain 4-subbands (LL, LH, HL and HH).
Step5: Repeat step2, the result is the watermarked image with size (256*256).
Step6: Apply the inverse transform ISLT for the modified image to reconstruct the watermarked image.
Step7: End.

Extraction Watermarking Algorithm

In this stage, a watermarked image is extracted from the host image, and this is done by applying the reverse of embedding. This process is passed through two steps; first step extracting is accomplished after the watermarked image is transformed using SLT, in the second step the output from the watermarked image is extracted after transformed using DWT. This algorithm is illustrated in algorithm (2):

Algorithm (2): Extracted Watermarking.
Input: Watermarked image, factor controlling (F).
Output: Watermark image.
Step1: Apply the transform SLT to watermarked image with size (256*256); obtain 4-subbands (LL, LH, HL and HH).
Step2: Extract the embedded watermarked image with size (128*128) from high frequency coefficient by applying the reverse of embedding as in the following equation.

$$C2(i2, j2) = C1(i1, j1) * F \quad \ldots (2)$$

Step3: Apply the inverse transform ISLT for the modified image to obtain the extracted watermarked image with size (128*128).
Step4: Apply the transform DWT to the extracted watermarked image; obtain 4-subbands (LL, LH, HL and HH).
Step5: Repeat step2, the result is the watermark image with size (64*64).
Step6: Apply the inverse transform IDWT for the modified image to obtain the extracted watermark image with size (64*64).
Step7: End.

Experiment Results

The evaluation of this watermark algorithm contains two parts: concealing and robustness against common types of attack. The concealing of the watermark is

quantitatively analyzed by using Peak Signal to Noise Ratio (PSNR). This Peak Signal to Noise Ratio is defined as in the following equation [11].

$$PSNR = 10log_{10}\frac{A^2}{\frac{1}{N\times M}\sum_{i=1}^{N}\sum_{j=1}^{M}[f(i,\ j)-f'(i,\ j)]^2} \quad \text{..... (3)}$$

Where

A, is the maximum value in the pixel (255). Its unit is db, and the bigger the PSNR value is the better the watermark conceals.

In this paper, the watermark image is embedded in the host image through two steps; the first step is accomplished by embedding the watermark image with size (64*64) in the host image with size (128*128) using DWT, and in the second step the resulted watermarked image from the first step is embedded in another host image with a bigger size (256*256) by using SLT, then compute the PSNR value for the final watermarked image. These two steps with PSNR values are illustrated in table (1).

Table (1): The PSNR Values of the Watermarked Images for Color Images.

Watermark Image with size (64*64)	Host Image with size (128*128)	Watermarked Image with DWT	Host Image with size (256*256)	Watermarked Image with SLT	PSNR (db)
					**38.685**
					**39.156**
					**39.76**
					**38.723**

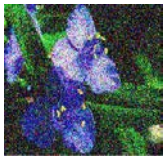
Robustness can be evaluated by applying various kinds of attacks. A quality estimation parameter to check the robustness of the extracted image, names as Accuracy Rate (AR), which is used to measure the ratio between the original watermark image and the recovered one. AR is defined as in the following equation [9, 12].

AR=CP/NP … (4)

Where NP is the number of pixels in the original watermark image and CP is the number of correct pixels obtained by comparing the pixels of the original watermark image to the corresponding ones of the recovered watermark image. The value of AR is between 0 and 1, and the bigger the value is the better the watermark robustness.

Anyway, there are number of attacks that effect on the watermarked image. In this paper, Gaussian noise and the JPEG2000 compression are used as an attack to measure how the extracted watermark image can be survived. In the first attack the Gaussian noise is added to the watermarked image which created from the second embedded step as show in table (1), then the watermark image with Gaussian noise attack is extracted and compute the AR value. In the second attack the JPEG2000 compression applied to the same watermarked image, then the watermark image with the JPEG2000 compression attack is extracted and again computes the AR value. These two attacks with AR values are illustrated in table (2).

Table (2): The AR Values against Gaussian Noise and JPEG2000 Compression for Color Images.

Adding Gaussian Noise to Watermarked Images with SLT	Extracted Watermark Images with Gaussian Noise Attack	AR	JPEG2000 Compression to Watermarked Image	ExtractedWatermark Image with JPEG2000 Compression Attack	AR
		**0.873**			**0.831**
		**0.821**			**0.805**
		**0.88**			**0.852**
		**0.842**			**0.817**

Finally, implementing the watermark in an image by using two layers of transform methods (DWT and SLT) support the embedding method resistance against attack and keeping a good transparency for the host image. Also, PSNR and AR values as illustrated in table (1) and table (2) are in acceptable range in spite of embedding was in two layers of (DWT and SLT).

Conclusions

Robustness is the very important requirements of digital watermarking, so that improving the robustness in a watermarking may decrease the imperceptibility, and vice versa. This paper introduces watermarking algorithm for digital image based on combining both DWT and SLT. Watermarking signal is embedded into the high frequency band of wavelet and SLT transformation domain. The experimental results in terms of PSNR and AR show that this watermarking system not only can keep the image quality well, but also can be robust against common image processing attacks such as adding Gaussian noise and JPEG compression. Using two transforms make the security of data more robust against intruders.

References

[1] Bhupendra Ram, "Digital Image Watermarking Technique Using Discrete Wavelet Transform and Discrete Cosine Transform", International Journal of Advancements in Research & Technology, IEEE, ISSN 2278-7763, Volume 2, Issue4, April-2013

[2]ShikhaTripathi, Nishanth Ramesh, Bernito A, Neeraj K J, "A DWT based Dual Image Watermarking Technique for Authenticity and Watermark Protection", Signal & Image Processing : An international journal(SIPIJ) Vol.1, No.2, December 2010.

[3]Nidhi H. Divecha, N. N. Jani, "Image Watermarking Algorithm using Dct, Dwt and Svd", International Journal of Computer Applications (IJCA), 2012.

[4] Chirag Sharma, Deepak Prashar,"DWT Based Robust Technique of Watermarking Applied on Digital Images", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.

[5] Dr. Nidaa F. Hassan and RuaaKadhimJaber, "Proposed Algorithm for Digital Image Watermarking Survival against JPEG Compression", Eng. & Tech. Journal, Vol.32, Part (B), No.1, 2014.

[6] Ammar Abdul-AmerRashed, AymenDawood Salman and Saddam KamilAlwane, "Secret Technique to Hiding Image after Compression in Cover Image", Eng. & Tech. Journal, Vol. 29, No.10, 2011.

[7] Mohammed Mustafa Siddeq, "Using Two Levels DWT with Limited Sequential Search Algorithm for Image Compression", Journal of Signal and Information Processing, 3, 51-62, 2012.

[8] Dr. Eyad I. Abbas and Hameed R. Farhan, "Face Recognition using DWT with HMM", Eng. & Tech. Journal, Vol.30, No.1, 2012.

[9]Keshav S Rawat, "Digital Watermarking Schemes for Authorization against Copying or Piracy of Color Images", IEEE, Indian Journal of Computer Science and Engineering, Vol. 1 No. 4 295-300, 2010.

[10] G. Panda, P. K. Dash, A. K. Pradhan, and S. K. Meher, "Data Compression of Power Quality Events Using the Slantlet Transform", IEEE Transactions on power delivery, VOL. 17, NO. 2, APRIL 2002.

[11] Mei Jiansheng1, Li Sukang1 and Tan Xiaomei2, "A Digital Watermarking Algorithm Based On DCT and DWT", ISBN 978-952-5726-00-8 (Print), Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09), Nanchang, P. R. China, pp. 104-107, 2009.

[12] Shang-Lin H., I-Ju T., Bin-Yuan H., and Jh-Jie J., "Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform", Journal Of Multimedia, Vol. 3, No. 4, 2008.