A Study on a Digital Watermarking Method for Still Images

Tomokazu Onuki [†], Takeharu Adachi [†], Madoka Hasegawa [††], and Shigeo Kato [††]

[†] Graduate School of Engineering, Utsunomiya University

[††] Faculty of Engineering, Utsunomiya University

Kato lab., Yoto 7-1-2, Utsunomiya-shi, Tochigi 321-8585, Japan

Tel&Fax: +81-28-689-6256

E-Mail: onuki@mclaren.is.utsunomiya-u.ac.jp

Abstract: In this paper, we propose a watermarking method for still images using Discrete Cosine Transform (DCT). Watermarking is a copyright protection technique for digital contents by hiding secret information into the contents. The proposed method embeds the watermark information into DCT coefficients. To obtain a watermarked image that is not only high quality but also has robustness for compression, we considered a method to change the degree of embedding by utilizing the activity of each DCT block. The simulation results show that the proposed scheme can obtain high quality watermarked images and we can extract most of the embedded data even if they are compressed by JPEG scheme.

1. Introduction

Recently, with the development of digital communication and media technique such as DVD, the distribution of multimedia contents is coming into prevalence. However, because these digitized multimedia data can be repetitively duplicated without any distortion or degradation, copyright issue for re-utilizing multimedia data and preventing illegal copy are getting widespread concern. One counterpart of illegal copy is to embed the author's digital signature or ID number into digital contents such as still images or video. Such methods are called the watermarking technique. When the contents are used unexpectedly or illegally without the permission from the author, it is possible to protect the copyright by extracting the embedded authentication [1].

In the literature, several watermarking techniques have been developed. One of the watermarking methods is spatial domain watermarking, but it is that a common picture editing and lossy compression operation may eliminate the watermark. Other than spatial domain watermarking, frequency domain approaches, for example, have also been proposed [2][3]. JPEG makes use of DCT to lossy compression, so frequency watermarking, which embeds information to DCT coefficient, has robustness to JPEG compression.

Since the noise in a high frequency region is not so sensitive to human vision, the watermark should be embedded into the higher frequency coefficients. However, the watermark information in the higher frequency coefficients might be discarded after quantization operation of JPEG compression. Therefore, the information should be embedded in various frequency ranges considering the effect of quantization.

In this paper, a watermarking method for still images using DCT is proposed. The proposed method is to embed watermark information into DCT coefficients, with considerations to embedded image quality and robustness to attack. Especially, the proposed scheme is highly robust to JPEG compression. We show the simulation results of the proposed scheme in the last part of this paper.

2. Watermarking Method Using DCT

Various watermarking methods using orthogonal transform are proposed in bibliographies [2][3]. Our scheme also can be classified as a watermarking method using DCT, one of orthogonal transforms [4]. This method restrains image quality, but has robustness against JPEG compression. This method can extract embedded information without the original image. We explain the proposed method in the following section.

2. 1 Watermark embedding

We explain watermarking method that embeds authentication information, such as a signature or a logo mark into an image.

1. Original image ($X \times Y$ pixel, 8bit/pixel) is divided into blocks of size 8×8, which are denoted as $B_{m,n}$ (m=0, 1,..., M-1, n=0, 1,..., N-1). Here, $M=X/8$, $N=Y/8$.
2. 8×8 DCT is applied to each block $B_{m,n}$.
3. Watermark information $W(m,n)$ is embedded by modifying the DCT coefficient $C_{m,n}(i,j)$ as shown in equation (1) and equation (2).

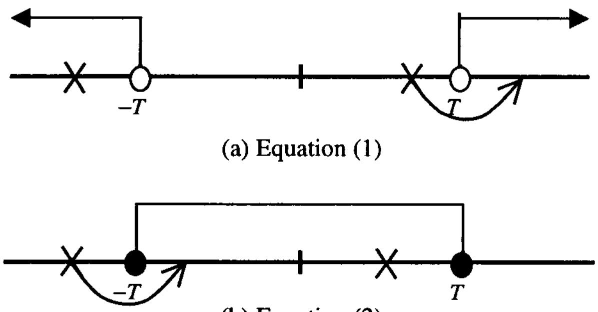
$W(m,n)=0$ and $|C_{m,n}(i,j)|<T$ then

$$C'_{m,n}(i,j)=C_{m,n}(i,j)+sign(C_{m,n}(i,j))T \quad (1)$$

$W(m,n)=1$ and $|C_{m,n}(i,j)|\geq T$ then

$$C'_{m,n}(i,j)=\mathrm{mod}(C_{m,n}(i,j),T) \quad (2)$$

where T is the threshold value, which represents embedding strength. Figure 1 shows the idea of these equations.



(b) Equation (2)

Figure 1. Watermark embedding

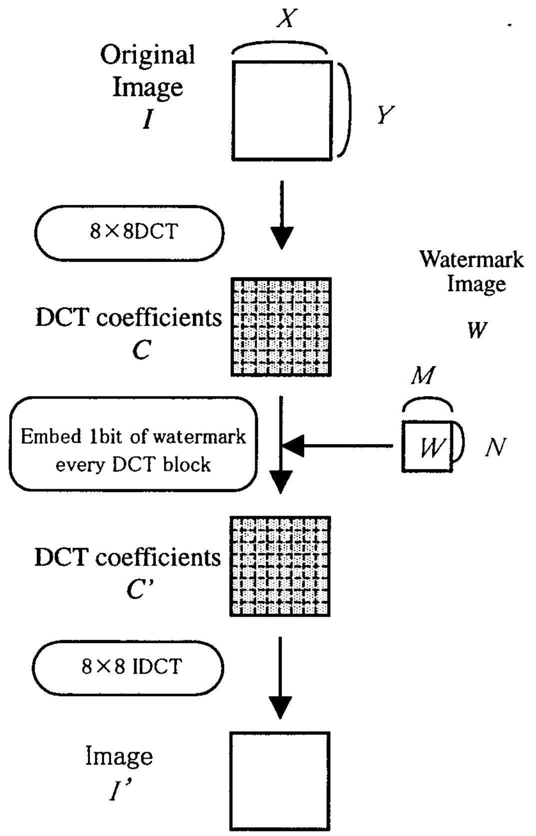


Figure 2. The outline of proposed scheme

4. After above procedures, perform inverse DCT on all blocks to obtain a watermarked image I'.

Figure 2 shows the outline of these steps.

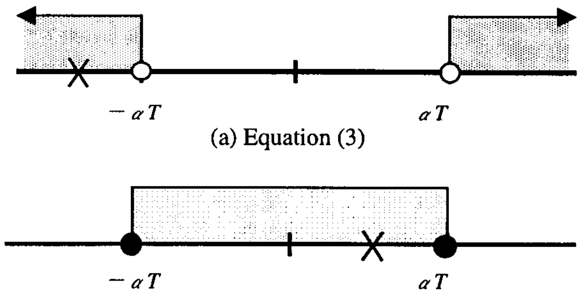
2.2 Watermark extraction

When we extract watermark, we perform inverse procedure of watermark embedding. In other words, watermarked image I' is divided into blocks, and DCT is performed on each block. Then the DCT coefficients $C_{m,n}(i,j)$ at the embedding positions are confined, and watermark information is obtained by equation (3) and equation (4).

$$|C'_{m,n}(i,j)|>\alpha T \text{ then } W(m,n)=0 \quad (3)$$

$$|C'_{m,n}(i,j)|\leq\alpha T \text{ then } W(m,n)=1 \quad (4)$$

where α is a parameter which defines the degree of freedom in the judgment. Figure 3 shows the idea of these equations.



(b) Equation (4)

Figure 3. Watermark extracting

3. The Embedding Method Considering Image Quality and Robustness

3. 1 Decision of the embedding position

In order to decide the position of DCT coefficient for watermark embedding, we define evaluation value ρ considering quality of image and robustness against attack as

$$\rho=\beta\cdot SNR+\gamma\cdot DRR \quad (5)$$

$$(\beta+\gamma=1.0,\ \beta>0,\ \gamma>0)$$

where *SNR* is signal to noise ratio, and *DRR* is data remaining ratio that is the ratio of correct extracted watermark information. *DRR* is defined as

$$DRR=\frac{h_0}{n_0}\times\frac{h_1}{n_1}\times 100 \quad (6)$$

where n_0 and n_1 is the number of bit 0 and 1 of embedded information, and h_0 and h_1 is the number of bit 0 and 1 of correctly extracted information in attacked image respectively.

We embed the watermark into the DCT coefficient which maximize the evaluation value ρ.

3. 2 Decision of the threshold value T

Generally, human vision is not so sensitive to the noise in a high frequency region. Therefore, in a low frequency region in image, we set the threshold value T low, and in a high frequency region, we set the threshold value high. This technique improves image quality than using a fixed threshold.

In the proposed method, we change adaptively the threshold value T according to activity value [5]. Activity value $P_{m,n}$ is mean power in AC components of DCT coefficients every block. The threshold value T is decided by considering the activity value $P_{m,n}$ in the following way:

$P_{\min} < P_{m,n} < P_{mean}$ then

$$T = \frac{(T_{\max} - T_{\min})(P_{mean} - P_{\min})}{(P_{m,n} - P_{\min})} + T_{\min} \qquad (7)$$

$P_{mean} < P_{m,n} < P_{\max}$ then

$$T = T_{\max} \qquad (8)$$

where P_{min} is minimum, and P_{max} is maximum $P_{m,n}$ of all block. P_{mean} is mean activity value of all blocks. T_{min} and T_{max} are obtained by

$$T_{max} = Q \qquad (9)$$

$$T_{min} = Q/2 \qquad (10)$$

Q is component of JPEG recommended quantization table **Q**, shown Table 1, namely, watermarking position (i, j) match quantization step size.

Table 1. JPEG recommended quantization table **Q**

j, i	0	1	2	3	4	5	6	7
0	16	11	10	16	24	40	51	61
1	12	12	14	19	26	58	60	55
2	14	13	16	24	40	57	69	56
3	14	17	22	29	51	87	80	62
4	18	22	37	56	68	109	103	77
5	24	35	55	64	81	104	113	92
6	49	64	78	87	103	121	120	101
7	72	92	95	98	112	100	103	99

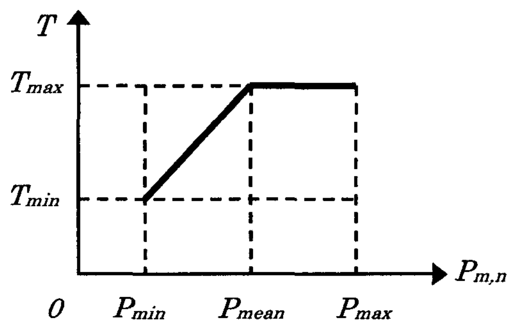


Figure 4. Relationship between $P_{m,n}$ and T

If $P_{m,n}$ of watermarking block is larger than P_{mean}, threshold value T is set T_{max}. On the other hand, if $P_{m,n}$ of watermarking block is smaller than P_{mean}, threshold value T is adaptively changed according to the value $P_{m,n}$, the region from P_{mean} to P_{min}. The relationship between $P_{m,n}$ and T is shown in Figure 4.

3. 3 Encryption on watermark information

Before embedding process in our scheme, we encrypt the watermarking information, i.e, authentication image, using a secret key. At first, we perform the exclusive-OR operation between authentication image and a pseudo-random sequence, which is generated from the secret key. Then, we change the position of the resulted sequence using hash function, so that watermarking information was difficult to be extracted without the secret key. However, if the secret key is known, all the above processings are reversible so that the watermarking information can be perfectly reconstructed.

4. Simulation Results

The luminance component of the image AUTO (512×512 pixel, 8bit/pel) from SIDBA (Standard Image Data BAse) is used for simulation. We embedded an authentication image (64×64 pixel, 1bit/pel) shown in Figure 5. Before embedding process, we encrypt the authentication image using a secret key to prevent extraction by illegal users. Then, we embed the watermark in position (i, j)={(1,3), (2,2), (3,1)}, which are decided by using estimation equation (5) in case of the number of watermarking position equals 3. Table 2 shows the ranking embedded position by evaluation value ρ.

Table 2. Ranking embedded position (Image AUTO)

	Watermarking Position (i, j)	*SNR* [dB]	*DRR* [%]	ρ
1	{(1,3),(2,2),(3,1)}	40.451	90.401	76.237
2	{(2,2),(3,1),(4,1)}	39.847	93.819	76.015
3	{(2,2),(3,1),(3,2)}	40.167	92.644	75.730
4	{(1,3),(2,2),(4,1)}	39.749	92.651	75.513
5	{(2,2),(3,1),(3,3)}	39.499	93.964	75.449

Figure 5. Authentication image (64×64 pixel, 1bit/pel)

Figure 6 shows the watermarked image. The *SNR* of watermarked image is 40.45[dB]. We can see that the quality of watermarked image is fairly high when the *SNR* is above 40[dB].

Next, we compress the watermarked image using JPEG scheme, then extract watermark and measure DRR. Here, we use JPEG baseline option of StirMark [6](ver3.1.79) as compression scheme. StirMark is an attacking tool for watermarked images.

Figure 6. Watermarked image (SNR=40.45[dB])

Table 3 shows the details of simulation results of StirMark's compression parameter q vs. compression ratio, *SNR*, *DRR*, and α. This defines Figure 7 shows the simulation results of q vs. DRR. The x-axis and y-axis show the compression parameter q and the *DRR*, respectively.

Table 3. The details of simulation results

Parameter q	Compression ratio	*SNR* [dB]	*DRR* [%]	α
(No compression)	1.000	40.45	99.66	1.0
90	0.239	37.95	99.51	1.0
80	0.159	36.60	93.29	0.8
70	0.127	35.80	88.96	0.9
60	0.106	35.06	88.05	0.8
50	0.094	34.34	91.66	1.0
40	0.080	33.64	85.11	1.2
30	0.064	32.89	56.51	1.0
20	0.046	32.02	34.29	1.0
10	0.029	29.96	24.54	1.0

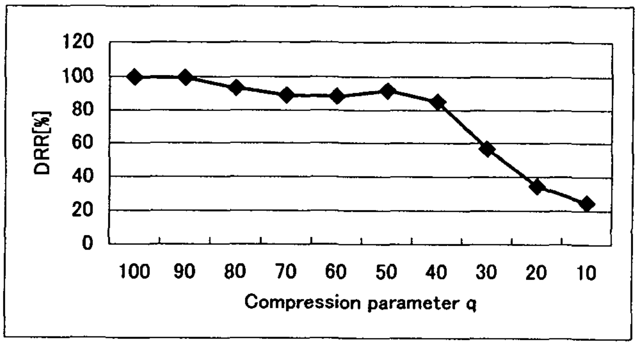


Figure 7. DRR against JPEG compression

(a) q=40 (b) q=30

Figure 8. Extracted authentication images

Figure 7 shows that the *DRR* of watermark is above 80[%] when the compression parameter q is above 40. Extracting image when parameter q is 40, Figure 8 (a), can recognize easily authentication information. However, when the parameter is below 30, the *DRR* tends to decrease. Extracting image when parameter q is 30, Figure 8 (b), doesn't show clearly authentication information because of remarkably noise. The reason is that, when the compression ratio in JPEG is increased, the information in an embedded image is reduced by quantization.

5. Conclusion

In this paper, a watermarking method for still images using DCT is proposed. The proposed method embeds watermark information into DCT coefficients, with considerations to embedded image quality and robustness to attack.

Simulation results show that our scheme can achieve high quality of watermarked image, and high resistance against JPEG compression.

In our future works, we will study a watermarking method that has robustness against the other kinds of attacks such as clipping and scaling.

Reference

[1] Kineo Matsui, "The foundation of watermarking," The Morikita Publishing Co. 1988.

[2] Yoonki Choi, Kiyoharu Aizawa, "Digital watermarking using inter-block correlation," ICIP'99, No.2, pp.216-220, Oct. 1999.

[3] C.T. Hsu, J.L. Wu, "Hidden digital watermarks in images," IEEE Trans. on Image Processing, Vol.8, No.1, pp.55-68, Jan. 1998.

[4] Takeharu Adachi, Madoka Hasegawa, Shigeo Kato, "A study on a watermarking method for still images using DCT," Tech. Rep. HCS99-43, Vol.99, No.384, pp.17-22, Oct. 1999.

[5] Supervised Hiroshi Harashima, "Compression image information," The Ohm Co. pp.99-110, 1991.

[6] Fabien A. P. Petitcolas, Ross J. Anderson, Markus G Kuhn, "Attacks on copyright marking systems," 2nd Workshop on Information Hiding, Vol.1525 of Lecture Notes in Computer Science, pp.218-238, Apr. 1998.