

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/228412965>

Color image watermarking based on the DCT-domain of three RGB color channels

Article · January 2009

CITATIONS

3

READS

151

5 authors, including:



I. El-Feghi

Misrata University

43 PUBLICATIONS 193 CITATIONS

SEE PROFILE



Zakaria Suliman Zubi

Sirte University

37 PUBLICATIONS 89 CITATIONS

SEE PROFILE



Faraj A. El-Mouadib

University of Benghazi

20 PUBLICATIONS 21 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Deep Learning [View project](#)



Data Mining book in Arabic [View project](#)

All content following this page was uploaded by [Faraj A. El-Mouadib](#) on 31 May 2014.

The user has requested enhancement of the downloaded file.

Color Image Watermarking based on the DCT-Domain of Three RGB Color Channels

I. El-Fegh¹, D. Mustafa², Zakaria Suliman Zubi³, Faraj A. El-Mouadib⁴

¹ Department of Electrical Engineering, Faculty of Engineering, Al-Fateh University, Tripoli, Libya,
<idrivel@gmail.com>

² Department of Electrical Engineering, Faculty of Engineering, Al-Fateh University, Tripoli, Libya,
<dimdream@hotmail.com>

³ Computer Science Department, Faculty of Science, Al-Tahadi University, Sirt, Libya,
<Zszubi@yahoo.com>

⁴ Computer Science Department, Faculty of Information Technology, Garyounis University, Benghazi, Libya,
<elmouadib@yahoo.com>

Abstract: *Color image water marking is becoming increasingly important and finding application in diverse areas of discipline. Developing robust image water marking algorithm which is immune to noise, cropping and compression is a challenging task. Altering the size of the image or its orientation reduces the recoverability of the watermarked image. In this paper, we proposed a new block DCT-based digital watermarking scheme based on embedding an adapted watermark in the three RGB channels of the original colour 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 superiority of the proposed scheme over a classic DCT watermarking.*

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

I. Introduction

A recent proliferation and success of the Internet, together with availability of relatively inexpensive digital recording and storage devices have created an environment in which it became very easy to obtain, replicate and distribute digital content without any loss in quality. This has become a great concern to the multimedia content (music, video, and image) publishing industries, making an urgent need for techniques that will to help establish and prove ownership rights, track content usage, ensure authorized access, facilitate content authentication

and prevent illegal replication. This need attracted attention of research community and industry leading to the creation 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 the following two components; a watermark 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 and noise, they are famous for their computation burden. Other algorithm used exact histogram exact histogram specifications[4-5].

The classic and still most popular domain for image processing is that of the Discrete-Cosine-Transform, or DCT[6-8]. 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 and noise attacks (high frequencies) .

2. Classic DCT Technique

The classic and still most popular domain for image 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 and noise attacks (high frequencies) [6].

One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, the middle-band frequencies (FM) of an 8x8 DCT block is defined as shown below in fig. 1.

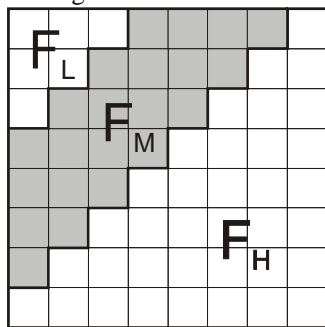


Figure 1 - Definition of DCT Regions

F_L is used to denote the lowest frequency components of the block, while F_H is used to denote the higher frequency components. F_M is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image [7]. The Next two locations $Bi(u_1,v_1)$ and $Bi(u_2,v_2)$ are chosen from the F_M region for comparison. Rather than arbitrarily choosing these locations, extra robustness to compression can be achieved if we base the choice of coefficients on the recommended JPEG quantization table shown below in Table(1). If two locations are chosen such that they have identical quantization values, there is higher confidence 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) would make suitable candidates for comparison, as their quantization values are equal. The DCT block will

encode a “1” if $Bi(u_1,v_1) > Bi(u_2,v_2)$; 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 $Bi(u_1,v_1) - Bi(u_2,v_2) > k$.

Coefficients that do not meet this criteria are modified through 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 watermark size can be up to $1/(8 \times 8 \times 8)$ the size of the original image. On the 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 Digital Watermarking

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 be 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

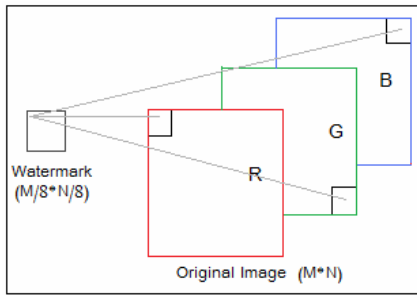


Figure 2- insertion of the first bit value

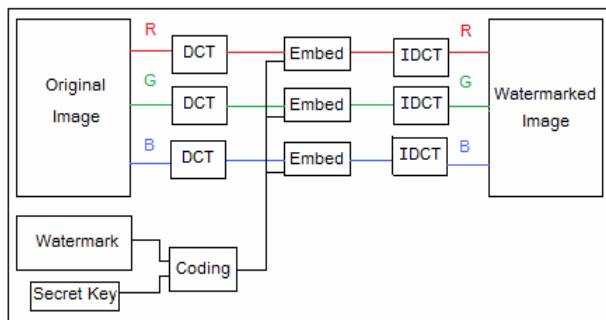


Figure 3 – The embedding flow chart

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. Robustness Against 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 .

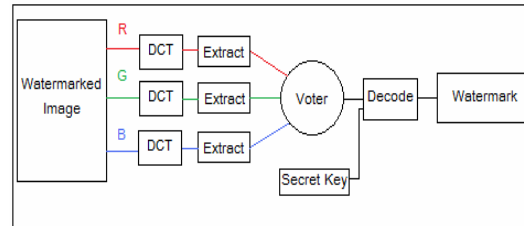


Figure 4 –The extraction flow chart

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 scheme 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 the attacks 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] Lin, C.Y., Wu, M., Bloom, J.A., Cox, I.J., Miller, M.L., and Lui, Y.M.: "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. Image Process.*, vol. 10, pp. 767-782, 2001
- [2] 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
- [3] Patrick Bus, Nicolas Le Bihan and Jean-Marc Chassery, "Color Image Watermarking using Quaternion Fourier Transform," *ICASSP*, vol.3,524-528, 2003
- [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] 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
- [8] 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 2005.

Table 2. Comparison of proposed and classic DCT algorithms with the correlation between the retrieved image and the original image

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			