

# A Robust Watermarking and Image Authentication Scheme used for Digital Content Application

Chih-Ming Kung

Shin-Chien University, Kaohsiung, Taiwan, R.O.C.  
Email: alex@mail.kh.usc.edu.tw

Shu-Tsung Chao; Yen-Chen Tu

Chang-Jung Christian University, Tainan, Taiwan, R.O.C.  
Email: {stream, pinapple}@mail.cjcu.edu.tw

Yu-Hua Yan

Tainan Municipal Hospital, Tainan, Taiwan, R.O.C.  
Email: anne@cvig.org

Chih-Hsien Kung<sup>1</sup>

Chang-Jung Christian University, Tainan, Taiwan, R.O.C.  
Email: kung@mail.cjcu.edu.tw

**Abstract**—The development of computers and Internet has exploded in the last few years. The digital images are distributed and duplicated easily through WWW, thus the protection of the intellectual property rights of digital images becomes an important issue. In this paper, we proposed two techniques that are robust watermarking and image authentication scheme. The proposed scheme includes two parts. The first is a robust watermarking scheme performed in the frequency domain. It can be used to prove the ownership. The second is a signature process, which can be used to prove the integrity of the image. The input of the signature process is the edge properties extracted from the image. The signature can be correctly verified when the image is incidentally damaged such as lossy compression. Such a scheme can provide a high degree of robustness against JPEG compression attacks. Experimental results are also presented to demonstrate the validity and robustness of the new approach.

**Index Terms**—Watermark, Robust, Authentication

## I. INTRODUCTION

Since digital images and video are now widely distributed via the internet and various public channels, there is an urgent need for copyright protection against unauthorized data reproduction. The watermark is an owner-designed logo or trademark, which can be hidden in the owner's image products [1, 2].

Digital watermarking provides a complete solution

that embeds private information into digital signals and makes claiming legitimate usage, authentication of authorized users, and providing extra information for digital contents become possible.

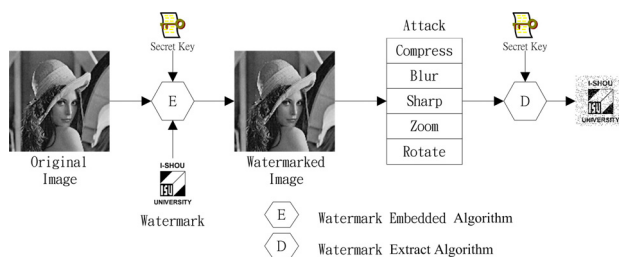


Figure 1. The Architecture of Imperceptible Digital Watermark System

Fig. 1 is the architecture of imperceptible digital watermark system. Among the proposed schemes, the imperceptible watermark technology can be broadly classified into two categories: (1) spatial domain based and [8, 9] (2) transform domain based [10, 11] approaches.

When the watermarked images are distributed via public channels such as the internet, it can discourage unauthorized copying. This is because the owner can prove his ownership by extracting the watermark using open methods and some security keys. Digital watermarking has recently been proposed as a means to provide copyright protection of multimedia data against unauthorized uses [3, 4]. In most cases the research was focused on un-oblivious watermarking [5, 6, 7].

<sup>1</sup> Corresponding Author

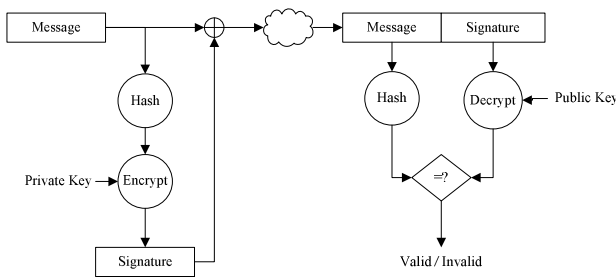


Figure 2. Signature and Authentication System

Hiding the logo in the spatial domain is the simplest watermarking technique [8,9,12]. However, the hidden information can be easily removed by the users or destroyed by JPEG compression. Some authors utilized the polarity information to modify the middle frequency coefficients to achieve a robust approach [7, 13, 14].

The conventional signature and authentication system is shown as Fig. 2.

The edge properties are essentially the content of the image. It can survive against lossy compression systems such as JPEG. Therefore, the signature can be correctly verified even when the image is incidentally damaged. The locations of the image which are maliciously altered can also be detected [12]. In the image, each block is classified to a certain class and given a context. The information serves as the input of the signature scheme. It's usually hashed with some author's data followed by an encryption using his secret key such that the receiver can verify the signature.

In this paper, a frequency domain scheme developed expressly for oblivious watermarking and signature process are presented. It uses the self-information of coefficients of the middle frequency in the host image, and explicitly takes in the cross-correlation between coefficients of the middle frequency and the watermark, and signature process that input is the edge properties extracted from the image. The signature can be correctly verified when the image is incidentally damaged such as lossy compression.

II. WATERMARK AND IMAGE AUTHENTICATION SYSTEM

The block diagram of the watermark and image authentication embedding and extracting system is shown in Fig. 3 and Fig. 4.

Fig. 3 shows the brief diagram of watermark and digital signature embedding system. First, given a message of arbitrary length and describe it, a fixed information is obtained by a hash operation. The signature is generated by using the private key to sign on the hashed digest. The original message associated with its signature is a watermarked image.

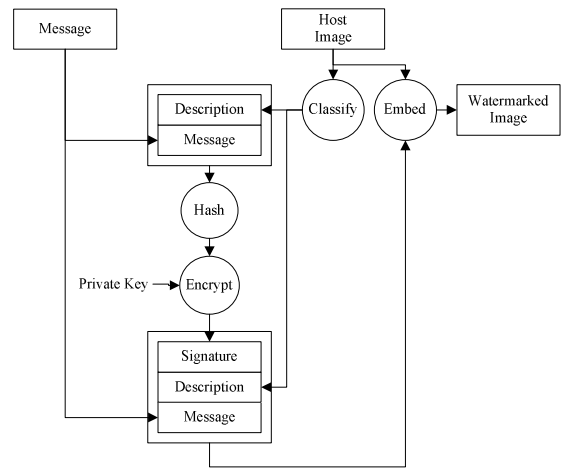


Figure 3. Watermark and Image Authentication Embedding System

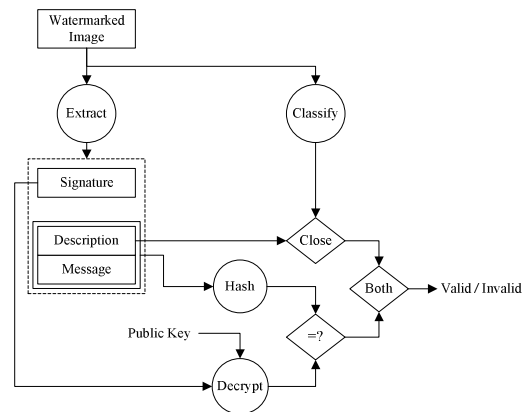


Figure 4. Watermark and Image Authentication Extracting System

Referring to Fig. 4, it shows watermark and image authentication extracting system. Where one is decrypted from the signature and the other is obtained by re-hashing the received message. And extracting the features includes histogram map, edge and more. Then the recipient can verify: (1) whether his received message was altered and (2) whether the message was really sent from the sender, by using the sender's public key to authenticate the validity of the attached signature [16, 17].

III. COPYRIGHT AND IMAGE AUTHENTICATION SCHEME

To provide a well-developed intellectual property rights protection scheme, a innovative approach which integrates robust watermarking and fragile watermarking schemes is proposed.

The robust watermarking technique used for image authentication detects, the integrity of image employ the fragile watermarking scheme based on digital signature technique. The image authentication (robust watermarking scheme) can be proved to use the retrieved watermark, and simultaneously the signature (fragile watermarking scheme) can check the integrity of image.

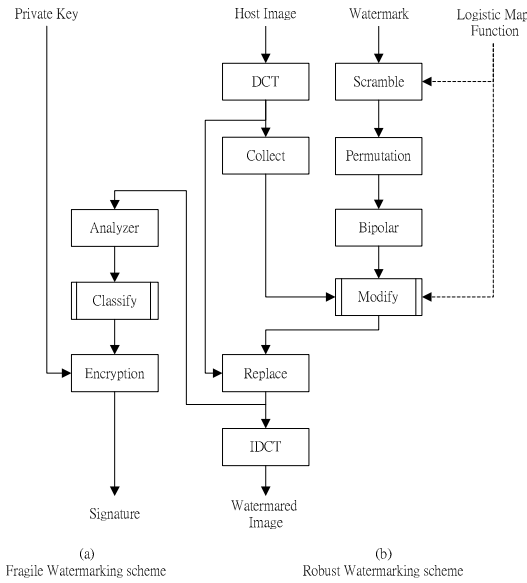


Figure 5. The Signature and Watermark Embedding Scheme

As illustrated in Fig. 5(a), the proposed image authentication scheme utilizes the characteristic of image features that it is robust under compression attack. The features of blocks, such as horizontal edge, vertical edge, and diagonal edge blocks of watermark embedded host images are retrieved by using classifier and to be used as the input information of digital signature.

IV. CLASSIFIER DESIGN

In this research, the two-dimension DCT coefficients,  $C_{01}$  and  $C_{10}$ , are adopted as classification criterion. According to the Edge Oriented Classification, the search region pixels are classified into four directions in the motion estimation algorithm and listed as the following, the Shade Block Horizontal Edge Block, Vertical Edge Block and Diagonal Edge Block. Then, the two-dimensions DCT coefficients,  $C_{01}$  and  $C_{10}$  are employed for classification process.

Fig. 6(a) and Fig. 6(b) illustrate the relationship between the edge orientations and the two DCT coefficients of  $C_{01}$  and  $C_{10}$ .

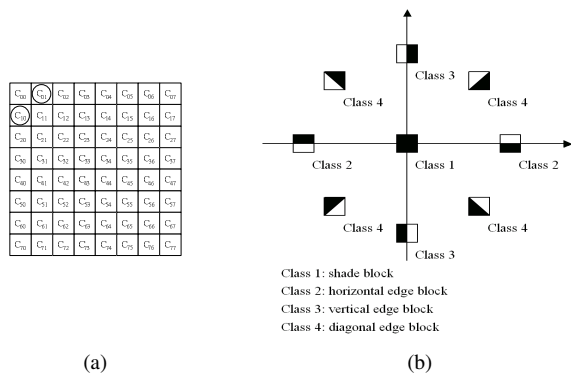


Figure 6. (a) DCT Coefficients, (b) DCT Coefficients Relations to Edge Orientations

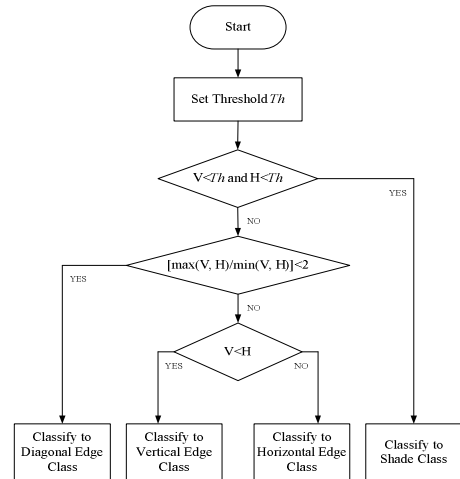


Figure 7. The Edge Oriented Classification Workflow

The next topic in this session is the “image authentication scheme on the edge information”. Fig. 7 illustrate the edge oriented classification method. Let  $H$  and  $V$  denote the first two AC coefficients ( $C_{01}, C_{10}$ ), that is, first horizontal and vertical coefficients of the DCT-transformed block, respectively. The classifier is designed according to the magnitudes of  $H$  (horizontal edge class) and  $V$  (vertical edge class) which is more significant. The block is classified to “diagonal edge class”, if both  $H$  and  $V$  are not significant.

V. WATERMARK IN THE FREQUENCY DOMAIN

The basic idea to hide information in the frequency domain is to alter the magnitude of some of the DCT coefficients. To achieve the robustness property, the hiding mechanism according to the quantization algorithm of JPEG which is the most commonly used lossy compression standard.

The DCT transforms image blocks from spatial domain to frequency domain. Let the block  $b(u,v)$  denote the transformed coefficients. The quantization is performed by:

$$b_q(u,v) = b(u,v) // Q(u,v), \quad 0 \leq u,v < 8 \quad (1)$$

where  $Q(u,v)$  is the quantization table of size  $8 \times 8$ . In the decoding process, the quantity  $b'(u,v)$  is retrieved from the de-quantization

$$b'(u,v) = b_q(u,v) \times Q(u,v), \quad 0 \leq u,v < 8 \quad (2)$$

The data loss of JPEG compression comes from the quantization and the de-quantization processes given above. There are two quantization tables for JPEG, one is the luminance table and the other is the chrominance table. It can be easily seen from that higher values of  $Q(u,v)$  will produce more loss of the original block at the position  $(u,v)$ . For the recommended quantization table, the values of  $Q(u,v)$  are smaller at the low frequency region and bigger at the high frequency region.

8	6	5	8	12	20	26	31
6	6	7	10	13	29	30	28
7	7	8	12	20	29	35	28
7	9	11	15	26	44	40	31
9	11	19	28	34	55	52	39
12	18	28	32	41	52	57	46
25	32	39	44	52	61	60	51
36	47	48	49	56	50	52	50

Figure 8. Mid-Frequency Region chosen from JPEG Quantization Table for Luminance.

Therefore, if the information is hidden in high frequency region which divide higher quantization values, it will be easily erased by JPEG attack. On the other hand, if it is hidden in the low frequency region, the host image will be damaged seriously. The information will be hidden in the middle frequency region which is selected according to the values of table  $Q(u,v)$  as shown in Fig. 8.

VI. LOGISTIC MAP FUNCTION

Before the binary watermark is embedded, it is first scrambled such that the total numbers of 0s and 1s are nearly the same. This scrambling is performed through a 1-dimensional map given in [19, 20], which is the logistic map from the unit interval [0,1] into [0,1] defined by

$$f_{\mu}(x) = \mu x (1 - x) \tag{3}$$

In (3), the parameter  $\mu$  can be chosen with  $0 \leq \mu \leq 4$ . This map constitutes a discrete-time dynamic system in the sense that the map generates a semi-group through the operation of composition of functions.

The state evolution is described by  $x_n = f_{\mu}(x_{n-1})$  and is denoted as

$$x_n = \mu x_{n-1} (1 - x_{n-1}) = f_{\mu}^{(n)}(x_0) \tag{4}$$

where  $f_{\mu}^{(n)} = \underbrace{f_{\mu} \circ f_{\mu} \circ f_{\mu} \dots \circ f_{\mu}}_n$  and  $\circ$  is

function composition. The preceding eight bits below the decimal point of the binary representation of  $x_n$ ,  $n=1,2,\dots$  are extracted to constitute the chaotic binary sequence  $c$ .

Let  $x_n = (0.x_n(1)x_n(2)\dots x_n(8)x_n(9)\dots)_2$ . The relations of the binary sequence  $c(j)$ ,  $j=1,2,\dots$  and  $x_n$  can be represented by

$$\begin{aligned} x_n &= (0.x_n(1)x_n(2)\dots x_n(8)x_n(9)\dots)_2 \\ &= (0.c(8n-8)c(8n-7)\dots c(8n-1)x_n(9)\dots)_2 \end{aligned}$$

As an illustrative example, let  $x_0 = 0.75$  and  $\mu = 3.93$ , then the first 8 entries of  $c$  can be obtained from  $x_1$  by  $x_1 = (3.93 \times 0.75 \times 0.25)_{10} = (0.736875)_{10} = (0.10111100\dots)_2$ . Thus, the following sequence can be obtained as:

$$\begin{aligned} c(0) &= 1, c(1) = 0, c(2) = 1, c(3) = 1, \\ c(4) &= 1, c(5) = 1, c(6) = 0, c(7) = 0. \end{aligned}$$

VII. PERMUTATION

If a subpart of the watermarked image was extracted, the watermark could no longer be recovered. However, even at this minimum image size, the watermark could still be recovered, however, part of the watermark was destroyed. Therefore the permuting function which performs pixel permutation on the watermark is modified.

This permutation process is defined as  $T_K$ , and the permutation matrix is given by

$$T_K = \begin{bmatrix} 1 & 1 \\ K & K+1 \end{bmatrix} \tag{5}$$

For any positive integer  $K$ , there exists a minimum number  $\rho(K)$  such that  $T_K^{\rho(K)} = I_2$ , the  $2 \times 2$  identity matrix. The quantity  $\rho(K)$  is referred as the period. It is clear that if  $\alpha + \beta = \rho(K)$ , then  $(T_K^{\alpha})^{\beta} = I_2$ . The permutation is performed on the pixel positions of watermark  $w$ . The permuted watermark  $w_p$  is given by

$$w_p(x', y') = w(x, y) \tag{6}$$

where

$[x' \ y']^T = T_K^{\alpha} [x \ y]^T \pmod{N_p}$ , for  $0 \leq x, y \leq m-1$ ,  $N_p$  is some integer with  $N_p \geq N$ .  $[x \ y]^T$  is denoted as the matrix transpose and  $\alpha < \rho(K)$ . This permuted watermark can be easily retrieved by additional  $T_K^{\beta}$  operation on  $w_p$ , where  $\alpha + \beta = \rho(K)$ .

There are three purposes for performing the permutation on the watermark. First, the spatial correlation can be removed. Second, the watermark is robust against picture-cropping operations. Third, the parameters  $K$  and  $\alpha$  can be kept for security considerations.

VIII. WATERMARK EMBEDDING SCHEME

The DCT transforms image  $f(x, y)$  blocks from spatial domain to frequency domain, the transform and inverse transform are defined as:

$$\begin{aligned} F(u, v) &= \frac{2}{N} C(u)C(v) \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} f(x, y) \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N} \\ f(x, y) &= \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)F(u, v) \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N} \end{aligned}$$

where  $C(m) = 1/\sqrt{2}$  for  $m = 0$  and  $c(m) = 1$  elsewhere.

The energy of most natural images are concentrated in lower frequency rang, and the information hidden in the higher frequency components might be discarded after quantization operation of lossy compressions.

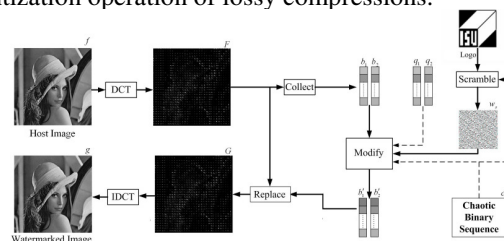


Figure 9. The overall block diagram of JPEG encoder and decoder

The overall block diagram of JPEG encoder and decoder is depicted as Fig. 9.

Let the block  $b(u,v)$  denote the transformed coefficients. The quantization is performed by

$$b_q(u,v) = \text{round}(b(u,v)/q(u,v)), \quad 0 \leq u,v < 8 \quad (7)$$

where  $q(u,v)$  is the quantization table of size  $8 \times 8$ .

In the decoding process, the quantity  $b'(u,v)$  is retrieved from the de-quantization

$$b'(u,v) = b_q(u,v) \times q(u,v), \quad 0 \leq u,v < 8 \quad (8)$$

The data loss of JPEG compression comes from the rounding operation in (7) and the retrieval in (8).

We proposed the watermarking embedded scheme comprises the following nine steps:

Let  $f$  denote the 8-bit gray level host image of size  $M \times M$  and  $w$  denote the  $N \times N$  binary watermark image to be hidden in  $f$ , where  $N^2 \leq M^2/16$ . Here, in the sense of raster scan order,  $w = w(x,y)$ ,  $0 \leq x,y < N$  may be regarded as an 1-dimension array  $w = w(l)$ ,  $l = x + y \times N$ .

**Step 1: Watermark Generation**

Using the watermark generation to encode  $M$ , host image  $F$  to obtain  $w_g$  by:  $w_g = \text{Gen}(M, F) = \text{Mix}(S, D, M)$  where Description  $D = \text{Classify}(F)$ , and Signature  $S = \text{RSA}(\text{Hash}(\text{Mix}(D, M)))$ .

**Step 2: Scramble.**

Perform the scrambling operation on the watermark  $w_g$  to obtain  $w_s$  by  $w_s = w_g \oplus c$ , where  $c$  is the chaotic binary sequence of size  $N \times N$ .

**Step 3: Permutation.**

Perform the permuting operation on the scrambled watermark  $w_s$  to obtain  $w_p$  by:

$$w_p(x', y') = w_s(x, y)$$

where  $[x' \ y']^T = T_k^\alpha [x \ y]^T \pmod{N_p}$  for  $0 \leq x, y < N$ ,  $N_p$  is some integer with  $N_p \geq N$  and  $\alpha < \rho(K)$ .

**Step 4: Bipolar.**

Transform the watermark value using the bipolar function. The watermark value is defined in the bipolar form  $\{-1, 1\}$ , namely,

$$w_b(x, y) = \begin{cases} 1, & \text{if } w_p(x, y) = 1 \\ -1, & \text{else} \end{cases} \quad (9)$$

**Step 5: DCT.**

Perform the block transform of the host image  $f$  using DCT to obtain  $F$ . The block size is chosen to be  $8 \times 8$  to adapt the JPEG compression standard.

The transformed blocks are sequentially labeled as  $B_k$  for  $0 \leq k < M \times M / 64$ .

**Step 6: Collect.**

Collect the middle frequency coefficients: For each  $8 \times 8$  block  $B_i$ , collect 16 coefficients out of the middle frequency coefficients. Eight of them are appended to the

sequence  $b_1(j)$  and the other eight are appended to  $b_2(j)$ , where the index  $j$  related to  $i$  is labeled as shown in Fig. 10.

Thus both of the sequences  $b_1$  and  $b_2$  have  $((M \times M)/(8 \times 8)) \times 8 = (M \times M)/8$  elements.

Define the sequence  $q_1$  and  $q_2$  as:

$$q_1 = 11, 12, 13, 20, 26, 28, 18, 25$$

$$q_2 = 11, 12, 12, 20, 26, 28, 19, 15$$

where the entries are selected from the quantization table and corresponding to  $b_1$  and  $b_2$ . And then, repeat the sequence such that  $q_1, q_2$  and  $b_1, b_2$  have the same lengths.

According to the defined map  $\gamma$  from  $\{0, 1, 2, \dots, N \times N - 1\}$  to  $\{0, 1, 2, \dots, (M \times M / 8) - 1\}$  for select subsequences.

The sequences  $q_1, q_2$ , map  $\gamma$ , and the sequences  $b_1, b_2$  are modified to obtain  $b'_1$  and  $b'_2$ . Furthermore let  $b'_1 = b_1$  and  $b'_2 = b_2$ .

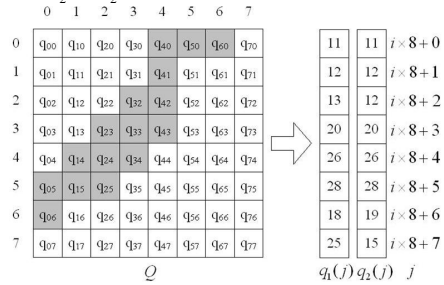


Figure 10. The Selected Coefficients of Middle Frequency

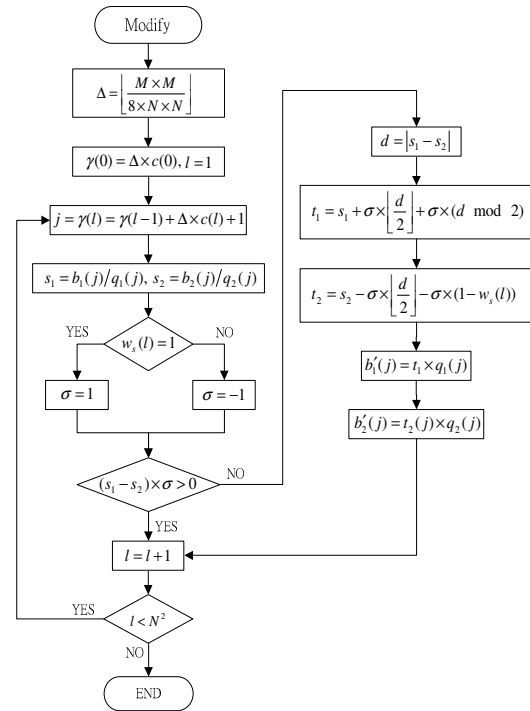


Figure 11. The Flowchart of Modify Process.

**Step 7: Modify.**

The flowchart of modify process is depicted as Fig.11. which illustrates the modification of the middle frequency

coefficients: For the preprocessed watermark  $w_b$  of size  $N \times N$ , one labels the pixels sequentially as  $w_{b,j}(l)$  where  $l$  and  $j$  run through  $0 \leq l < 16$  and  $0 \leq j < M \times M / 64$ , respectively.

**Step 8: Replace.**

Replace the sequences  $B_j(l)$  into  $F$  to obtain  $G$  by reversing the procedure given in Step 6.

**Step 9: IDCT.**

Perform the inverse block DCT on  $G$  to obtain  $g$ .

**IX. WATERMARK EXTRACTING SCHEME**

The block diagram of the extracting process is given in Fig. 12, and the detail of the extracting process as follows:

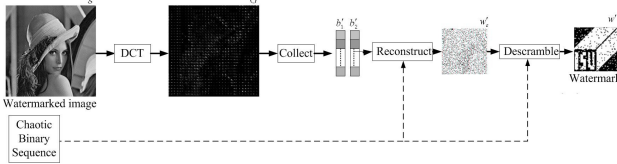


Figure 12. Watermark Extracting Scheme

**Step 1: DCT.**

Perform the block transform of the watermarked image  $g$  using DCT to obtain  $G$ .

**Step 2: Collect.**

Perform the block transform of the watermarked image  $g$  using DCT to obtain  $G$  and collect the mid-frequency region of  $G$  as sequences  $b'_1(j)$  and  $b'_2(j)$ , for  $0 \leq j < (M \times M) / 8$ .

Let  $\gamma$  be the same map defined in modify process of the embedding scheme and  $j = \gamma(l)$ .

**Step 3: Reconstruct.**

Retrieve the permuted watermark using the demodulation function defined as:

$$w_{b,j}'(l) = \sigma = \text{sign}(|b'_1(j)| - |b'_2(j)|) \quad (10)$$

**Step 4: Debipolar**

Inverse the watermark value using the inverse bipolar function:

$$w'_p(x, y) = \text{inbipolar} [w'_b(x, y)] \quad (11)$$

where  $0 \leq x, y < N$ ,  $w'_p(x, y) \in \{-1, 1\}$

$$\text{inbipolar} (w) = \begin{cases} 1, w = 1 \\ 0, w = -1 \end{cases}$$

**Step 5: Depermute**

Reverse the permutation. The reverse can be achieved by the transform  $T_s^{\beta}$  on the pixel positions of  $w'_p$ , where  $r$  is given in step 2 in the embedding method.

**Step 6: Descramble.**

Reverse the scrambling process using the chaotic binary sequence  $c$  to obtain  $w'_g$  by  $w'_g = w'_s \oplus c$ .

**Step 7: Watermark Decoder.**

Reverse the watermark generation process to obtain the retrieved watermark and Signature by  $w' = \text{Gen}^{-1}(w'_g)$ .

**X. THE INTEGRITY OF IMAGE AND AUTHENTICATION DETECT SCHEME**

The new frequency domain image is denoted by  $G$  which is obtained from  $F$  with the corresponding modified coefficients  $B_j'(l)$ . The watermarked image is the inverse DCT of  $G$ , and denoted as  $g$ . The integrity of image and authentication detect scheme is shown in Fig. 13. After modify process, the sequences  $b'_1$  and  $b'_2$  reduce to the mid-frequency region of  $F$  to obtain  $G$ , and inversed the block DCT on  $G$  to obtain the watermarked image  $g$ .

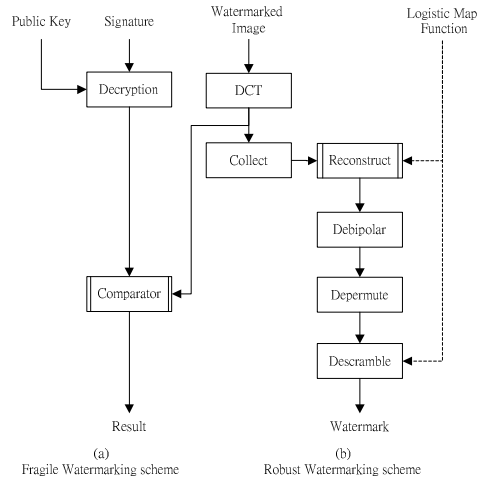


Figure 13. The Integrity of Image and Authentication Detect Scheme

Because of the reason that the signature base watermark technique is designed based on the fragile watermarking scheme such that when the watermark is under malicious falsification such as modification or alteration, the damaged image can be detected and positioned according to the conditions of damaged signature. When the image is under attack of compression, since the features of image have not been altered, the proposed mechanism can endure incidental loss of compression attack. Thus the image can be protected from malicious falsification and the position of falsification can be detected effectively as Fig. 14.

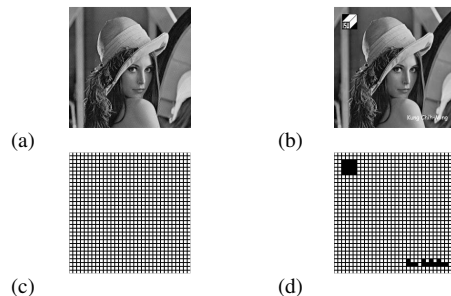


Figure 14. (a) Normal image, (b) Modify image, (c) Signature of normal image, (d) Signature of modify image.

**XI. MEASUREMENT OF THE QUALITY**

The measurement of the quality between two images  $f$  and  $g$  of sizes  $N \times N$  is defined as:

$$PSNR = 10 \times \log(255^2 / MSE) \tag{12}$$

where  $MSE = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (f(x, y) - g(x, y))^2 / N^2$ .

The similarity between the original watermark  $w$  and the retrieved watermark  $w'$  is measured by

$$NC(w, w') = \frac{w \cdot w'}{w \cdot w} = \frac{\sum_x \sum_y w'(x, y) \times w(x, y)}{\sum_x \sum_y w(x, y)^2} \tag{13}$$

$NC(w, w')$  implies stronger evidences. Evidently, (13) measures the amount of altered information which is originally one and is denoted as white NC (WNC). In order to accurately calculate the effect of the attack, the amount of altered information which is originally zero and denoted as black NC (BNC) are also calculated. The formula of BNC is the same as (13) with all 1's changed to 0's and vice versa.









XII. EXPERIMENTAL RESULTS AND CONCLUSION

The proposed method has been simulated using the C++ program on Windows XP platform. All the watermarks are binary images of size 128x128 and the host images are 8-bit gray level images of size 512x512.

It is observed that the qualities (PSNR) of embedded image with respect to the host image are more than 36 dB in average. In Table 1, all watermarks are visible. Also, the NC values of the retrieved watermarks are all above 99%. This demonstrated that the proposed scheme provides a good mechanism for watermarking applications.

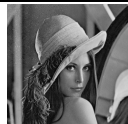

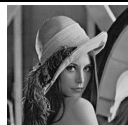

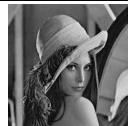

To demonstrate the robustness of the proposed scheme, the 'Lena' image is tested using the "ISU" logo as watermark. The embedded images are then subjected to attacks by various image operations such as JPEG compression, sharpen, blur, noise and cropping. The results obtained are summarized in Table 2.

TABLE I. QUALITY OF WATERMARKED IMAGES AND RETRIEVED WATERMARKS, IN WHICH DIFFERENT HOST IMAGES ARE USED.

Watermarked Image	Retrieved Watermark	Results	
		PSNR	Signature
		PSNR	37.4
		WNC	0.999
		BNC	0.998
		Loss	0.09%
		Signature	Verify
		PSNR	36.1
		WNC	0.999
		BNC	0.997
		Loss	0.17%
		Signature	Verify
		PSNR	37.6
		WNC	0.998
		BNC	0.999
		Loss	0.12%
		Signature	Verify
		PSNR	38.6
		WNC	0.999
		BNC	0.996
		Loss	0.22%
		Signature	Verify

Various degrees of compression using JPEG are applied to the watermarked image. It can be found that using the traditional approaches for the uncompressed images could obtain excellent results for both the clarity of watermark and the quality of image. Nevertheless, the higher the compression rate the more severe the watermark is corrupted. When the BPP of image is down to 0.54 (Compression ratio was up to 14.81), the loss of the watermark was about 33%, and the watermark can no longer be recognized. Employing the proposed algorithm, even though there are minor corruptions on watermark in uncompressed images, the corruption rate does not increase with the compression rate. This suggests that the presented approach.

TABLE II. QUALITY OF THE WATERMARKED IMAGES AND THE RETRIEVED WATERMARKS UNDER VARIOUS JPEG COMPRESSION RATIOS.

Watermarked Image	Retrieved Watermark	Results	
		Compress Ratio	Signature
		6.25	Verify
		WNC	0.998
		BNC	0.997
		Loss	0.53%
		Signature	Verify
		11.43	Verify
		WNC	0.979
		BNC	0.948
		Loss	5.17%
		Signature	Verify
		13.69	Verify
		WNC	0.881
		BNC	0.709
		Loss	27.7%
		Signature	Verify

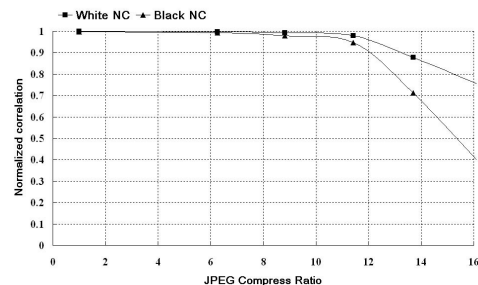


Figure 15. Normalized correlation versus JPEG compress ratio for the proposed scheme.

Fig. 15 shows the quality of the watermarked images and the retrieved watermarks under various JPEG compression ratios and illustrate the normalized correlation versus JPEG compress ratio for the proposed scheme. As demonstrated in the experimental results, the proposed intellectual property rights protection scheme can visually identify the owner of image, the signature can be completely retrieved from the compressed watermarked image, and the falsification position within the image can be detected when the image is falsified.

REFERENCES

[1] C. Y. Lin and S. F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," *IEEE Transaction on circuits and systems of video technology*, vol. 11 (2), pp. 153-168, 2001.

- [2] C. M. Kung, J. H. Jeng, and C. H. Kung, "Watermarking Base on Block Property," *16th IPPR Conference on Computer Vision, Graphics and Image Processing*, pp. 540-546, 2003.
- [3] B. M. Macq and J. J. Quisquater, "Cryptology for digital TV broad-casting," *Proc. IEEE*, pp. 944-957, 1995.
- [4] M. D. Swanson, M. Kobayashi and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, pp. 1064-1087, 1998.
- [5] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamon, "Secure spread spectrum watermarking for multimedia," *Image Processing, IEEE Transactions on*, pp. 1673-1687, 1997.
- [6] E. Koch, J. Rindfrey and J. Zhao, "Copyright protection for multimedia data," in *Proc. Int. Conf. Digital Media and Electronic Publishing*, 1994.
- [7] C. T. Hsu and J. L. Wu, "Hidden digital watermarks in images," *IEEE Trans. on Images Processing*, pp. 58-68, 1998.
- [8] G. Voyatzis and I. Pitas, "Embedding robust watermarks by chaotic mixing," in *Proceedings of 13th International Conference on Digital Signal Processing (DSP'97)*, pp. 213-216, 1997.
- [9] M. Kutter, F. Jordan and F. Bossen, "Digital watermarking of color images using amplitude modulation," *Journal of Electronic Imaging*, pp. 326-332, 1998.
- [10] C. M. Kung, J. H. Jeng.; T. K. Truong.; "Watermark technique using frequency domain," *Digital Signal Processing, 2002 14th International Conference*, vol. 2, pp. 729 -731, 2002.
- [11] A. Sinha, A. Das, and S. Pandith, "Pattern based robust digital watermarking scheme for images," *Acoustics, Speech, and Signal Processing, 2002 IEEE International Conference*, pp. 3481-3484, 2002.
- [12] F. Alturki and R. Mersereau, "An oblivious robust digital watermark technique for still images using DCT phase modulation," *Acoustics, Speech, and Signal Processing, 2000. ICASSP '00. Proceedings. 2000 IEEE International Conference on*, vol. 4 (14), pp. 1975-1978, 2000.
- [13] S. K. Bandyopadhyay, D. Bhattacharyya, P. Das, "Quantum Watermarking and Extraction for handwritten signature", *Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference*, pp. 959-963, 2008
- [14] M. Wang; K. Fan; X. Li; Q. Zeng, "A Novel Digital Content Protection Scheme Combining Iris Identity Based Digital Signature and Semi-fragile Watermark", *Communication Technology, 2006. ICCT '06. International Conference*, pp.1-4, 2006
- [15] C. M. Kung, T. K. Truong and J. H. Jeng, "A Robust Watermarking for Image Authentication Technique", *2003 IEEE International CARNAHAN Conference on Security Technology, 37th Annual Conference*, pp.400-404, 2003.
- [16] Q. Sun, S. Chang, "A secure and robust digital signature scheme for JPEG2000 image authentication", *Multimedia, IEEE Transactions*, vol. 7(3), pp. 480-494, 2005.
- [17] L. Me; R. G Arce, "A class of authentication digital watermarks for secure multimedia communication", *Image Processing, IEEE Transactions*, vol. 10(11), pp. 1754-1764, 2001.
- [18] J. R. Shyu, J. H. Jeng; T. K. Truong, "Fast Fractal Image Compression Using Frequency Domain with Classification", 1999.
- [19] C. W. Wu and N. F. Rul'kov, "Studying chaos via 1-D maps-a tutorial," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions*, pp.707-721, 1993.
- [20] A. Sinha, A. Das, and S. Pandith, "Pattern based robust digital watermarking scheme for images," *Acoustics, Speech, and Signal Processing, 2002 IEEE International Conference on*, vol. 4, pp.3481-3484, 2002.



**Chih-Ming Kung** was born in Tainan, Taiwan, R. O. C. He received the B.S. degree in electronic engineering from Fu Jen Catholic University, Taiwan, R. O. C., in 1991, the M.B.A degree in business and operations management from Chang Jung Christian University, Taiwan, R. O. C., in 1999, and the Ph.D. degree in electrical engineering from the I-Shou University, Taiwan, R. O. C., in 2006. He is the Assistant Professor at Department of Information Technology and Communication, Shih Chien University Kaohsiung Campus, Kaohsiung County, Taiwan, R.O.C. His research interests include watermarking, soft-computing, image compression, and error-correcting code.



**Shu-Tsung Chao** was born in Tainan, Taiwan, R. O. C. He received the B.S. and M.S. degree in information & computer engineering from Chung-Yuan Christian University, Taiwan, R. O. C. He is the Lecturer at Department of Engineering & Management of Advanced Technology, Chang Jung Christian University, Tainan County, Taiwan, R.O.C. His research interests include watermarking, image compression, channel router, and embedded system.



**Yen-Chen Tu** was born in Taichung, Taiwan, R. O. C. He received the B.S. degree in industrial engineering & management from Hsing-Kuo University of Management, Taiwan, R.O.C., in 2005, the M.B.A. degree in business and operations management from Chang Jung Christian University, Taiwan, R.O.C., in 2008. Her research interests include watermarking, optimization algorithm, multi-project wafers, and technology management.



**Yu-Hua Yan** was born in Kaohsiung, Taiwan, R. O. C. She received the B.S. degree in Health Care Administrator from Chang Jung Christian University, Taiwan, R.O.C., the M.S. degree in business and operations management from Chang Jung Christian University, Taiwan, R.O.C. She is a Ph.D. candidate in Graduate Institute of management from the National Kaohsiung First University of Science and Technology, Taiwan, R. O. C. She is the Senior Specialist at Tainan Municipal Hospital, Tainan County, Taiwan, R.O.C. Her research interests include watermarking, health care industry, management performance, and network.



**Chih-Hsien Kung** was born in Tainan, Taiwan, R.O.C. He received the B.S. degree in electrical engineering from Feng-Chia University, Taichung, Taiwan, in 1989, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Missouri, Columbia, in 1991 and 1995, respectively. He joined the faculty of the Department of Engineering & Management of Advanced Technology, Chang-Jung Christian University, Tainan, Taiwan, in 2002, where he is now an Associate Professor. His research interests include watermarking, image compression, artificial intelligence, soft-computing, and VLSI architecture design.