Digital Watermarking Using DCT Transformation

Wen Yuan Chen and Shih Yuan Huang

Department of Electronic Engineering
National Chin-Yi Institute of Technology

Abstract

Owing to personal computers being applied in many fields and Internet becoming popular and easier to use, most information is transmitted with digital format. Therefore, data copying and back up are more and more easier in the world wide web and multimedia. The copyright and authentication gradually lose their security. How to protect intellectual property becomes important in technical study and research. Recently, the watermarking technique was proposed to solve the problem of protecting the intellectual property.

In this paper, a watermark embedded in the host image by DCT transform has been proposed. There are several papers using the same manner to embed watermark into middle-band coefficients of DCT block. The Joint Photograph Expert Group (JPEG) image compression usually discards the high-band frequency in DCT block including some middle-band data. In this paper the lower-band coefficient of DCT block was employed, since it is robust against the attack by the JPEG. In order to improve the imperceptions, only one bit was embedded in each coefficient of a DCT block. The experimental results show the proposed approach is correct.

Keywords – Discrete Cosine Transform (DCT), Frequency Domain, Joint Photographic Experts Group (JPEG), Robust, Transparency.

1. Introduction

Since, Computer and Internet make the world become digitization. Most information is easy to transmit and duplicate but unauthorized reproduction becomes a serious problem. Unlike the traditional visible watermark found on paper, the dispute here is to introduce a digital watermark that does not vary the perceived quality of the image content. Watermarking is a potential method to discourage

unauthorized copying or attest the origin of the image. Generally, digit watermarks must satisfy the following requirements.

a. Imperceptible

The watermark should be imperceptible to human observe while the host image is embedded with secret data and illegal removal of watermark must be impossible.

b. Secure and reliable

The embedded watermark cannot be deleted and retrieved from the host image, even if the embedded algorithms are known.

c. Robust

The watermarked image must be resistant encounter any type of signal and geometric distortion processing. The watermark can survive from all of the international attacks like as JPEG compression, cropping and resizing.

d. **Unambiguous**

The objective of watermarking technique includes author identification, verification, and copyright protection. The watermark logo must be unambiguously identifying the owner.

The watermarking techniques can be classified into two categories: one is processed in spatial domain and the other is accomplished in transform domain. In the spatial domain [1-3], visual modes derived from data compression are very suited for the digital watermarking situation. Many great performance of perceptual coding is based on the just noticeable distortion (JND), so there are many papers based on JND to embedded watermark into host image [11,12]. A number of data embedding techniques are based on the method of replacing the least significant bits in the pixels of the host image and a pseudo-random number system is usually used to the security task.

Many approaches [4-6], based on the Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) in which watermarks are embedded in transform domain [7-9]. The Discrete Fourier transform (DFT) is another method in transform domain to hidden watermark based on polar map for the accurate and efficient recovery image [13]. The proposed approach is also hiding watermark in transform domain.

This paper is organized as follows. In Section 2, some watermarked images embedded into the lower band coefficients of DCT in host image will be discussed. The embedding approach is described in Section 3, and the extraction method is

presented in Section 4. Experimental results are found in Section 5. Finally, conclusions are presented in Section 6.

2. The Discrete Cosine Transform

The DCT is a very popular transform function used in signal processing. It transforms a signal from spatial domain to frequency domain. Due to good performance, it has been used in JPEG standard for image compression. DCT has been applied in many fields such as data compression, pattern recognition, image processing, and so on. The DCT transform and its inverse manner can be expressed as follows:

$$F(u,v)=\frac{4C(u)C(v)}{n^2}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1}f(j,k)\cos[\frac{(2j+1)up}{2n}]\cos[\frac{(2k+1)vp}{2n}], \quad (1)$$

$$f(j,k)=\sum_{u=0}^{n-1}\sum_{v=0}^{n-1}C(u)C(v)F(u,v)\cos[\frac{(2j+1)up}{2n}]\cos[\frac{(2k+1)vp}{2n}], \quad (2)$$

where

$C(w)=1/\sqrt{2}$ when w =0

$C(w)=1$ when w =1,2,3,… $n-1$

As an image transformed by the DCT, it is usually divided into non-overlapped $m\times m$ block. In general, a block always consists of 8×8 components. The block coefficients are shown in figure 1. The left-top coefficient is the DC value while the others stand for AC components. The zigzag scanning permutation is implied the energy distribution from high to low as well as from low frequency to high frequency with the same manner. The human eyes are more sensitive to noise in lower-frequency band than higher frequency. The energy of natural image is concentrated in the lower frequency range. The watermark hidden in the higher frequency band might be discarded after a lossy compression. Therefore, the watermark is always embedded in the lower-band range of the host image that transformed by DCT is perfect selection. The lower-band coefficients of DCT block are described as in Figure 2.

3. The Proposed Embedding Algorithm

In our approach, an original gray-level image of size $(N \times N)$ is divided into $n = (N \times N)/(8 \times 8)$ non-overlapped blocks (8×8) which are transformed to frequency domain by the DCT. Each block has 64 coefficients as shown in Figure 1. The watermark bit stream is embedded into eight coefficients in lower band of each block shown in Figure 2.

For the purpose of scattering watermark into the host image and prompting security, we use pseudo random system to generate a random position in watermarking algorithm. The secret number is as a seed to feed into pseudo random number system in which a size of n $(N \times N/64)$ non-repeated random numbers is generated. Since it is time consumption in the pseudo random number system, we can calculate the random number set with off line manner. The processing of embedding watermark is described below.

1. Sequentially extract out every 8-bit data from watermark-bit-stream.
2. Obtain a random number, generated by pseudo random system, which points to one of n blocks of host image.
3. Embed extracted the 8-bit watermarking data into the 8 lower-band coefficients in the block pointed by previous step.
4. Repeat step 1 to step 3, until the watermark bit stream is run out.
5. The proposed employee replace bit to embedded watermark bit stream, and it was hidden at position bit 3 in the selected 8-bit coefficient. If the watermark bit is "1" then bit 3 to "1" otherwise "0".

The detail embedding process is shown in Figure 3.

4. The Extraction Algorithm

The extraction step of watermark from host image is similar to the process of the embedded algorithm. We use the same set of random number, which is applied in the embedded strategy. The watermarked image must be transformed to frequency domain by DCT approach. The 8-bit watermark data of each DCT block will be extracted by mean of the inverse step that is embedded. Once all of the 8-bit watermark data are extracted, we rearrange the watermark bit stream to configure the original watermark image as soon. The exaction step is described below.

1. Transform the watermarked image to frequency domain by DCT.
2. Use the same set of random numbers, which is applied in the embedding process.
3. Apply the random number to find the exact location of the DCT block in the watermarked image.

4. Extract 8-bit watermark data from each DCT block by means of the inverse embedded. The watermark bit is “1” when bit 3 is “1” of selected DCT-block coefficient otherwise the watermark bit is “0”.
5. Rearrange the 8-bit data into watermark image.

The extraction algorithm is shown in Figure 4.

5. Experimental Results

5.1 Peak Signal Noise Ratio (*PSNR*) Measurement

The watermark should be imperceptible to human observation while the host image is embedded with secret data. How to get a method to measure the host image imperceptible is important. In this paper we employee the $PSNR$ to indicate the transparency degree. The $PSNR$ describe below

$$PSNR = 10\log_{10}\frac{255^2}{\frac{1}{N\times N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(x_{i,j}-\hat{x})^2} \tag{3}$$

where $x_{i,j}$, $\hat{x}_{i,j}$, are the gray-scale values of host and watermarked images and $N\times N$ is the size of image respectively.

5.2 Experimental results

Experimental results of the proposed data embedding and extraction are presented and discussed in this section. Two 8-bit images with a size of 64×64 “NCIT” were simulated. Imperceptible or transparency can be obtained from the $PSNR$ of embedded image.

The original image “Lena” with a size of 512×512 is shown in Figure 5(a). Embedded image was shown in figure 5(b). It cannot be found any difference by human vision. The embedded images compressed by JPEG method with quality 90%, 70%, painting, and cropping are shown in 5(c) to 5(f) respectively. The watermarked images attacked by JPEG compression method with quality 90%, 80%, 70%, and cropping and painting are shown in Figures 6(a) to 6(f).

Table 1 shows the transparency performance of the watermarked image. Most approaches embedded the hidden data into the middle band of the DCT block. In the proposed method, the bit stream is hidden in the lower band. Table 2 shows the performance comparison between the other’s scheme [14] and the proposed scheme. From the experimental results, the transparency performance is improved.

6. Conclusion

Many of watermarking techniques have presented in spatial domain and transform domain. The performance of watermarking is upgraded day by day. In this paper the watermarks were embedded the lower band of the DCT block in the host image. the pseudo random system are used to generate a scatter random number in order to enhance the security.

Since the 3-dimension image and digital movies such as DVD are widely applied in computer and Internet, the protection of authentication and copyright in the video image are very important. The owner will be grade to post his products in Internet if the copyright is protected. Due to the video being real-time playing, a good performance and fast algorithm based the proposed approach for watermarking in the video will be our future research.

References

[1] O. Bruyndonckx, J. J. Quisquater, and B. Macq, "Spatial method for copyright labeling of digital images," in Proc. *IEEE Nonlinear Signal and Image Processing*, pp. 456-459, June., 1995 .

[2] W. N. Lie, and L. C. Chang, "Spatial-Domain Image Watermarking By Data Embedding At Adaptive Bit Position," *IPPR Conference on Computer Vision, Graphics and Image processing*, pp. 16-21, 1999..

[3] S. C. Pei, Y. H. Chen and R. F. Torng, "Digital Image and Video Watermarking Utilizing Just-Noticeable-Distortion Model," *IPPR Conference on Computer Vision, Graphics and Image processing*, pp. 174-182, 1999.

[4] C. T. Hsu and J. L. Wu, "Hidden Digital Watermarks in Images," *IEEE Trans. On Image Processing*, vol. 8, no. 1, pp. 58-68, Jan., 1999.

[5] C. T. Hsu and J. L. Wu, "DCT-Based Watermarking for Video," *IEEE Trans. On Consumer Electronics*, vol. 44, no. 1,pp. 206-216, Feb 1998.

[6] M. Barni, F. Bartolini, V. Cappellini and A. Piva, "A DCT-Domain system for robust image watermarking," *Signal Processing*, vol. 66, pp. 357-372, 1998.

[7] M. J. Tsai, K. Y. Yu and Y. Z. Chen, "Joint Wavelet and Spatial Transformation for Digital Watermarking, " *IEEE Trans. On Consumer Electronics*, vol. 46, no. 1, pp.241-245, Feb 2000.

[8] Z. H. Wei, P. Qin and Y. Q. Fu, "Perceptual Digital Watermark of Images Using Wavelet Transform," *IEEE Trans. On Consumer Electronics*, vol. 44, no. 4, pp.1267-1272, Nov., 1998.

[9] H. Inoue, A. Miyazaki, A. Yamamoto, and T. Katsura, "A Digital Watermark Technique Based on the Wavelet Transform and Its Robustness on Image

Compression and Transformation," *IEICE Trans. Fundamentales*, vol. E82-A, no. 1, pp. 2-10 ,Jan 1999

[10] A. E. Jacquin, "Image Coding Based on a Fractal Theory of Iterated Contractive Image Transformation," *IEEE Trans. On Image Processing*, vol.1, no. 1, pp. 18-30, Jan 1992.

[11] C. H. Chou, and Y. C. Li, "A Perceptually Tuned Subband Image Coder Based on the Measure of Just-Noticeable-Distortion Profile," *IEEE trans. on circuits and systems for video technology*, vol 5,no. 6 pp. 467-476, 1995.

[12] C. I. Podilchuk, and W. Zeng, "Image-Adaptive Watermarking Using Visual Models", *IEEE Journal on selected areas in communications*, vol. 16, no. 4, pp.525-539,

[13] S. Pereira, and T Pun, "Robust Template Matching for Affine Resistant Image Watermarks", *IEEE trans. On Image Processing*, vol. 9, no. 6, pp. 1123-1129, 2000

[14] C. H. Chou and C. C. Hsieh, "Robust Image Watermarking Based on the Just Noticeable Distortion Profile", *IPPR Conference on Computer Vision, Graphics and Image processing*, pp. 182-188, 2000.

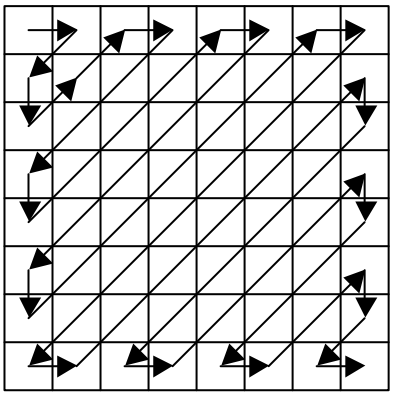


Figure 1. The DCT block coefficient and zig-zag

	1	5	6				
2	4	7					
3	8						

Figure 2. The eight lower -band coefficients.

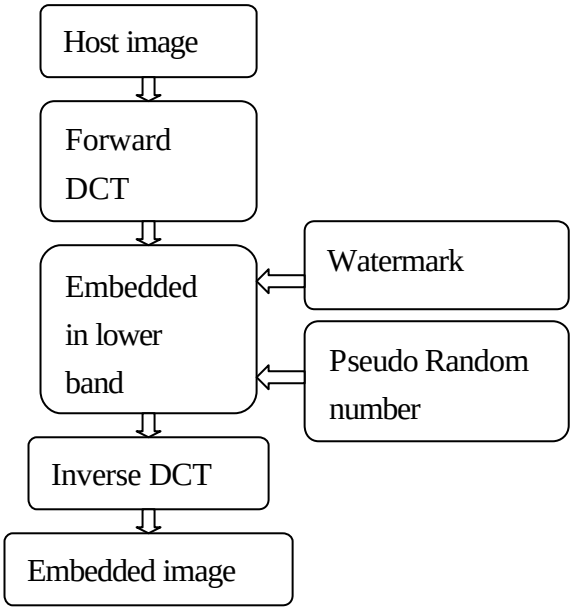


Figure 3. The embedded flow chart

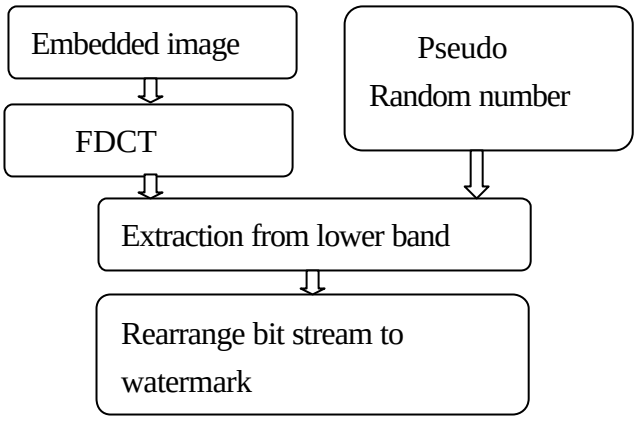


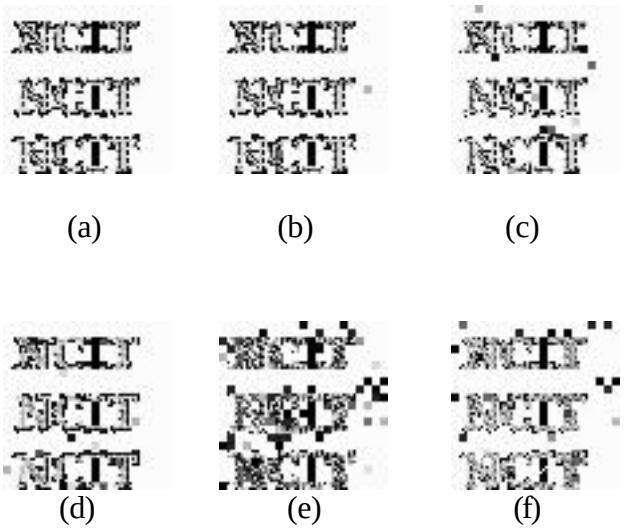
Figure 4. The extracted flow chart.

(a) (b)

(c) (d)

(e) (f)

Figure 5. Test images for several attacks: (a) Original image; (b) Embedded image; (c) JPEG 90% quality; (d) JPEG 70% quality; (e) Painting; and (f) Cropping.



(a) (b) (c)

(d) (e) (f)

Figure 6. Test image "NCIT": (a) Watermark "NCIT" through JPEG 100%; (b) JPEG 90% quality; (c) JPEG 80% quality; (d) JPEG 70% quality; (e)Cropping attack; and (f) painting attack.

Table 1. the PSNR of watermark embedded.

Embedded image	Watermark	PSNR
Lena	NCIT	42.15
Pepper	NCIT	43.1167

Table 2. the PSNR comparison of watermark embedded.

Embedded Approach	Embedded Image	PSNR
JND Approach A	Lena	40.438
JND Approach B	Lena	40.426
Proposed method	Lena	42.15
Proposed method	Pepper	43.1167

數位餘弦轉換域之數位浮水印隱藏技術

陳文淵　黃世演

國立勤益技術學院電子工程系

摘要

由於個人電腦與網際網路(Internet)發達，大部分的資訊都數位化，任意的拷貝或在網路上傳輸都很容易，因而造成著作權(Authentication)，與所有權(Copyright)逐漸的失去保障。而數位浮水印的技術是保障著作權，與所有權最有效的方法。

在這篇論文中，我們提出一種新方法，可將原始影像(Host Image)經過數位餘弦轉換(Discrete Cosine Transform)後，隱藏一個浮水印(Watermark)資料。在這之前已有多篇論文採用相同的方法將數位影像轉換至頻率域(Frequency Domain)，然後才藏入浮水印資料，但是為了防止檔案壓縮後浮水印資料被破壞，所以都將浮水印資料隱藏在 DCT 區塊的中頻段(Middle Band)。但經研究影像壓縮標準(Joint Photographic Experts Group, JPEG)的壓縮技術後發現，浮水印資料隱藏在 DCT 區塊的中頻段仍然不夠安全，也很容易受到 JPEG 壓縮後而被消除，或變得很差.然而經本論文研究發現將浮水印資料隱藏在 DCT 區塊的低頻段(Lower Band)，具有較佳的強韌性(Robust)，而且本論文採用每一個 DCT 區塊系數最多只隱藏一個位元(BIT)，所以使得隱藏後的影像(Watermarked Image)，絲毫看不出有任何的改變，也就是不可感知性(Imperceptible)很高，或稱為透明度(Transparency)很好。實驗結果也印證了本論文的說法。

關鍵字: 數位餘弦轉換(DCT)，頻率域(Frequency Domain)，靜態影像壓縮標準(JPEG)，強韌性(Robust)，透明度(Transparency)。