International Journal on
Advanced Science
Engineering
Information Technology

Vol. 2 (2012) No. 1
ISSN: 2088-5334

A Digital Image Watermarking Method in the Discrete Cosine Transformation Domain

Mohammad Reza Khammar, Yunusa Ali Saied, M. H Marhaban

Electrical and Electronic Department, Faculty of Engineering
University Putra Malaysia, 43400 UPM Serdang, Selangor
E-mail: khammar_m@yahoo.com, yunusaalisaid@yahoo.com, hamiruce@eng.upm.edu.my

***Abstract*— In this paper, a watermarking method has been proposed based on Discrete Cosine Transform(DCT) which can be used in order to protect copyrighting and to provide right of image ownership. In this method, the original image transferred to DCT domain after dividing into non-overlapped blocks 8×8 and to the same method, watermark image which can be whether a firm mark or any desired image from owner of the art work, after dividing into non-overlapped blocks 4×4, transferred to DCT domain. Watermark image coefficients after one step coding composed with low frequency coefficients of original image and create the final watermark image. On the other hand, the process of reforming watermarked image and extracting the original watermark on the secondary side is extractable by using original image and with reverse mechanism. Experiments show that this method in encountering with a number of routine attacks has a good resistance.**

***Keywords*— image; watermarking; discrete cosine transform**

I. INTRODUCTION

Development of information communication technology (ICT) infrastructure in the societies have made available multimedia products and provide possibility of entrance and occupation on these products, this has imposed moral and financial hurts on owners of products, this cause to create a new headline in order to creating methods for proving ownership right and preventing copyrighting multimedia products.

In fact, the aim of watermarking is, hiding one message or special information related to provider in different desired firms in original signal, for proving ownership right and preventing spoiling rights of providers of their products which is obvious that these goods can include special graphical outcomes, images, texts, or audio and video signals [1].

In order to protect images, that is based on this article, many past methods were popular, a well-known method has been putting a watermark like a signature on the corner or bottom of image. In fact, this method has been simple and of course it was visible and so it can be deleted from the original image by a simple cropping and acting some reforms with advanced software such as Photoshop.

Therefore, moving forward in the field of information hiding, achieving stability of any methods against intentional and unintentional attacks, has shown it importance. In other words, we are following a mechanism that can observe parameters set totally as follows capacity, robustness, transparency, security, computational simplicity [2] [1].

Accessing to all above-factors in a technique, is difficult, so practicing a series of compromises is done in every method, probably most important headlines of the compromise can be seen in the triangle figure 1 below [3].

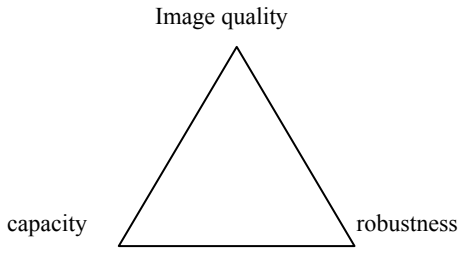

Figure 1 three important parameters in watermarking systems

In order to improve any parameter in the triangle, there must be a trade-off. So, different proposed methods are criticizable and verifiable in this respect. The most important division are implementation in special domain and transform domain, in order to implement watermarking.

The earliest method is related to hiding in special domain and in these methods an image pixels are affected directly. An example of these techniques is called least significant bits (LSBs) in which watermark image that does not has

much role in final quality of image because of its location for embedding [1]. The method possesses minimum embedding capacity and meanwhile is apt for destroying as most easy as possible.

Second method refers to transform domain which is more powerful and has the better properties in image watermarking. Naturally, in this field, the embedding capacity is improved and also the ability of algorithms in this way to encountering to some attacks are promoted, however, desired point in hiding process needs methods with stability in encountering with general attacks. The effort that has not been ascertained comprehensively so far and basically it needs more research. Meanwhile, as previously mentioned, complexity of watermarking system is a special important factor in embedding and extracting procedures.

Using transformations such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Wavelet and Ridgelet etc are current issues in this area. In this article, DCT method has been implemented for embedding watermark algorithm. In section 2 DCT methods was presented, section 3 shows circumstance of embedding and extracting watermark, section 4 presents experimental results, and final conclusion in section 5.

II. Discrete Cosine Transformation, Theory and Its Application

DCT is a summation of a finite numbers of cosine functions in different frequencies, which is shows the identification of processed signal. DCT transformation like others, intend to reduce existed redundancy in special domain for adjacent pixels in transform domain, and prepare some independent coefficients in the new domain [4]. This transformation can move information of any image to a space with minimum numbers of independent coefficients, so it can help to compress data with regards to maintain of valuable image information. The studies have been shown that the energy compaction based on DCT for the most images presented a better result than DFT and it is possible to show the suitable equivalent of energy in the lower numbers of coefficients [4].

The DCT is a separable transform which is useful to divide a two dimension process in two individual dimensions, for example first on the rows and then on the columns of a given image or vice versa, as a two dimensional function and because of its symmetry, there is no difference to start scanning in vertical or horizontal direction [5]. Another property of the transform is that, its basic functions are orthogonal and therefore it prepares whatever more eases to process of forward and reverse transformation in term of calculation and reduce the computational complexity [6].

The most important point in distinction of DCT and DFT that is, after implementation DFT, the result will be a complex function with amplitude and phase but for DCT, just a function with real coefficients is observable [1]. For these reasons and regarding to the variety of properties of the DCT transformation that it is useful tool in different applications of image processing, such as image compression in JPEG and etc.

The equations of two dimensional discrete cosines transform (DCT), And inverse discrete cosine transform (IDCT), are given below in order [1], [6].

$$C(u,v) = a(u).a(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y).cos[\frac{(2x+1)u\pi}{2N}].cos[\frac{(2y+1)v\pi}{2N}]$$

u,v=0,1,…..,N-1 (1)

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{V=0}^{N-1} a(u).a(v).C(u,v).cos[\frac{(2x+1)u\pi}{2N}].cos[\frac{(2y+1)v\pi}{2N}]$$

x,y =0,1,2,…,N-1 (2)

In this article, DCT has been used for watermarking image, original image with dimension (512×512) divided into non-overlapped blocks and then DCT is taken for each block. According to the size of selecting block, 8×8, the numbers of block which cover the whole image is 4096. Each block includes one DC coefficient which is coming from the average of the whole 64 values of every given block and its located at the top left of the block, the rest 63 locations are called AC coefficients which denote the tolerance and variation of original values of each given block.

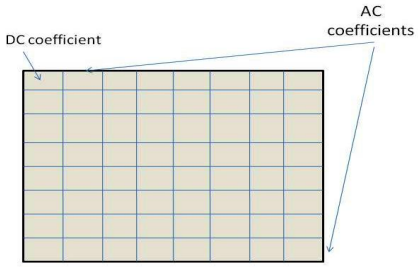

Figure 2 a block of original image with regards to AC and DC coefficients

Figure 2 shows a block of image. AC coefficients close to DC value expresses the low frequencies and then mid frequency, and others refer to high frequencies coefficients, it means that the distant coefficients expressing high frequencies existed in the given block and of course the values of these locations are not so big and we can ignore them in image compression [6].

III. Describing the Proposed Algorithm

A. Embedding algorithm using DCT

In order to embed watermark image in host image, assumed that image has been a grayscale with dimension of 512×512 and so watermark image is also grayscale with dimension of 128×128. The needed steps given as observed for embedding procedure.

Step 1: Resize and convert the original image and watermark image to grayscale image with size of 512×512 and 128×128, respectively.

Step 2: Perform a simple coding in one process on the watermark image in order to improve safety and preventing of observation of watermark image by a non-responsible individual.

Step 3: Dividing main image to blocks 8×8 and calculating DCT transform and preparing a stream from DCT coefficients.

Step 4: Dividing watermark image to blocks 4×4 and calculating DCT transform and preparing a stream from

DCT coefficients and then multiplying coefficients by value α.

α is an important constant that its value can effect perceptual quality of host image in order to get a powerful watermark in encountering with types of attacks, we need a large α, and, on the other hand, being large of it, can scratch main image quality, therefore, in fact, a compromise should done in selecting α[4].

Step 5: Make a new stream of coefficients regards to the coefficients of previous step and low frequency coefficients from host image for each block.

$$w_{ij} = a_{ij} + \alpha.b_{ij}$$

Step 6: Reconstructing watermark image that is a new compound and following some activities like Desizag and IDCT and also putting blocks in a proper area of compatible with the original image. Figure 3 shows different parts of watermark embedding system.

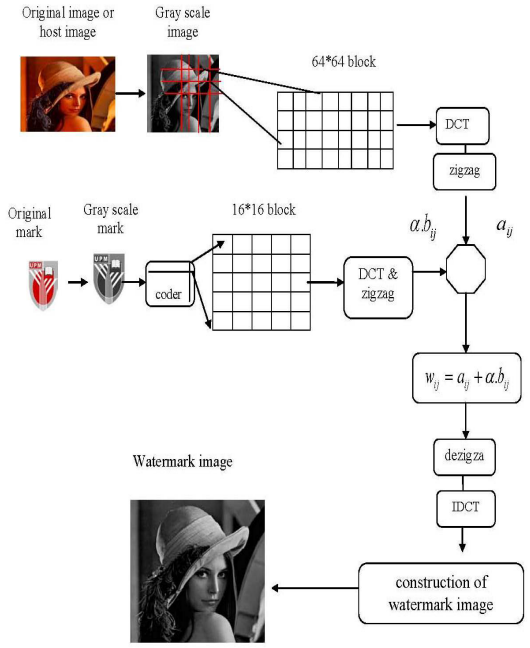

Figure3: watermark embedding system

Tests implemented on images such as Lena, Cameraman, and fruit and also the watermark image is a part of logo of Putra University of Malaysia. Figure 4 shows the original watermark image.

Figure 4 : Original watermark

B. *Extracting algorithm*

Extracting watermark from host image includes some familiar steps which was discussed in previous section so have been explained briefly.

Step 1: Dividing watermarked image which is contaminated by noise or changed in term of quality based on some intentional or unintentional attacks into non-overlapping blocks and calculates the appropriate coefficients in order to yield the original watermark.

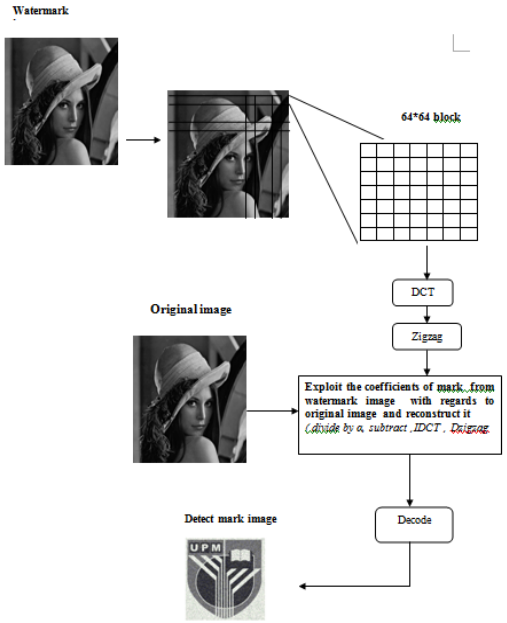

Figure 5: extraction watermark

The original host image is needed in this section to help us to get the desired coefficients via comparing coefficients obtained, with coefficients of original image without acting watermark.

Step 2: Recovery of watermark image via some activities like Dezigzag , IDCT and etc

Step 3: Decoding the result of previous step to get the watermark image which will be similar in term of appearance with the original watermark image.

Figure 5 shows important parts of extracting watermark system. The presented algorithm is simulated in term of embedding and extracting by MATLAB. In order to verifying quantitatively results obtained, in multiple experiments, MSE and PSNR have been used. The Peak Signal to Noise Ratio (PSNR) is utilize to calculate the similarity between the original image and watermarked host image. This factor is presented below [5].

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N} \quad (3)$$

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right) \quad (4)$$

The MSE (mean square error) will compute firstly and then the value for PSNR will be available secondly. Here $I_1(m,n)$ and $I_2(m,n)$ respectively represent the gray values of original host and the watermarked images (R=255).

IV. EXPERIMENTAL RESULTS

Tests implemented on some popular images with regards to watermark image which is a part of UPM logo. Figure 4 shows the two inputs (first row) and outputs (second row) for the given host image ("cameraman").

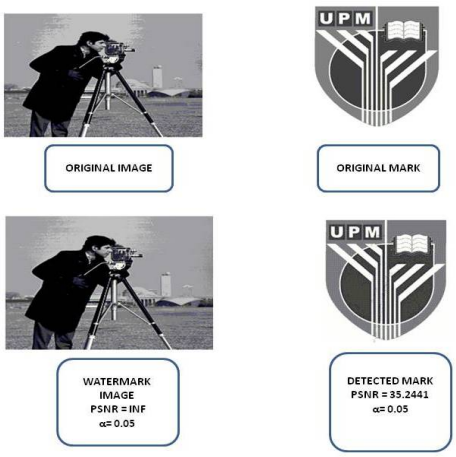

Figure 6 original image and watermark

The experimental results show that increasing the value of α can make some bad effects on the watermark host image and the watermark image will be visible. On the other hand, α=0 denoted to cancel the role of watermark from our subject, so, for this reason, we should find a tradeoff. Figure 7 shows how we can see the watermark in the watermark host image which is not good. Therefore, we selected α = 0.05 as a suitable value for the rest exercises.

Figure 7 variation of α in watermark host image

In this section, some experimentation results have been presented to show robustness of the proposed method. The experimentation reveals that the results are quite good in most applications.

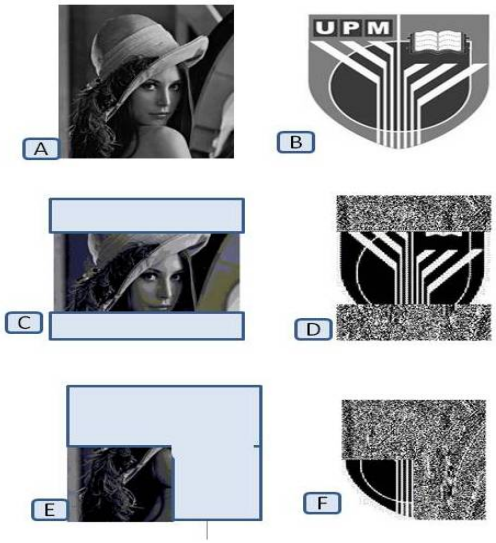

Figure 8 watermark host image (A), detected watermark without any attacks (B), and the rest C, D, E, F shows the cropping attacks and the results

In continue, we study verifying resistance of selective algorithm, about part of attacks. Figure 8 illustrated geometric cropping attacks on image in different modes, in all of them; there is possibility of viewing initial watermark image. From the quality of watermarked images and the values of PSNRs, we can conclude that the presented method provide good invisibility while retaining good PSNR.

Another subject that is important in communication of images is image compression techniques. They can change the original image and make a new one with lower capacity which will be more flexible to move from channels and present an optimum sending criterion. so in this particular way, it is possible we lost our watermark which is embedded in the host image, therefore, it is essential that watermarking methods resist against it and causes of deletion or scratching initial watermark would not be prepared.

Figure 9 presents the results after JPEG compression and table 1 shows value of PSNR and also watermark image capacity in different modes of compression.

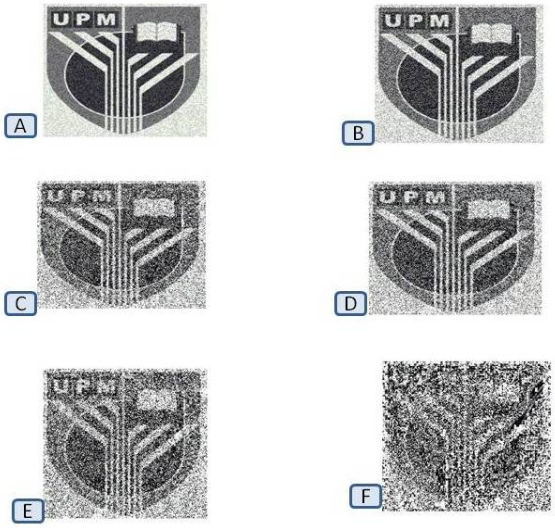

Figure 9 : The extraction mark after JPEG compression A,B,C,D,E,F, for 90% , 80% , 60%, 50%, 40 %, 20% , respectively

TABLE 1: THE CHANGES OF PSNR AND WATERMARK CAPACITY

	20%	**40%**	**50%**	**60%**	**80%**	**90%**
PSNR	30.77	31.01	31.01	31.12	31.67	32.89
Watermark capacity (kB)	10.9	16.8	19.6	22.8	36.1	56.9

Table 1 presents PSNR values and the capacity of watermark image after compression (the original capacity of host image was around 270KB) for different scales of compression. However, we reduced the size and change the quality of host image which extracted the watermark as well.

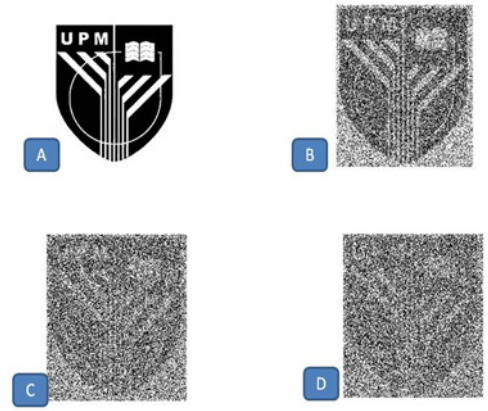

Figure 10 The extracted watermarks from the Gaussian noise contaminated watermarking images

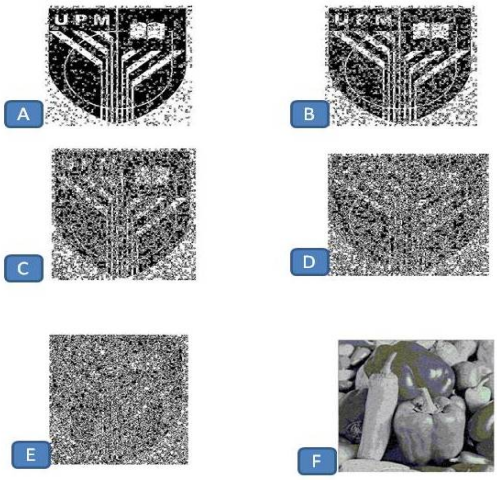

Figure 11 The extracted marks from the salt and pepper noise contaminated watermarking images

Another important subject is noise contamination which changes the properties of watermark image and so it will be difficult to extract the watermark. The watermark extracted from the watermarking images which are contaminated by Gaussian noise whose average value is zero and variance changes 0 , 0,0001,0.0004, 0.0006 and salt and pepper noise whose strength is from 0.005 ,0.01 , 0.02 ,0.03, 0.04 , which are shown in figure 10 and 11 , respectively.

V. Conclusions

In this paper, a digital image watermarking embedding algorithm based on DCT is proposed. After the preparation of the low frequency coefficients of every block of host image, the watermark is embedded in the frequency domain. Experimental results show robustness of the present scheme on many attacks.

References

[1] I. Cox, M. Miller and J. Bloom. Digital watermarking: principles and practice. Morgan Kaufmann Publishers, USA, 2002.

[2] Hsu C T,Wu J L (1999),Hidden digital watermarks in images". International Journal of IEEE Trans Image Processing .Vol. 8,No. 1,pp.58-68.

[3] M. Barni, F. Bartolini, V. Cappellini, A. Piva, "A DCT-Domain System for Robust Image Watermarking", Signal Processing, Vol. 66, No. 3, pp. 357-372, 1998

[4] JIANG Ming,SUN Shui-fa,ZHENG Sheng (2008). "Digital image watermarking based on relationship of coefficients in DCT domain". Journal of Computer Engineering and Applications, Vol. 44, No. 5, pp.125-127.

[5] FENG Mao-yan, FENG Bo, SHEN Chun-lin (2008). "Adaptive image watermarking algorithm based on block DCT transform and Arnold shuffling". Journal of Computer Application, Vol. 28, No. 1, pp.171-173.

[6] M. A. Suhail, M. S. Obaidat, "Digital Watermarking-Based DCT and JPEG Model," IEEE Trans. Instrumentation and Measurement. vol. 52, no. 5, pp. 1640-1647, Oct. 2003.