Propose an Image Watermarking Algorithm Stand against JPEG Compression based on Space Transformation and Image Features

Nidaa Flaih Hassan* (Assist.Prof) Ph.D Ruaa Kadhim Jaber*

Abstract

In this proposal, a new algorithm is introduced to watermarked digital images (with format BMP). After trying number of features to decide which blocks of image are the best hosts, two features DC (Direct Current) Coefficient(resulting for Discrete Cosine Transform(DCT)) and the Entropy (H) are chosen, since these features are specifying embedding locations that cause a minimal degradation to the cover image and determining the blocks that can keep the embedded value stand against compression .This algorithm produces a watermarked image that can be subjected to lossy JPEG (Joint Photographic Experts Group) compression without losing its watermark. Fidelity Criteria evaluates the errors between the original and cover images, good tests are achieved without perceptual degradation for the transparency of the cover image.

Key Words: Watermarking, Features, DC Coefficient, Entropy, lossy Compression, JPEG.

*University Of Technology

1. Introduction

The internet is abrilliantsupply system for digital media, for its effectivenessand inexpensiveness. Files can be readily shared, easily used, handled, and transmitted that cause serious difficulties such as illegal use and handling of digital media. As a result, there is anessentialneed for authentication methods to secure digital files. Digital watermarking is a method that embeds information or secret data (called digital signature or watermark) into the digital files in order to secure it fromany alteration of its content [1].

The necessity to enable transmission, storage, and archiving of multimedia digital files has directed to many researchesconcerned in the progress of efficient compression structures, such that, digital media that are high quality can compress the data stream to less so it can be transmitted over the network in faster time [2].

Although compression is one of the most important operations that facilitates and speeds up the transmission of large files through the internet, lossy compression results in losing some details of the file and is considered as one of the attacks that may circumvent the intended purpose of the watermarking technique. Therefore, watermarking techniques that can embed a resistant watermark against lossy compression is needed,since most files must be compressed before storage or transmission in order to minimize the storage and bandwidth requirements. In this paper, a new algorithm is proposed to embed a watermark in BMP image, which is stand against JPEG compression.

2. Watermarking

A digital watermark is information that is survival and invisibly embedded in the host data, so it cannot be removed. Watermark usually contains information about the origin, status, or the receiver of the host data[3].

Methods of digital watermarking can almost be classified into two types: non-blind watermark methods and blind watermark methods. Non-blind methods require the original image when the extraction process is ended; while the means blind methods do not. Blind methods are more

useful than those that are non-blind methods,since original image may not be available in actual scenarios[4].

It can be found on the watermarking system with as a communication system which consists of three main components: the Embedder, a channel of communication, and the detector. Watermark is included in the information signal in such a way that it can be extracted by the detector. To be more precise, watermark information is included within the host signal before that signal is sent watermarked on the communication channel, so that it can detect the watermark at the receiving end; in any revealed [5]. Figure (1) shows the generic schema of digital watermarking.

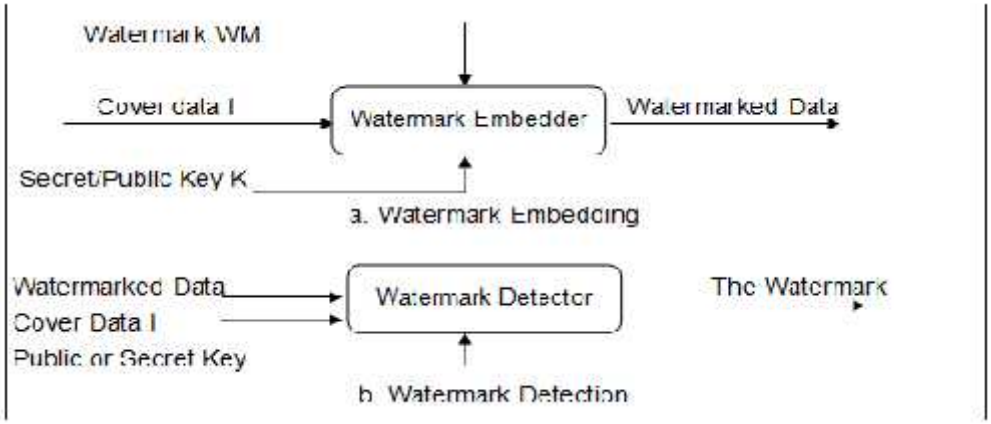

Figure (1): Generic Digital Watermarking Scheme [6].

3. Image Compression

Image compressionisappliedto compress the datathat encodethe original imagewith a small numberof bits.The aim ofimage compressionis to reduce therepetitionof the imageandstorageimage data that are transferinan effectiveform[7]. Figure (2) shows a General image compression system.

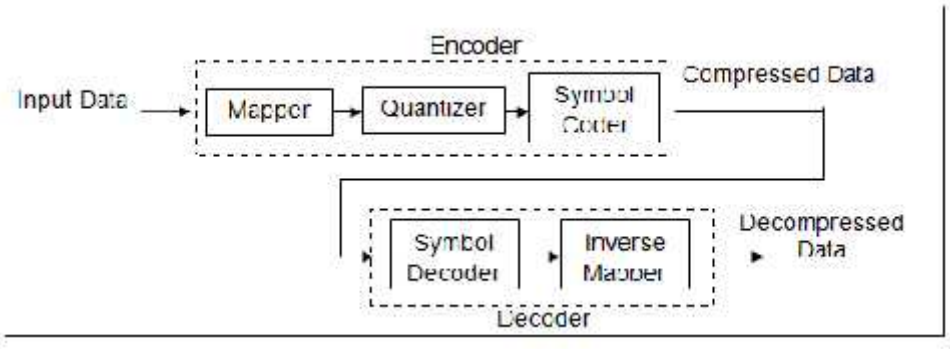

Figure (2): General image compression system [8].

Image compression systems are classified into lossless or lossy methods, depending on whether the image is recreated from a single compressed is the equivalent as the original image or not. Lossless image compression systems do not change from the original image qualityseeming by the observer, but they achieve low compression ratios, while, lossy image compression systems in an attempt to take advantage of perceived quality by the observer, and the reduction of the number of bits required to represent those parts of the image where the human visual system is unable to perceivethese part of image. In order to achieve this objective, lossy image compression systems typically have four stages: preprocessing, transformation, quantization and coding structure[9].

JPEG the international standard is an example of lossy compression; it is used commonly in digital imaging, digital cameras, the inclusion of images in Web pages, and many other productions. In compressing images, JPEG has found widespread as a means of simple and active ways to compress moving images (in the form of JPEG digital video) movement. The data is a single image 8 × 8 block address at one time. It may be processed color or aircraft components (such as R, G, B or Y, Cr, Cb) separately (one component at one time) or for interleaved order (for example, three successes of color components is treated as block) [10]. All blocks are coded via the steps that are shown in Figure (3).

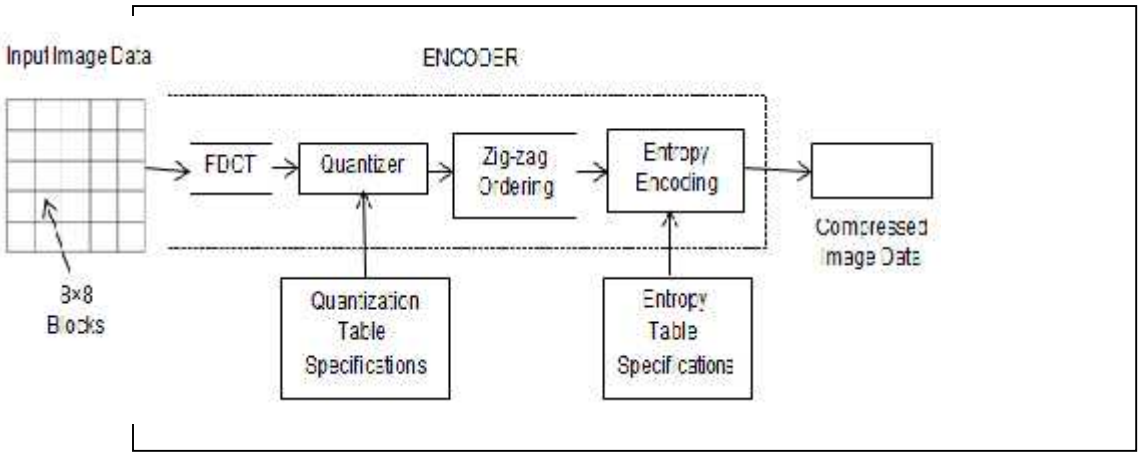

Figure (3): JPEG Compression [11].

4. Transform Domain Techniques

Transform coding reliant on the principle that pixels in the digital imagehave a certain level of interrelated relationship with its neighboring pixels. As a result, these links can be exploited to forecast the value of the pixel from neighbors. Therefore transform coding set the definition of these spatial related (correlated) coefficientsof imagefrom unrelated (uncorrelated)coefficientsof image [12]. Watermarking methods that are used transform coding operate in three stages,at first stage image is transformed using some transform coding methods such as discrete cosine transform (DCT) or discrete wavelet transform (DWT), in the second stage a watermark is embedded in the coefficientsof image data, and in the third stage the inverse transform coding is applied to get a watermarked image

In this paper, watermark embedding in the most used transform (the Discrete Cosine Transform DCT) which is explained below.

4.1 Discrete Cosine Transform (DCT)

An important feature of DCT in image compression is that it takes (correlated)image data entry and focuses its energy within the first few transform coefficients. Thefirst transforms coefficientreferred to as DC coefficient ;and AC coefficients to all other transforms coefficients. The two

DC and AC coefficients symbolize "Direct Current" and "Alternating Current ". The DCT takes the correlated image entry and only focuses its energy in the first few conversion coefficients, while thesubsequentconversion coefficientsthat are produced by DCT arezeros or small numbers. The first coefficients contain important imageinformation(low frequency), andthe subsequentcoefficients contain less importance image information(high-frequency) [12].

To embed a watermark in DCT, the original image is segmented into fixed sizes blocks, those blocks are discrete cosine transformed, the watermark is embedded, and then the image passes through inverse DCT [11].

The two dimensional DCT for an N x N image can be formulated as:

$$F(u,v) = \alpha(u)\,\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad ...(1)$$

The inverse transform is defined as:

$$f(x,y) = \alpha(u)\,\alpha(v) \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} F(u,v) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad ...(2)$$

$$\alpha(u,v) = \begin{cases} \sqrt{\frac{1}{N}} & For\ u,v = 0 \\ \sqrt{\frac{2}{N}} & Otherwise \end{cases} \quad .....(3)$$

For x, y, u ,v = 0,1 ,…,N-1, N are image dimensions (x is a width and y is height), f(x ,v) is the original image, and (u is a width and v is height), F(u,v) is the transformed image [13].

5. The Proposed Watermarking Algorithm

There is a conflicting between compressions and watermarking, although image compression aims to identify the perceptually unimportantblocks of the image data and eliminate them, watermarking techniques try to embedinformation in these blocks. In this paper, a new watermarking algorithm is proposed to hide secret data in the cover image that are able to stand against JPEG compression, watermarked is embedded and extracted in the proposed algorithm are based on analyzing the image using the two measures the DC Coefficient(resulting for Discrete Cosine Transform (DCT)) and the Entropy (H), which can be defined as:

DC Coefficient:A signal is converted from spatial domain to frequency domain by DCT transform, where the important visual information is focused on first coefficient transform (AC)

H:The entropy is a measure that tells how many bits are needed to code image data. It can be calculated using the following equation:

$$H= -\sum_{g=0}^{L-1} P(g)\log_2[P(g)] \quad \text{.....(4)}$$

WhereL is the gray level range such as [0, 1], [0 to 7] or [0 to 255], P (g) is probability of gray level g in the image[14]. The embedding and extraction modules for the proposed algorithm are explained below.

5.1 Embedding Module

The watermark is first converted into binary digits, then the cover image is divided into 7 bytes blocks, the host blocks are determined based on two features which are(DC coefficient (resulting from DCT of the block), and the Entropy (H)).

The host block must have DC within the range [330 to 360] and H >= 0.4. These thresholds imply that the block has large values differ from each other. It is found that, this kind of blocks maintain its values and can survive against compression than the blocks that have smaller values. Since compression eliminates or reduces redundant data, image locations that contain similar values are said to have redundant data. Therefore, the blocks that have different values are less affected by compression since they do not have redundant data. In addition, when block values are large, even if these values are affected by compression, they remain closer (either smaller or larger) to their original values.

Odd block means that block index is odd and even block means that block index is even. In order to recognize bit 1 from bit 0, an odd block is used for bit 1 and even block for bit 0.

In order to get correct extraction after decompression, the host block must be **enforced,** by slightly changing its values, therefore, when the values are affected by compression, they remain within a known range. The enforcement is done as follows:

1. If the host block satisfy all required conditions, then if the (DC< 340) then the DC is increased by incrementing block values by 5, but if the (DC >350) then the values are decremented by 5 to decrease the DC. The increment and decrement help in keeping the DC at the middle of the required range, so if the values are affected by compression, the DC remains within [330 to 360].
2. If the block does not satisfy the required conditions, then if the DC > 350 then the values are incremented by 15, but if the DC < = 350, then the values are decremented by 15, this helps in remaining the block outside the determined range.

H does not change by incrementing and decrementing the values, since it depends on the probability of the value, and not the value itself. Block enforcement represents the embedding process; where the embedding process depends on block features, by maintaining these features, the block survives lossy compression that leads to correct extraction. Watermark embedding steps for this algorithm are illustrated in Algorithm (1).

Algorithm (1): Transform and Features Based Embedding.

Input: Original cover image (Image_1) and Watermark (WM).
Output: The watermarked image (WM_Image).
Step 1: Convert WM into binary digits saved in Bits_array ( ), and addthe Flag. // The Flag is 7 zeros, to indicate end of extraction operation at the receiver side.
Step 2: Encrypt the bits in Bits_array ( ), by performing an XOR operation between the bits and the bits of a key. //The used key is common between the sender and the receiver.
Step 3: Transfer the header part (60 bytes) from Image_1 into WM_Image, and Initialize (I = 1 and Index = 0).
Step 4: While not (end of Bits_array ( )) do // Bits Embedding process.

Bit = Bits_array (I): Index = Index + 1.
Get a seven bytes block from Image_1.
Calculate block H and DC.
If H>=0.4 and DC within [330 to 360] then
If (Bit =1 and Index is odd) or (Bit = 0 and Index is even) then the block is a host: I = I + 1.
End if
Else
The block is not a host
End if
If the block is a host then
If DC < 340 then increment block values by 5.
If DC > 350 then decrement block values by 5.
If DC within [340 to 350] then do not change block values.

End if

If the block is not a host then
If DC > 350 then increment block values by 15.
If DC <= 350 then decrement block values by 15.
End if
Transfer the block into WM_Image.

While End

Step 5: Transfer remaining blocks from Image_1into WM_Image.

5.2 Extraction Module

Like embedding, extraction operation depends on block features, where H and DC of the block are calculated; if H >= 0.4 and DC within [330 to 360] then the block index specifies whether the embedded bit is 0 or 1. If the index is odd, the extracted bit is 1 or 0 otherwise. Watermark extraction steps are illustrated in Algorithm (2).

Algorithm (2): Transform andFeatures Based Extraction.

Input : The watermarked image (WM_Image).

Ouput : The embedded watermark (WM).

Step 1: Skip the header part (60 bytes) of WM_Image, and initialize (Flag = 0 and Index = 0).

Step 2: While (Flag < 7) // Bits Extraction

Index = Index + 1 //get seven bytes block fromWM_image

Calculate block H and DC.

If H >=0.4 and DC within [330 to 360] then

If Index is odd then Bit = 1: Else Bit = 0

Decrypt Bit.

If Bit = 1 then Flag = 0: Else Flag = Flag + 1

Save Bit in Bits_array ( ).

End If

While End

Step 3 : While (Not End of Bits_array( )) //Bits converted into ASCII, and then into characters toform WM.

Convert each 7 bits into ASCII.

Convert the ASCII into character.

WM = WM + character. // Characters are merged to Form WM.

While End

6. Results and Discussion

The loss of real or quantitative information of digital image could be caused by removing unrelated or unimportant visually image information, there are two types of measures used to determine lostin image information:

1. **Objective FidelityCriteria:** Mathematical function is used to determine the loss of information for input and output of compression process
2. **Subjective FidelityCriteria**: The two images (original and reconstructed) are subjected to number of expert persons to be evaluated, then the average of their evaluations are computed [8].

Objective tests are adopted for testing the performance of the suggested algorithm, and they are Mean Squared Error (MSE), Mean Absolute Error (MAE), Normalized Cross Correlation (NCC), Signal to Noise Ratio (SNR), and Peak Signal to Noise Ratio (PSNR). These measures define the overall error between the original BMP image, and the corresponding BMP watermarked image. This kind of measures can be a good testing tool for quality; Figure (4) shows an example of test images before and after hiding a watermark and Table (1) list object tests for these images.

The signal is the original image and the noise is the errors that are caused by embedded of watermark bits in the cover image. The ratio of signal to noise is high which is good, since value of PSNR is high. Whereas lower values for MSE and MAE, mean lesser error. Signal greater than noise can be produced when SNR ratio is higher than (1:1), while for the NCC, the best value is the closed to 1[15].

The proposed watermarking algorithm in [16] is used to embed a watermark in digital image such that, it can survive against lossy JPEG compression, but it is not use DCT transform or image features.

The proposed watermarking algorithm based on DC and H has two advantages in compare with watermarking algorithm in [16], first one, embedding in DCT transform blocks is more robust to JPEG compression more than other blocks, and the second, this proposed watermarking algorithm requires less time than watermarking algorithm in [16] since it does not need to compares corresponding bytes of original and decompressed images, although it results less hiding rate.

Original Image	*Watermarked Image*
	
Image_1	
	
Image_2	
	
Image_3	

Figure (6): Test images before and after hiding a watermark.

Table (1): Test images before and after watermarking.

Test Image	Watermark Images	MSE	MAE	NCC	SNR	PSNR
Image_1	Image_1	5	0.3	0.99	0.99	39.3
mage_2	Image_2	7.15	0.4	1	1	35.7
Image_3	Image_3	1.8	1.2	1	1	26.3

From the results listed in the above table, it is noted that these metrics give good results for keeping the watermarked image transparent and infernearersimilarity between the watermarked and the original images.

7. Conclusion and Future Works

This paper presents a new watermarking algorithm; the basic concept of this algorithm is to understand image blocks nature by using two measures including H and DC, after analyzing a number of test images using these two measures, it is possible to determine the blocks that can keep their values and stand against JPEG lossy compression. This work can be improved by using Wavelet Transform Domain to obtain robust watermark and to retain image quality, also compressing secret data before embedding in the cover increase the hiding rate.

References

1. Sathik M., and Sujatha S. **"An Improved Invisible Watermarking Technique for Image Authentication"**, International Journal of Advanced Science and Technology Vol. 24, Novembre, 2010.
2. Su P., Wang H. and KuoC.,**"AnIntegratedApproach to Image Watermarking and JPEG-2000 Compression"**, Journal of VLSI Signal Processing 27, 35–53, 2001.
3. Hartung F., Kutter M., **"MultimediaWatermarking Techniques",**Proceedings of the IEEE, Vol. 87, NO. 7, July 1999.
4. Minamoto T. and Aoki K., **"A blind Digital Image Watermarking Method Using Interval Wavelet Decomposition"**, International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 3, No. 2, June, 2010.
5. El-Gayyar M., **"Watermarking Techniques, Spatial Domain, Digital RightsSeminar"**,URL: http://wob.iai.uni-bonn.de /Wob / images /55867298.pdf, May 2006.
6. Pan J., Huang H. and Jain L., **"Intelligent Watermarking Techniques"**, World ScientificPublishing Co. Pte. Ltd., 2004.
7. Wei W., **"An Introduction to Image Compression"**, URL: http://www.unioviedo.es/compnum/transversal_eng/intro_compression.pdf, 2008.
8. Tcheslavski G., **"Image Compression Fundamentals"**, ELEN 4304/5365 DIP, spring 2008.
9. Joancomart J., Minguillon J. and Megias D., **"A Family of Image WatermarkingSchemesbased on Lossy Compression"**, Information Technology: Coding and Computing [Computers and Communications], Proceedings, ITCC 2003. International Conference 28-30 April 2003.
10. Richardson I., **"Video Codec Design, Developing Image and Video Compression Systems"**, John Wiley& Sons Ltd, 2002.

11. Acharya T. and Tsai P.,"**JPEG 2000 Standard for Image Compression Concepts, Algorithms and VLSI Architectures"**, John Wiley& Sons Inc., 2005.
12. Salomon D., **"Data Compression, the Complete Reference, Third Edition "**, Springer, 2004.
13. Khayam S., **"The DiscreteCosineTransform (DCT): Theory and Application"**, ECE 802 – 602: Information Theory and Coding, 2003.
14. Umbaugh S., **"Computer Vision and Image Processing"**, Prentice Hall, 1998.
15. Aliwa M., El-Tobely T., Fahmy M., Nasr M. and Abd El-Aziz M. **" A New NovelFidelity Digital WatermarkingBased on AdaptivelyPixel-Most-Significant-Bit-6 in Spatial Domain Gray Scale Images and Robust",** American Journal of Applied Sciences 7 (7): 987-1022, 2010 ISSN 1546-9239.
16. Nidaa F. Hassan and Ruaa Kadhim Jaber**, "ProposedAlgorithm for Digital Image WatermarkingSurvivalagainst JPEG Compression ",** Eng. & Tech. Journal .Vol.32, Part (B), No.1 , 2014.

اقتراح خوارزميه لإخفاء علامة مائية في الصورة الرقمية تصمد أمام ضغط JPEG بالاعتماد على المجال التحولي و خواص الصوره

أ.م.د.نداء فليح حسن* رؤى كاظم جابر*

المستخلص

في هذا المقترح, تم تقديم خوارزمية جديدة لإخفاء علامة مائية في الصور الرقمية (ذات الامتداد BMP). بعد تجربة مجموعه من الخواص لأجل تحديد الكتل الأفضل ليتم استخدامها كمضيف, تم أختيار الخاصيتين: معامل DC(الناتج من المجال التحولي DCT)والانتروبي (H) Entropy , لأن هاتين الخاصيتين ساعدت في تحديد أماكن الإخفاء التي تسبب اقل انحلال للصورة الغطاء وكذلك في تحديد الكتل القادرة على المحافظة على القيم المخفية بها لتقاوم الضغط. في هذة الخوارزمية ينتج صوره ذات علامة مائية يمكن ضغطها بأستخدام طريقة JPEG (وهو ضغط من النوع الذي يكون مصحوب بخسارة جزء من بيانات الصورة) دون أن تفقد العلامة التي تحملها.

مقاييس الجودة قيمت الأخطاء بين الصورة الأصلية والصورة الغطاء, فقد تم تحقيق نتائج جيده بدون التسبب بانحلال ملحوظ للصورة الغطاء.

*الجامعة التكنولوجية