# A Robust Digital Watermarking with Mixed Transform Technique for Digital Image

Chien-Pen Chuang , Cheng-Hung Liu , Yi-Tsai Liao , Huan-Wei Chi

***Abstract*—In this paper, we developed a robust digital watermarking technique to protect intellectual property right of digital image. A scale-invariant feature transform technique was employed for resisting geometric attacks and two dimensional bar code was used for its high capacity and fault tolerance to enhance digital watermarking capacity. Besides, the discrete wavelet transform (DWT) and discrete cosine transform (DCT) were joined to cope with noise problem and enhance perceptual transparency of watermarking image. The algorithm performance was presented with a plurality of experimental results, including several attack models such as lossy compression, scaling, blurring and sharpening etc. The experimental results proved the robustness of this mixed transformation technique on protecting intellectual property right of digital image.**

***Keywords*—watermark, mixed transform technique, digital image**

## I. Introduction

LOSTS of intellectual property protecting methods have been developed for years. To encrypt data with key was one of best methods to protect data, but once the key was cracked, the data would be arbitrarily misappropriated; while for watermarking, the intellectual property rights are embedded on the data directly, and integrated with data itself, when the appropriator arbitrarily misappropriate the information, the watermark would be still existed on the data, with the extracted watermark, the intellectual property right would be shown, thereby the right protected. Generally speaking, a good watermarking technique includes: perceptual transparency, blindness, robustness, unambiguity, capacity and security [1][2].

In this study, our approach is a robust digital watermarking with mixed transform technique for digital Image. Using discrete wavelet transform to the $LL_1$ band in performing the discrete cosine transformation. As the discrete wavelet transform in the $LL_1$ band represents the whole image of the low-frequency energy. The slightest change will have a visual impact dramatically. As the result, we have chosen to embed the high-frequency block in this location. The experimental results show that the image can be obtained a well image quality and the robustness of the watermark.

In the paper, the embedded watermarking algorithm adopted can be divided into five stages:

stage 1: With scale-invariant feature transforms to extract feature information, so as to solve synchronization problem of watermarking.

stage 2: In discrete wavelet transform domain, with noise visibility function,to estimate watermarking embedded robustness.

stage 3: In discrete cosine transform domain, in accordance with JPEG quantization table, to select embedded position for the watermark.

stage 4: By Toral Automorphism to disturb watermarking sequence for embedding.

stage 5: According to estimated robustness of watermark, to embed the watermark onto frequency domain coefficient of original image.

Manuscript received December 30, 2011; revised January 17, 2012.

Chien-Pen Chuang is with the Dept. of Applied Electronics Technology, National Taiwan Normal University, Taiwan, R.O.C. (corresponding author to provide phone:+886-2-77343553; cellphone: 886-919-979-154; e-mail: chuang@ntnu.edu.tw).

Cheng-Hung Liu is with the Dept. of Applied Electronics Technology, National Taiwan Normal University, Taiwan, R.O.C. (e-mail: greenhat888@gmail.com).

Yi-Tsai Liao is with the Dept. of Industrial Education, National Taiwan Normal University, Taiwan, R.O.C. (e-mail: name9061@yahoo.com.tw).

## II. Procedure for Paper Submission

In the paper, Scale-Invariant Feature Transform (SIFT) [3][4] technique was employed to extract features, the feature information include coordinates(i, j), scale(δ), directions(ɵ) and eigenvectors($\bar{U}$) of the features and to transmit the feature information to image authentication center for verification.

### *A Estimating Watermarking Embedded Rrobustness*

--First, Conducting a first-order discrete wavelet transform for the original image, and isolating frequency band $LL_1$.

--Second, Assume the width of frequency band $LL_1$ as N×N with blocks of 8×8 pixels, wherein, the embedded robustness of watermark block of number $z$ sub-block presented as $\Psi(z)$ , then the equation for calculation is as following:

$$\Psi(z) = \frac{\sum_{z=1}^{\frac{N\times N}{64}} \sum_{i=1}^{8} \sum_{j=1}^{8} \psi(z, i, j)}{64} \quad (1)$$

Wherein, $\psi(z,\ \mathrm{i, j})$ representing for embedded robustness value of coordinates (i, j) in sub-block z number.

$$\psi(i, j) = (1 - NVF(i, j)) \cdot S_f + NVF(i, j) \cdot S_m \quad (2)$$

Wherein, NVF stands for Noise Visibility Function [5], NVF(i, j) shows local texture change of band $LL_1$ at

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

coefficient position (i, j), NVF ranges among [0, 1], when local texture is in extreme flat, NVF verges to 1, contrarily, verges to 0, $S_f$ represents weighted coefficient, $S_m$ represents flatness weighted coefficient.

$$NVF(i,j)=\frac{1}{1+\sigma_x^2(i,j)} \tag{3}$$

Wherein, $\sigma^2_x$ represents the acquired local variance of window with coordinates(i, j) as center, the calculation equation is as following:

$$\sigma_x^2(i,j)=\frac{1}{(2L+1)^2}\sum_{k=-L}^{L}\sum_{l=-L}^{L}(x(i+k,j+l)-\bar{x}(i,j))^2 \tag{4}$$

Wherein, $(2L+1)^2$ is window size of local variance; $\bar{x}(i, j)$ represents the added total average value of coordinates centers in the range of window size, the calculation equation is as following:

$$\bar{x}(i,j)=\frac{1}{(2L+1)^2}\sum_{k=-L}^{L}\sum_{l=-L}^{L}x(i+k,j+l) \tag{5}$$

### B Selecting Watermark Embedded Position

Firstly, conduct DCT (discrete cosine transform) for block of band $LL_1$ with 8x8 pixel size, wherein, embed 8 watermark pixels for each 8x8 set frequency domain block. Where, JPEG quantization table led in to determine watermark embedded position. As shown in Fig .1:

| Y \ X | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 16 | 11 | 10 | 16 | 24 | 40 | 51 | **61**(1) |
| 2 | 12 | 12 | 14 | 19 | 26 | 58 | **60**(1) | **55**(2) |
| 3 | 14 | 13 | 16 | 24 | 40 | **57**(3) | **69**(2) | 56 |
| 4 | 14 | 17 | 22 | 29 | **51**(3) | 87 | 80 | 62 |
| 5 | 18 | 22 | 37 | **56**(4) | **68**(5) | 109 | 103 | 77 |
| 6 | 24 | 35 | **55**(4) | **64**(6) | 81 | 104 | 113 | 92 |
| 7 | 49 | **64**(6) | **78**(7) | **87**(8) | 103 | 121 | 120 | 101 |
| 8 | **72**(6) | **92**(7) | **95**(8) | 98 | 112 | 100 | 103 | 99 |

Fig. 1. JPEG quantization table

Wherein, 8 pairs of coefficient coordinates with similar quantization quality are selected as watermark embedded position, and further store their coordinates positions into array ( $A_u$ , $B_u$ ) and ( $C_u$ , $D_u$ ), and the range of u is integer value of [1, 8].

### C Disturbing Watermarking

In order to improve the security of watermark, t times Toral Automorphism algorithm (developed by scholars of G. Voyatis and I. Pitas)[6] were implemented before embedding watermark. All coordinate were rearranged and sent k、t values to Image Authentication Center. The equation of Toral Automorphism algorithm is depicted as ：

$$\begin{pmatrix}x_{t+1}\\ y_{t+1}\end{pmatrix}=\begin{pmatrix}1 & 1\\ k & k+1\end{pmatrix}\begin{pmatrix}x_t\\ y_t\end{pmatrix}(\mathrm{mod}\ N) \tag{6}$$

Wherein, $(x_t , y_t)$ is coordinates of original image; $(x_{t+1} , y_{t+1})$ is coordinates of original image after first-order matrix operation, k is control variable and N is original image size.

### D Embedding Watermark

The embedded algorithm is as shown in the following:

If $V=$ black

$$(A_{z,u},B_{z,u})=Mean+\frac{\Psi(z)\times\alpha_u}{\beta}$$

$$(C_{z,u},D_{z,u})=Mean-\frac{\Psi(z)\times\alpha_u}{\beta}$$

Else $V=$ white

$$(A_{z,u},B_{z,u})=Mean-\frac{\Psi(z)\times\alpha_u}{\beta}$$

$$(C_{z,u},D_{z,u})=Mean+\frac{\Psi(z)\times\alpha_u}{\beta}$$

$$Mean=\frac{(A_{z,u},B_{z,u})+(C_{z,u},D_{z,u})}{2} \tag{7}$$

Wherein, $V$ represents pixel values of watermark. ( $A_{z,u}$ , $B_{z,u}$ )represents coefficient value of coordinates position ( $A_u$ , $B_u$ ) in sub-block number $z$ in discrete cosine frequency domain, β is adjustment factor for adaptability, so that adjustment could be made by the user according to requirements, if β coefficient were smaller, the robustness becomes better. $\alpha_u$ is a weighted factor, which is estimated by experiment. The flow chart of embedded algorithm is shown in the Fig.2.

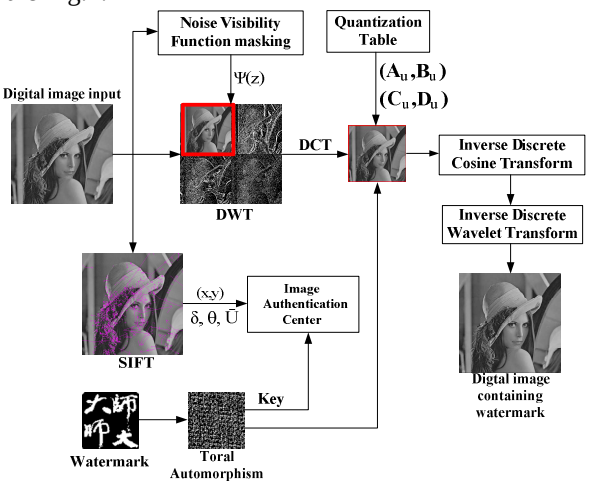


Fig. 2. Flow chart diagram of embedded algorithm

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

## III. WATERMARKING EXTRACTION SCHEME

The extracting stage uses the reverse technique as embedding stage. First, it can be obtained from the features information of both original image and watermark information at the image authentication center. Then, the scale and direction of watermark image will be modified with the data of feature to make watermark and watermark image synchronization. The extraction of watermark with DWT and DCT will be under the condition of :

### *A Extracting Watermark Information*

$$\begin{cases} If \quad (A_{Z,u}, B_{Z,u}) > (C_{Z,u}, D_{Z,u}) & ,V = black \\ Else & ,V = white \end{cases} \quad (8)$$

This means that if the coefficient value of $z$ sub-block coordinate ( $A_u$ , $B_u$ ) of DCT frequency domain is bigger than ( $C_u$ , $D_u$ ), then the pixel of watermark *V* will be black, otherwise, it will be white.

### *B Restore The Original Watermark by Toral Automorphism.*

From the image authentication center can be obtained watermark information by k、t information which can make Toral Automorphism (6).

### *C Enhance Watermark Recognition*

When pixel values of four directions (up, down, left, right) of coordinate (i,j) are the same, set same pixel values of this coordinate(i,j). From the experiment results, it is shown that with this algorithm, the watermark noise could be effectively decreased as show in the Fig.3.

(a) (b)

Fig. 3. (a) original compressed image (b) noise decreased image.

## IV. EXPERIMENTAL RESULTS

After watermark embedded onto original image, Peak Signal-to-Noise (PSNR) was employed for evaluation standard of image transparency. Bit Correct Ratio (BCR) was used for evaluation standard of robustness.

### *A Transparency Test of Watermark Algorithm*

In this section, the transparency test of watermark algorithm that we raised will be described, the embedded watermark size being 90x90 pixels, image format being 8 bit black and white bitmap, as shown in Fig.4. With watermark separately embedded on the test image, and the performance of transparency was deliberated. In the experiment, the test image used for transparency test was provided by USC-SIPI image database with six image samples [7], as shown in Fig.5.

(a) (b)

Fig. 4. (a) original watermark (b) disturbed watermark.

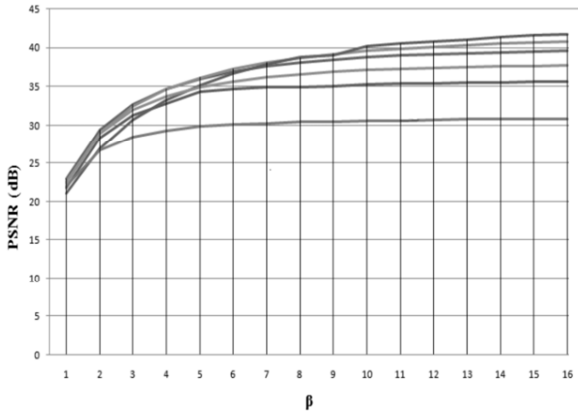


Fig. 5. Line chart comparison from 6 different images, x-coordinate being coefficient, y-coordinate being PSNR value

After coefficient reached 3, all PSNR value could reach 30dB, as shown in Fig. 5. It represents that the embedded algorithm we put forward has good performance.

### *B Watermark Algorithm Robustness Test*

In this section, two kinds of watermark robustness test will be described including watermark and QR watermark, as shown in Fig.6. Wherein, mean value 8 was taken for test. In the following, robustness test for extracted watermark after simulated watermark image attack will be described.

(a) (b)

Fig. 6. (a) watermark (b) QR watermark.

Owing to that discrete cosine transform was employed in the embedded algorithm, and embedded into discrete cosine coefficient according to watermark robustness, thus under various attack status, the watermark contents could still be correctly determined. The following is the Lena image at different attack types, made the experimental results.

TABLE I
BCR VALUE OF WATERMARK AND WHETHER QR WATERMARK COULD BE NORMALLY DECODED UNDER JPEG COMPRESSION ATTACK

| ***QF*** | ***50*** | ***60*** | ***70*** | ***80*** | ***90*** |
|---|---|---|---|---|---|
| ***BCR(%)*** | 96.96 | 98.16 | 99.01 | 99.36 | 99.37 |
| ***QR Decode*** | Y | Y | Y | Y | Y |

As shown in Table I, Quality Factor (QF) for compression test. When QF reached 50, it could distinguish a higher BCR(%) and QR watermark that could be decoded.

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Table II
BCR VALUE OF WATERMARK AND WHETHER QR WATERMARK COULD BE NORMALLY DECODED UNDER JPEG 2000 COMPRESSION ATTACK

| *QF* | *50* | *60* | *70* | *80* | *90* |
|---|---|---|---|---|---|
| *BCR(%)* | 95.26 | 98.16 | 98.79 | 99.25 | 99.25 |
| *QR Decode* | Y | Y | Y | Y | Y |

As shown in Table II, when QF reached 50, it could distinguish a higher BCR(%) and QR watermark that could be decoded.

Table III
BCR VALUE OF WATERMARK AND WHETHER QR WATERMARK COULD BE NORMALLY DECODED UNDER RESIZE ATTACK

| *Rate* | *0.5* | *0.7* | *0.9* | *1.1* | *1.3* |
|---|---|---|---|---|---|
| *BCR(%)* | 96.1 | 93.65 | 90.95 | 98.73 | 96.99 |
| *QR Decode* | Y | Y | Y | Y | Y |
| *Rate* | *1.5* | *1.7* | *1.9* | | |
| *BCR(%)* | 96.99 | 96.99 | 96.99 | | |
| *QR Decode* | Y | Y | Y | | |

As shown in Table III, is watermark image under resize attack. When Rate at 0.5, it could distinguish a higher BCR(%) and QR watermark that could be decoded.

Table IV
BCR VALUE OF WATERMARK AND WHETHER QR WATERMARK COULD BE NORMALLY DECODED UNDER BLURRING AND SHARPENING ATTACK

| *Type* | *Average filter (3x3)* | *Average filter (5x5)* | *Median filter (3x3)* | *Gaussian filter* | *Sharpening* |
|---|---|---|---|---|---|
| *BCR(%)* | 95.31 | 47.36 | 95.16 | 97.37 | 96.78 |
| *QR Decode* | Y | N | Y | Y | Y |

As shown in Table IV, for greater extent blurring attack, the extract results was not appropriate with this paper, owing to that in the beginning of the algorithm design, for enhancing both robustness and transparency, gives and takes needed to be considered. However, under smaller extent blurring attack, a satisfactory results could still be obtained.

## V. CONCLUSIONS

The algorithm in this paper, not only objective BCR value of watermark could be enhanced, but also subjective identification capability for watermark could be enhanced. The transparency of watermark was improved through embedding in the low frequency part of wavelet transformation. Besides, the key of watermark made by Toral Automorphism can reduce the demand of original image size in extraction. Therefore, it is robust to compete against compression, resize, blurring and sharpening attacks after experiments. The mixed technique of DWT and DCT with Toral Automorphism can enhance the robustness of watermarking for digital images.

## REFERENCES

[1] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, “Multimedia data-embedding and watermarking technologies,” Proceedings of the IEEE, vol. 86, no. 6, pp. 1064–1087, 1998.

[2] C. H. Lee and Y. K. Lee, “An adaptive digital image watermarking technique for copyright protection,” IEEE Transactions on Consumer Electronics, vol. 45, issue. 4, pp. 1005–1015, Nov. 1999.

[3] D. G. Lowe, “Distinctive Image Features from Scale-Invariant Keypoints”, International Journal of Computer, vol. 60, vo. 2, pp. 91–110, 2004.

[4] SIFT Library (2011). Available at http://blogs.oregonstate.edu /hess/code/sift/.

[5] S. Voloshynovskiy , A. Herrigel , N. Baumgaertner and T. Pun, “A Stochastic Approach to Content Adaptive Digital Image Watermarking,” Proceedings of the Third International Workshop on Information Hiding, pp.211-236, Sep. 1999.

[6] G. Voyatzis and I. Pitas, “Applications of Toral Automorphisms in Image Watermarking,” In Proceeding of the IEEE International Conference on Image Processing, vol. 3, pp. 219-222, 1996.

[7] University of Southern California (2011). Available at http://sipi.usc.edu/database/database.php.

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)