NON MONO IMAGE WATERMARKING BASED ON THE DCT-DOMAIN OF THREE RGB COLOR CHANNELS

MohmadKashifQureshi*

Abstract:

Color image water marking is becoming more and more important and finding application in different areas of discipline. Developing robust image water marking algorithm which is immune to noise, cropping and compression is aexigent task. Altering the size of the image or its orientation reduces the recoverability of the watermarked imaged .In this paper I proposed a new block of DCT –based digital watermarking scheme based on embedding an adapted watermark in the three RGB channels of the original color image.Voting is used to extract the best candidate pixel value. The proposed embedding procedure improves the imperceptibility and the robustness of the watermarked image against the different attacks such as noise, cropping and JPEG compression. Experimental results have shown the superiority of proposed scheme over a classic DCT watermarking.

Keywords: Image processing, Image recognition, pixel transformation,DCT algorithms,
RGB channels.

IJMRA

* Assistant Professor, Jizan University, Jizan, Saudi Arabia.

I. Introduction

Through Internet it became very easy to obtain, copy, replicate and distribute digital contents without any loss in the quality of digital content.

Unfortunately this course of action became a serious threat to the publishing industries, and industries came into the immediate need for techniques that may protect ownership and from unauthorized access.

To solve this major concern there was evolution of a new information hiding form called Digital Watermarking. The basic idea is to create a metadata containing information about a digital content to be protected, and hide it within that the content of that image. Image watermarking system usually contains at least two components are follows : a watermarking embedding system and watermark extraction(recovery) system . The watermark embedding system takes as input the watermark bits, the image data, and optionally a secret or public key as inputs. The output of the watermark embedding system is the watermarked image. The watermark extraction system takes as input an image that contains a watermark and possibly a secret or public key to detect the watermark. It may also output a confidence measure that indicates the probability with which the extracted watermark is similar to the embedded one.

Digital image watermarking has been subject to research for many year. Some algorithms have relied on Fourier transform as watermarking domain such as [1-3]. Although Fourier based algorithms could perform well against rotation andnoise, they are famous for their computation burden.

Other algorithm used exact histogram exacthistogram specifications[4–5]. The classic and still most populardomain for image processing is that of theDiscrete-Cosine-Transform, or DCT[6–8].

TheDCT allows an image to be broken up into different frequency bands, makingit mucheasier to embed watermarking information into the middle frequency bands of an image.The middle frequency bands are chosen such that they avoid the most visual important parts of theimage (low frequencies) without over-exposingthemselves to removal through compression andnoise attacks (high frequencies) .

2. Classic DCT Technique

The classic and still most popular domain forimage processing is that of DCT. The DCT allows an image to be broken up into different frequency bands,making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression andnoise attacks (high frequencies) [6].One such technique utilizes the comparison ofmiddle-band DCT coefficients to encode a single bitinto a DCT block. To begin, the middle-band frequencies (FM) of an 8x8 DCT block is defined as shown below in fig. 1.

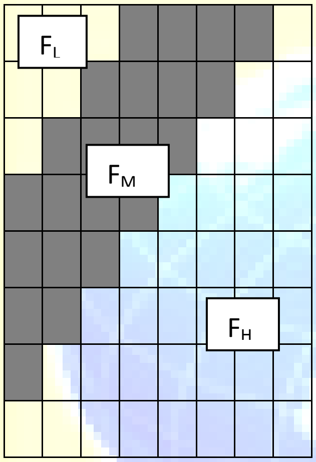


Figure 1 - Definition of DCT Regions

FL is used to denote the lowest frequency components of the block, while FH is used to denote the higher frequency components. FM is chosen as theembedding region as to provide additional resistanceto lossy compression techniques, while avoiding significant modification of the cover image [7]. The next two locations Bi(u1,v1) and Bi(u2,v2) are chosenfrom the FM region for comparison. Rather then arbitrarily choosing these locations, extra robustnessto compression can be achieved if we base the choice of coefficients on the recommended JPEG quantization table shown below in Table(1). If twolocations are chosen such that they have identicalquantization values, there is higher confident that any scaling of one coefficient will scale the other by the same factor preserving their relative size.

Based on the table, we can observe that coefficients (4,1) and (3,2) or (3,2) and (2,3) wouldmake suitable candidates for comparison, as their quantization values are equal. The DCT block will encode a “1” if Bi(u1,v1) > Bi(u2,v2); otherwise it will encode a “0”. The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded [8].

The swapping of such coefficients should not alter the watermarked image significantly, as it is generally believed that DCT coefficients of middle frequencies have similar magnitudes. The robustness of the watermark can be further improved by introducing a watermark “strength” constant k, such that Bi(u1,v1) - Bi(u2,v2) > k. Coefficients that do not meet this criteria are modified though the use of random noise as to then satisfy the relation. Increasing k thus reduces the chance of detection errors at the expense of additional image degradation [8]. As mentioned earlier, in this DCT method each 8x8 block provides one bit to hold the watermark bits. This means that the whole watermarks size can be up to 1/(8x8x8) the size of the original image. On other hand if we assumed that the correlation threshold is 70% then the DCT methods will pass all of these attacks, which means that it’s a robust algorithm

Table 1 - Quantization values used in JPEG compression

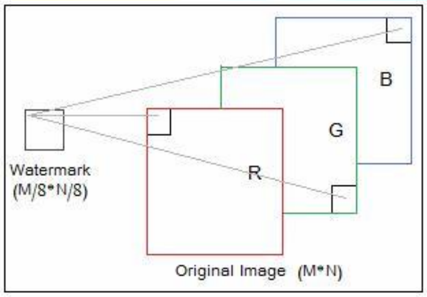
16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

3. Three Channels DCT-Based DigitalWatermarking

This technique can be considered as an improvement of the classic DCT technique. Since we can apply the algorithm mentioned previously in section on the three RGB channels instead of only one of channel, higher robustness can achieved.

3.1. Embedding Process

In this new algorithm each information channels is divided into 8x8 DCT blocks located at different positions. For example if we start with the high left corner block in the R channel , we will use the low right corner block in the G channel and other different location for the first block in the B channel as can be seen in fig.2. The next step is to perform the DCT transform on each three corresponding blocks , to embed the watermarking bit into the middle frequency bands of those blocks as was explained before . Fig.3 shows an outline of the embedding algorithm



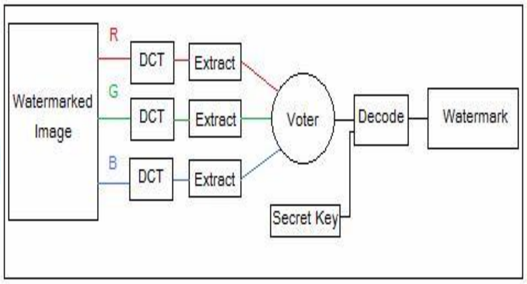


Figure 2- insertion of the first bit value **Figure 3** – The embedding flow chart

3.2. Extraction Process

At first we have to divide the RGB channels into blocks at the same order of the embedding , and then apply the extraction process steps of the classic DCT algorithm on each three corresponded blocks , to extract three possible values for one watermark bit ,which will be used as inputs to a voting process that gives the final value of that bit (one if there are two or more ones and zero if there are two or more zeroes), this is repeated until the hidden text is obtained .

To obtain higher security level, a public/private key can be used to code the embedded bits value by an optional operation , which must be used again after the extraction process to decode the result value and forming the correct watermark. For example, logical ANDing operation between the bit value and the binary secret key bit by bit). Fig.4 shows an outline of the extraction algorithm

3.3. Robustnessagainst Attacks

With this improvement technique we can increase the probability of extracting a correct bit even if the watermarked image has been exposed to an attack such as noise, cropping and JPEG compressing.

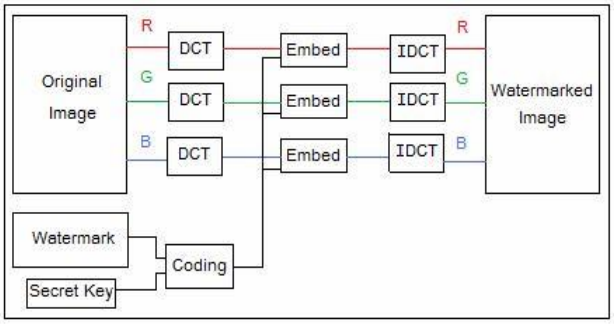


Figure 4 –The extraction flow chart

Since an affected pixel from the watermarked image may cause an error in one of three bit value and the other two values have the chance to make the voter deviate to the correct value. This means that the probability of avoiding such attack will be doubled.

3.4. Experimental Results

The experimental results in Table (2) show that the proposed schemes have higher robustness than the classic one, especially for against noise and higher ratios of lossy compression.

It can be seen from Table (2) that the watermarked image resulted from the two algorithm has the same similarity to the original one, on other hand the correlation factor was considered practically as a measuring parameter to present the different robustness of the two techniques by calculating the cross correlation between the embedded watermark and the extracted one even after different attacks outlined in Table (2).

4. Conclusions

In this paper, we have introduced a novel watermarking method based on the three color channels. The proposed method takes the advantage of localized attacks and tries to embed the watermarks in such a way that the effect of theattacks is minimized. The experimental results have shown the improved performance, compared to the classic method. Moreover, the value of cross-correlation between the watermarked and the retrieved image is improved.

References

[1] Fan Gu, Zhe-Ming Lu and Jeng-Shyang Pan "Multipurpose Image Watermarking in DCT Domain using Subsampling," 2005 IEEE International Symposium on Circuits and Systems, vol.5, pp: 4417-4420, May 2000.

[2] J.R. Hernandez, M.Amado, and F. Perez- Gonzalez,"DCT-Domain Watermarking Techniques for Still Images:Detector Performance Analysis And a New Structure, " IEEE Trans. Image Processing, vol. 9, pp 55-68, Jan. 2000

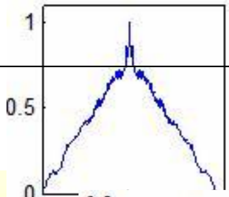
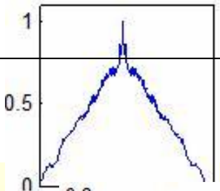
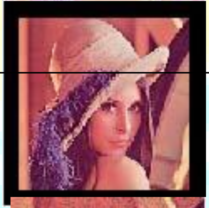
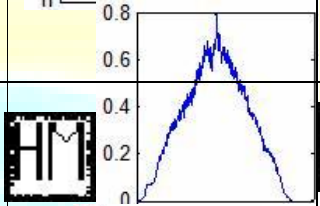
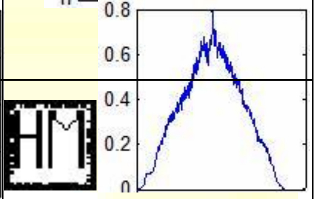
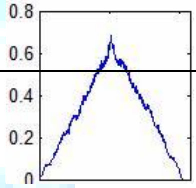
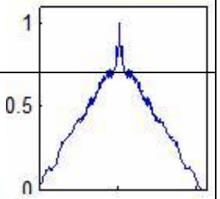
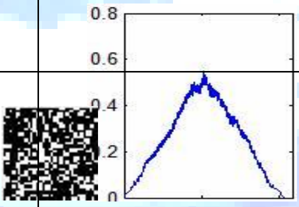
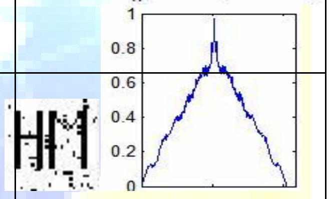
[3] Patrick Bus, Nicolas Le Bihan and Jean-Marc Chassery, "Color Image Watermarking using Quanternion Fourier Transform, " ICASSP, vol.3,524-528, 2oo3

[4] Coltuc, D., and Bolon, Ph.: "Robust watermarking by histogram specification, ICIP'99, vol. 2, pp. 236–239, October 1999

[5] Chareyron, G., Macq, B., and Tremeau, A.: "Watermarking of color images based on segmentation of the XYZ color space" CGIV, pp. 178–182, April 2004

[6] G. Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data, " IEEE Signal Processing Magazine, Vol 17, pp 20-43, September 2000

[7] Zheng, D., Zhao, J., and El Saddik, A.: "RST-invariant digital image watermarking based on log-polar mapping and phase correlation, " IEEE Trans. Circuits Syst. Video Technol, vol. 13, No.(8), pp. 753–765, 2003

The Attack description	Watermarked picture after attack	The Extracted Watermark With One Channel DCT Algorithm	The Extracted Watermark With The Proposed Algorithm
Original image (256*256 pixels) with watermark embedded			
cropping with borders of size = 20 Pixel			
Contaminated with Normal distributed noise (0-10)			
JPEG compress with quality (75%)			
JPEG compress with quality