# A watermarking technique based on JPEG quantization table

Shwu-Huey Yen, Yi-Wei Chen, Hwei-Jen Lin, Chia-Jen Wang
*Pria Lab., Department of Computer Science and Information Engineering*
*Tamkang University, Taipei, Taiwan, R.O.C*
*e-mail:* shyen@cs.tku.edu.tw, 693190869@s93.tku.edu.tw, wachje@pria.cs.tku.edu.tw

## ABSTRACT

*JPEG compression is a common processing when sending an image via the Internet, thus how to protect the ownership of an image after JPEG compression is a very important issue. In this paper, we propose a watermarking scheme which has a good capacity and imperceptibility and especially robust to the JPEG compression. First the host image is divided into 8 x 8 blocks and candidate blocks are determined based on the number of edge point of ± 45° lines. By observing the standard JPEG quantization table, pairs of positions with same quantization scale are chosen for candidate blocks of the host image for embedding the watermark information. The proposed method is also extended to the video watermarking. The experimental results show our method is robust against many kinds of general attacks, especially JPEG and MPEG compression, and the performance of imperceptibility is equally well.*

## 1: INTRODUCTIONS

Because the maturity and popularization of the computer science technology, many creations, for instance, films, music, images, articles, etc, are produced or stored in digital form. But digital data can be easily duplicated, even falsified by utilizing some application software and circulated via the Internet. Such action constitutes aggressions upon the intellectual property right. In order to solve this problem, a lot of systems are proposed. Among various kinds of relevant research, many efforts are invested in digital watermarking techniques.

A watermark can be a trade mark, a symbol, or a signature, which can identify the ownership of a digital creation. The watermark will be embedded into the host media [12], and extracted with a certain algorithm to confirm the copyright. In this paper, we focus on watermarking techniques in digital images.

There are two main fields for embedding watermarks. First one is to embed watermarks directly into host image pixels by replacing the least-significant-bit (LSB) with the watermark information [7]. In the second method, the host image is transformed into the frequency domain to embed the watermark information. After the embedding process, the host image is invert transformed back to spatial domain. The watermarking techniques on frequency domain are usually more robust to against malicious attacks. On the other hand, they might have less embedding capacity than those on spatial domain. Some researches use both fields to embed the watermark [4]. Besides, predictive coding is employed in some articles about data hiding in images [5][6]. As the proposed scheme is to embed watermarks on the frequency domain, we will give a brief introduction on the following two methods [1][2] and compare our method with them in Section 3.

Wang et al. [2] proposed a blind image watermarking scheme based on relative modulation of the DCT coefficients. Their method needs neither the original image nor the watermark, but the embedding capacity is sacrificed. Ni et al. [1] evaluated fractal dimension of the image to locate textured area as the feature blocks. The watermark is embedded in the feature blocks. A few mechanisms are adopted to increase the security of their scheme. Some extra information, a key, the original watermark and a reference watermark, are needed for extraction in this method.

There are many kinds of transformations used for transforming the host image into the frequency domain, for instance, the Discrete Fourier Transform (DFT), the Discrete Cosine Transform (DCT) [1-3], the Discrete Wavelet Transform (DWT) [8-11], and so on. Among them, the DCT transformation is also used in JPEG compression. JPEG compression can be regarded as a most common attack in the watermarking technique. To against the JPEG compression and some other common attacks, a watermarking scheme based on DCT quantization table is proposed in this paper. The Human Visual System is adopted in our scheme to increase the imperceptibility of the watermarked image.

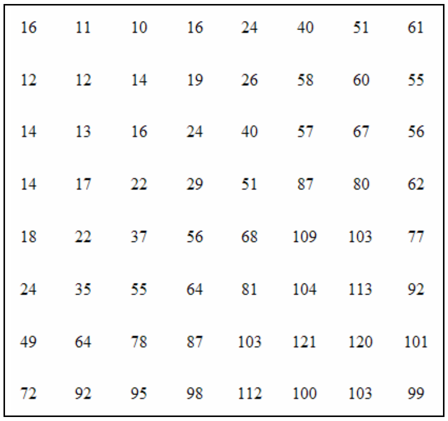
The remaining sections are organized as follows. In Section 2, we present our watermarking scheme including the embedding and extracting processes in detail. In Section 3, the experimental results are presented to show the performance of our scheme. Then conclusion and future works close this paper in Section 4.

# 2: THE PROPOSED SCHEME

With the characteristics of the JPEG standard quantization table, we proposed a scheme to embed the watermark into the DCT coefficients of the host image. When an image suffers JPEG compression, it is transformed into frequency domain by the DCT transformation. And for compressing, these DCT coefficients are quantized by the quantization table. Using the correlation between the coefficients which are quantized by the same scale elements, our scheme is robust under JPEG compression attack.

## 2.1: EMBEDDING PROCESS

The standard JPEG 8 × 8 quantization table is shown in Fig. 1.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 11 | 10 | 16 | 24 | 40 | 51 | 61 |
| 12 | 12 | 14 | 19 | 26 | 58 | 60 | 55 |
| 14 | 13 | 16 | 24 | 40 | 57 | 67 | 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 |

**Fig. 1.** JPEG standard quantization table

Observing the table, we find that there are pairs of quantization scales which have the same value. For example, in the position (1,0) and (1,1) are both "12", in the position (5,0) and (2,3) are both "24", and in (4,1) and (3,2) are both "22". When the JPEG compression ratio is 50, the DCT coefficients are quantized by the standard table as shown in Fig. 1. The DCT coefficients corresponding to those pairs will be divided by the same magnitude. Other compression ratios use different quantization tables. But those quantization tables are all derived from the standard quantization table. For the JPEG compression ratio is between 0 and 100, the formula used to derive the other tables is as following.

```
quality = the JPEG compression ratio;            (1)

if (quality < 50)
        quality = 5000 / quality;                (2)
else
        quality = 200 - quality*2;               (3)

q_table[i] = stdard_table[i] * quality / 100;    (4)
```

where the q_table[i] and the stdard_table[i] are the elements on the $i^{th}$ position of the derived quantization table and the standard quantization table respectively. When the JPEG compression ratio is less or equal to 0, the quality in Eq. (1) will be set to 1. When the JPEG compression ratio is more than 100, the quality in Eq. (1) will be set to 100. Form the formula above, some conclusions can be drawn:

- If a pair of positions with the same value in the JPEG standard quantization table, then they will have the same value in the quantization table for other compression ratios too.
- From Eq. (2) & (4), if the compression ratio is less than 50, the scale elements in the derived quantization table will be larger than the original ones in the standard quantization table when comparing elements of the same position.
- From Eq. (3) & (4), if the compression ratio is larger than 50, the derived scale elements in quantization table will be smaller than the original ones in the standard quantization table when comparing elements of the same position.
- If the compression ratio is low, then the image after decompressed will lose more details. In general, an image, to have acceptable image quality after decompressed, hardly has compression ratio smaller than 50.

Based on these observations, the proposed scheme hides one watermark bit in each pair of the positions with the same scale element. In an 8 x 8 block, let two DCT coefficients $S_1$ and $S_2$ be located at the positions which have the same quantization scale Q in the standard quantization table. If the embedded bit is "1", alter the values of $S_1$ and $S_2$, when needed, to make sure that Eq. (5) is satisfied. Similarly, if the embedded bit is "0", alter the values of $S_1$ and $S_2$, when needed, to make sure that Eq. (6) is satisfied.

$$|S_1'| \geq |S_2'| + \Delta. \tag{5}$$

$$|S_1'| < | S_2'| - \Delta. \tag{6}$$

where $S_1'$ and $S_2'$ are the altered $S_1$ and $S_2$ respectively, and Δ is a reference threshold, in here Q*60% is defined as Δ.

When the watermarked image is processed by JPEG compression, $S_1'$ and $S_2'$ will be both quantized by Q' and become $S_1''$ and $S_2''$. Q' is the quantization scale of the desired JPEG compression ration. Without loss of generality, assume the compression ratio is larger than 50, i.e., Q' is smaller than Q. Then the following relations (7), (8) hold for they are both quantized by a magnitude smaller than Q.

$$|S_1'| \geq |S_2'| + \Delta \quad \text{implies} \quad |S_1''| \geq |S_2''| \qquad (7)$$

$$|S_1'| < |S_2'| - \Delta \quad \text{implies} \quad |S_1''| \leq |S_2''| \qquad (8)$$

Considering the robustness and transparency, we embed two bits into an 8 x 8 block. In here, medium frequency positions [(5,0) , (2,3)] and [ (4,1) , (3,2)] are chosen such that each pair corresponds to the same quantization scale in Fig. (1). Moreover, to increase the imperceptibility further, the theory of Human Visual System (HVS) is adopted. Human eye is sensitive to the noise in smooth area, horizontal, and vertical lines, but less sensitive to the noise in textured area or lines of ± 45°. So we perform the edge detection of ± 45° lines on the host image, and count the edge points in each 8 × 8 block. Assume the watermark size is M x N, then $\lceil MN/2 \rceil$ candidate blocks with more edge points are chosen for embedding. Since DCT transform is applied on luminance components, if the host image is a color image, transform the RGB model to the YUV model first. Then the embedding processing is executed in the luminance component Y. Following is the detail procedure of our scheme:

- Perform the edge detection of ± 45° lines to the host image.
- Count the number of edge points for each 8 × 8 block, and N/2 blocks with more edge points are marked as candidate blocks for embedding, if the watermark size is N.
- Transform the host image to frequency domain by DCT transformation.
- In the candidate blocks, manipulate the coefficients in position [(5,0),(2,3)] and [(4,1) , (3,2)] if needed, to embed two bits into a candidate block. Let $S_1$ and $S_2$ represent the DCT coefficients in position (5,0) and (2,3) (or (4,1) and (3,2)) respectively:

  **If the embedded bit is "1":**
  If $|S_1| \geq |S_2| + \Delta$, then no modification is required. Else, adjust both $S_1$ and $S_2$ by the amount of $\Delta/2$ to make sure Eq. (5) is satisfied.

  **If the embedded bit is "0":**
  If $|S_1| < |S_2| - \Delta$, then no modification is required. Else, adjust those two values to make sure Eq. (6) is satisfied.

- Perform inverse DCT (IDCT) to obtain the watermarked image.

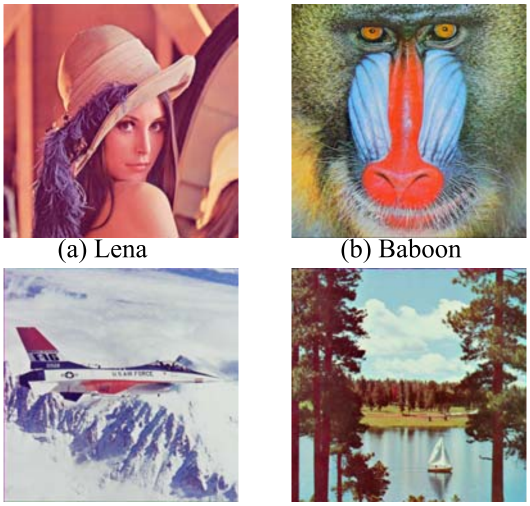
## 2.2: EXTRACTING PROCESS

To extract the watermark, we need to know which blocks are candidate blocks. But the original image and the watermark are not required. Following is the detail for extracting the watermark:

- Perform DCT transformation to the watermark image.
- In candidate blocks, check the coefficients in position pairs [(5,0), (2,3)] and [(4,1) , (3,2)]. If the coefficient in position (5,0) (or (4, 1)) is larger than or equal to the one in (2,3) (or (3, 2)), then bit "1" is extracted. If the coefficient in position (5,0) (or (4, 1)) is smaller than the one in (2,3) (or (3, 2)), then bit "0" is extracted.

## 3: EXPERIMENTAL RESULTS

Four color images of size 512 x 512 are used as host images and the watermark is a binary image of size 64 x 64, as shown in Fig. 2 and Fig. 3, respectively. In order to evaluate the performance of our scheme and compare with relative works, the peak signal-to-noise ratio (PSNR) value for imperceptibility, error rate and normalized correlation (NC) value, as in Eq. (9)- (11), for robustness against attacks are used. W( i , j ) and W'( i , j ) are the original watermark and the extracted watermark, and M × N and H ×W are the sizes of the watermark and the host image. For calculation in Eq. (11), bits in W and W' are considered as 1 or -1.



(a) Lena (b) Baboon

(c) Airplane (d) Sail boat

**Fig. 2.** 512 × 512 host images

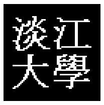


**Fig. 3.** 64 × 64 binary watermark

$$PSNR = 10\,log_{10}\frac{255^2}{MSE} \qquad (9)$$

where

$$MSE = \frac{\sum_{i=0}^{H-1}\sum_{j=0}^{W-1}\left((R_{ij}-\overline{R}_{ij})^2+(G_{ij}-\overline{G}_{ij})^2+(B_{ij}-\overline{B}_{ij})^2\right)}{3\times H\times W}$$

$$ErrorRate = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}W(i,j)\oplus W'(i,j)}{N\times M} \qquad (10)$$

$$NC = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}W(i,j)W'(i,j)}{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[W(i,j)]^2} \qquad (11)$$

In contrast with Wang et al.'s method [2], the watermark size is 4096 bits in our scheme which is much more than their maximal capacity (2205) when a 512 × 512 host image is used. If it is necessary, we can use more blocks in host image and more pairs in each block for embedding to increase the capacity. The PSNR values of our method and methods with Wang et al.'s [2] and Ni et al.'s [1] are compared, as shown in Table 1. The values for [1] and [2] are quoted from their papers, based on the same host images, and the lengths of the watermarks are 4096 in [1] and not more than 2205 in [2]. Our scheme obviously has the superiority on imperceptibility.

**Table 1.** Imperceptibility using PSNR (db)

| ColorImage | Our method | Method [2] | Method [1] |
|---|---|---|---|
| Lena | 47.09 | 43.37 | N/A |
| Baboon | 42.78 | 39.01 | N/A |
| Airplane | 47.23 | N/A | 44.90 |
| Sailboat | 46.88 | N/A | N/A |

To further compare the robustness against JPEG compression with Ni et al.'s method, a 512 × 512 8-bit grayscale "Lena" and the same length of the watermark 64×64 as in [1] are used. The PSNR of the watermarked image is 44.72 dB in Ni et al.'s method and 42.18 dB in ours. Although our PSNR is a little lower than Ni et al.'s, but from the comparison shown in Table 2, it is obviously that our method in the robustness against JPEG compression is much better than theirs. As recorded in Table 2, the proposed scheme can extract the watermark perfectly up to JPEG compression ratio of 50. Finally, some general attacks are also tested on our scheme. From Table 3, we observe that the extracted watermarks show the robustness of the proposed scheme against some general attacks. The color image "Baboon" has an error rate of 6.4% when it suffers the blurring attack which is due to high textured natural of the image.

The proposed scheme is also extended to video watermarking. Because MPEG video compression uses a similar compression method to JPEG when compress a frame format called "Intraframe" (or I frame). To carry out the experiment, a video with 60 frames is used as the host media with 352 × 240 for each frame and a 32 × 32 binary image is used as the watermark. 15 frames are randomly chosen for embedding the watermark. Instead of choosing the candidate blocks by calculating the edge points in each block as described in Section 2, candidate blocks are chosen randomly by a pseudo-random number generator. This is due to the fact that frames changes very quickly in a video, it is difficult for human eyes to notice the differences between frames. In this way, instead of recording candidate blocks for each frame which is a burden for the system, only a seed for the pseudo-random number generator is needed for extraction. After the watermark is embedded, the video is processed by MPEG compression and decompressed. Then watermark extraction is performed in these 15 embedded frames. The normalized correlation between extracted watermark and original watermark is shown in Table 4. The experimental result shows the watermark can be almost perfectly extracted which means our scheme is feasible in video watermarking.

**Table 2.** Results against JPEG compression (for gray scale "Lena")

| Quality Ratio | NC ([1]) | NC (ours) |
|---|---|---|
| 90 | 0.9605 | 1 |
| 80 | 0.9547 | 1 |
| 70 | 0.8891 | 0.9936 |
| 60 | 0.7550 | 0.9721 |
| 50 | 0.6433 | 0.9643 |
| 40 | 0.5314 | 0.6884 |

**Table 3.** Robustness result against general attacks (error rate %)

| Attack | Lena | Baboon | Airplane | Sailboat |
|---|---|---|---|---|
| Sharpen | 0 | 2.76 | 0 | 0.02 |
| Blur | 0.73 | 6.4 | 0.54 | 1.27 |
| Gaussian noise (2%) | 0.05 | 0.12 | 0.15 | 0.15 |
| Uniform noise (4%) | 1.07 | 0.63 | 0.68 | 0.71 |

**Table 4.** Robustness against MPEG attacks

| Frame number | #1 | #6 | #11 | #13 | #14 |
|---|---|---|---|---|---|
| NC value | 1 | 1 | 0.995 | 0.995 | 0.995 |
| Frame number | #25 | #30 | #32 | #33 | #37 |
| NC value | 0.990 | 0.995 | 0.990 | 0.995 | 0.995 |
| Frame number | #41 | #49 | #53 | #58 | #59 |
| NC value | 1 | 1 | 1 | 1 | 1 |

## 4: CONCLUSION AND FUTURE WORK

In this paper, a watermarking method based on JPEG quantization table is proposed. Choosing pairs of embedding positions corresponding to the same quantization scale in the JPEG standard quantization table, our watermarking scheme can resist many kinds of attacks, especially the JPEG compression. To improve the imperceptibility, the watermark information is embedded into the middle frequency coefficients of the candidate blocks. Candidate blocks are determined by the number of edge points which has slope of ± 45° since human eye is not sensitive to the ± 45° lines and textured areas pointed out by the Human Visual System (HSV). The experiment results show our scheme is robust to the JEPG compression and some general attacks. In addition, the imperceptibility of the watermarked image by our scheme is highly achieved. In the proposed method, the original image is not required in extraction procedure. Only the positions of the candidate blocks are needed. When the host image size is 512 × 512, there are 4096 8 × 8 blocks. Use an 1 or 0 to indicate a block is or not is a candidate block. So 4096 bits are required to indicate position of candidate blocks, i.e., it only requires an extra information of 512 bytes. In the future work, the Δ value in Eq. (3) and (4) will be further studied to achieve better tradeoff between imperceptibility and robustness. Besides, the maximal capacity with acceptable imperceptibility should be estimated for more applications.

The experiments also show our scheme is feasible in video watermarking to against MPEG compression. In here, a fixed watermark is embedded into selected frames. To avoid the collusion attack or watermark elimination by malicious attackers, some steps may be adopted. First, to embed a meaningful fixed watermark $W_1$, such as a logo, we can use a randomly generated watermark sequence $W_r$ such that $W_r \sim N[0, 1]$and XOR ($\oplus$) operation to produce another watermark $W_2 = W_1 \oplus W_r$ . Note that $W_2 \sim N[0, 1]$ and $W_2 \oplus W_r = W_1$. Thus with some keys and the original watermark $W_1$, we can generate different watermarks. By this way, we can avoid the estimation and elimination consequently from malicious attackers. Second, use different watermarks for different scenes of the video [12]. Since we can produce as many different watermarks as we wish, it is possible to give different watermarks for different scenes (or the same watermark in the frames of the same scene.) By this way, we can avoid watermark being washing out from averaging frames. More over, it is also robust to frame dropping or insertion. Related works is under progress now.

## REFERENCES

[1] R. Ni, Q. Ruan, H.D. Cheng, "Secure semi-blind watermarking based on iteration mapping and image features," *Pattern Recognition 38*, pp. 357-368, 2005.

[2] Y. Wang, A. Pearmain, "Blind image data hiding based on self reference," *Pattern Recognition Letters 25*, pp. 1681-1689, 2004.

[3] C.C. Chang, T.S. Chen, L.Z. Chung, "A steganographic method based upon JPEG and quantization table modification," *Inform. Sci. 141 (1-2)*, pp. 123-138, 2002.

[4] F. Y. Shih, S. Y.T. Wu, "Combinational image watermarking in the spatial and frequency domains," *Pattern Recognition 36*, pp. 969-975, 2003.

[5] Y.-H. Yu, C.-C. Chang, Y.-C. Hu, "Hiding secret data in images via predictive coding," *Pattern Recognition 38*, pp. 691-705, 2005.

[6] S.S. Maniccam, N. Bourbakis, "Lossless compression and information hiding in images," *Pattern Recognition 37*, pp. 475-486, 2004.

[7] C.-K. Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition 37*, 469-474, 2004.

[8] M.-S. Hsieh, D.-C. Tseng, Y. Huang, "Hiding Digital Watermarks Using Multiresolution Wavelet Transform," *IEEE Transactions on Industrial Electronics*, vol. 48, pp. 875-882, Oct. 2001.

[9] M. Barni, F. Bartolini, A. Piva, "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking," *IEEE Transactions on Image Processing*, vol. 10, NO.5, May 2001.

[10] P. Bao, X. MA, "Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol.15, No.1, January 2005

[11] A. A. Reddy, B.N. Chatterji, "A new wavelet based logo-watermarking scheme," *Pattern Recognition Letters 26*, pp. 1019-1027, 2005.

[12] S. Biswas, S. R. Das, E. M. Petriu, "An Adaptive Compressed MEPEG-2 Video Watermarking Scheme," *IEEE Transactions on Instrumentation and Measurement*, vol.54, No.5, Oct 2005.