Available online at www.sciencedirect.com

ScienceDirect

The Journal of Systems and Software 81 (2008) 1118–1129

The Journal of Systems and Software

www.elsevier.com/locate/jss

Adaptive watermark mechanism for rightful ownership protection

Chin-Chen Chang [a,b,*], Pei-Yu Lin [b]

[a] *Department of Information Engineering and Computer Science, Feng Chia University, 100 Wenhwa Road, Seatwen, Taichung 40724, Taiwan*
[b] *Department of Computer Science and Information Engineering, National Chung Cheng University, 160 San-Hsing, Min-Hsiung, Chiayi 621, Taiwan*

Received 13 February 2007; received in revised form 18 June 2007; accepted 25 July 2007
Available online 28 August 2007

Abstract

Watermarking is used to protect the integrity and copyright of images. Conventional copyright protection mechanisms; however, are not robust enough or require complex computations to embed the watermark into the host image. In this article, we propose an adaptive copyright protection scheme without the use of discrete cosine transformation (DCT) and discrete wavelet transformation (DWT). This novel approach allows image owners to adjust the strength of watermarks through a threshold, so that the robustness of the watermark can be enhanced. Moreover, our scheme can resist various signal processing operations (such as blurring, JPEG compression, and noising) and geometric transformations (such as cropping, rotation, and scaling). The experimental results show that our scheme outperforms related works in most cases. Specifically, our scheme preserves the data lossless requirement, so it is suitable for medical and artistic images.

Keywords: Copyright protection; Digital watermarking; Lossless images; Sobel; Torus automorphism; Digital signature

1. Introduction

Digital multimedia such as images, texts, music, and pictures are often interflowed through open channels of the Internet. Without proper protection mechanisms, digital data could be easily copied, modified, tampered, or forged without legal authorization during multimedia transmission. Hence, how to protect the integrity, validity, and ownership of digital multimedia is an important issue (Rivest et al., 1978; Katzenbeisser and Petitcolas, 2000; Chang et al., 2004; Nikolaidis and Pitas, 2004). DES (DES, 1997) is the main technique used to protect secret information from unauthorized tampering. The cipher text encrypted by DES; however, usually appears meaningless; this often catches the attention of intruders who are able to intercept the transferred message. The intruder can decrypt or disturb these messages, so that the original message recipient cannot obtain valid information.

Consequently, digital watermarking was brought forth to resolve such situations. Digital watermarking techniques allow users to embed verifiable watermarks such as logo, trademark, or copyright information into the host image without altering the surface of the original image in advance. The verifier can extract the watermarks in order to verify ownership. Digital watermarking can be classified into two types: robust and fragile.

Used to protect the ownership of host images, robust watermarking is embedded into the frequency domain, because watermarks in this domain are more robust than those in the spatial domain. Before embedding a robust watermark into images, engineers usually apply two techniques, discrete cosine transformation (DCT) (Chang et al., 2002a,b; Cox et al., 1997) and wavelet transformation (DWT) (Kim et al., 1999; Barni et al., 2001; Chen et al., 2005), to transform pixels of the host image into

[*] Corresponding author. Address: Department of Information Engineering and Computer Science, Feng Chia University, 100 Wenhwa Road, Seatwen, Taichung 40724, Taiwan. Tel.: +886 4 24517250x3790; fax: +886 27066495.

E-mail addresses: ccc@cs.ccu.edu.tw (C.-C. Chang), linpy@cs.ccu.edu.tw (P.-Y. Lin).

0164-1212/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2007.07.036

its corresponding frequency domain. However, these techniques are time-consuming and alter the significant pixels of the host image, thus decreasing the image quality.

In contrast, fragile watermarking authenticates the integrity of images by embedding watermarks in the perceptually invisible parts of the spatial domain. The quality of the image processed with fragile watermarking is better than that of robust watermarking. Hence, the intruder may not pay attention to the inconspicuous information when watermarked media are delivered through an open channel. However, the robustness of fragile watermarking is not as good as that of robust watermarking.

Conventional watermarking methods embed watermarks into host images in the frequency domain for the sake of robustness and stability (Chang et al., 2002a,b; Kim et al., 1999; Cox et al., 1997; Barni et al., 2001; Chen et al., 2005). These methods are not only time-consuming but also distort the host image. Chen et al. (2005) proposed a novel copyright-proving scheme that could resist malicious attacks. The main advantage of their method is that the host image is lossless after watermarks are embedded. However, their scheme is still unsuitable for low computation devices, since it adopts DWT to transform pixels of the host image into the frequency domain and applies the public key cryptosystem to preserve the integrity of signatures.

In this paper, we propose an adaptive copyright protection scheme in the spatial domain. The novel approach allows the image owner to adjust the strength of watermarking through a threshold, so that the robustness of watermarks can be enhanced. Although we embed the watermark in the spatial domain, our scheme can completely achieve the essentials of copyright protection listed as follows (Kundur and Hatzinakos, 1999; Lin and Chang, 2001; Chang et al., 2002c):

Robustness: The extracted copyright must be robust enough so that the ownership of the host image can be verified, even though signal processing attacks and geometric transformation attacks such as blurring, cropping, JPEG compression, rotation, and scaling may occur.

Unambiguity: The extracted logo must be clear enough so that can indicate the ownership of the host image exactly.

Security: Even if intruders figure out the embedding algorithm, they still cannot extract the embedded data without the secret key possessed by the image owner.

Transparency: After watermarks are embedded, the modification of the host image must be inconspicuous to avoid drawing attention from the intruder.

Multiple watermarking: The watermarking algorithms must allow image owners to embed multiple watermarks in the protected image.

Public verification: The watermark can be publicly verified according to a predefined procedure without revealing the secret information of the signer.

Time consumption: Watermark signing and logo verification must be completed within a reasonable period.

Blindness: Even if a protected image has ever been tampered, its copyright can still be verified without the original image.

Experimental results show that our scheme outperforms related works in most cases. Specifically, our scheme preserves the lossless requirement so that it is suitable for medical and artistic images. The rest of this paper is organized as follows. In Section 2, we briefly introduce Sobel technology and Chen et al.'s copyright-proving scheme. Our adaptive copyrights protection scheme is elaborated in Section 3, followed by the experimental results and performance analyses in Section 4. Finally, we make conclusions in Section 5.

2. Literature review

In this section, we briefly describe the common Sobel technology (Armstrong and Gray, 2000; Kazakova et al., 2004; Kanopoulos et al., 1988; Qu et al., 2005) and Chen et al.'s copyright-proving scheme (Chen et al., 2005) in Sections 2.1 and 2.2, respectively.

2.1. Sobel technology

Sobel technology is a famous edge detection approach (Kazakova et al., 2004), which utilizes the kernels to detect the edge directions: horizontal, vertical and diagonal. For instance, Fig. 1a shows the eight neighboring pixels a, b, c, d, e, f, g, and h of an input pixel x of an image. Fig. 1b–e indicate the four Sobel kernels of the input pixel x which defined as follows:

Horizontal kernel

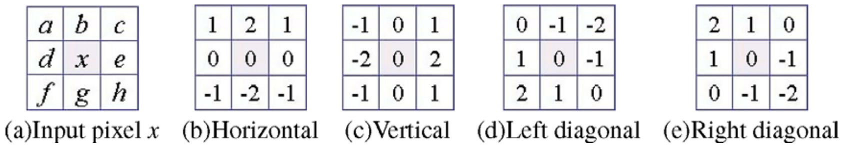
$$E(H) = (a + 2b + c) - (f + 2g + h), \tag{1}$$

Vertical kernel

$$E(V) = (c + 2e + h) - (a + 2d + f), \tag{2}$$

Left diagonal kernel

$$E(DL) = (d + 2f + g) - (b + 2c + e), \tag{3}$$



a	*b*	*c*
d	*x*	*e*
f	*g*	*h*

(a)Input pixel *x*

1	2	1
0	0	0
-1	-2	-1

(b)Horizontal

-1	0	1
-2	0	2
-1	0	1

(c)Vertical

0	-1	-2
1	0	-1
2	1	0

(d)Left diagonal

2	1	0
1	0	-1
0	-1	-2

(e)Right diagonal

Fig. 1. Sobel edge detection kernels.

Right diagonal kernel

$$E(DR) = (b + 2a + d) - (e + 2h + g). \tag{4}$$

Here, $E(H)$ denotes the variance of pixel x in the horizontal direction, $E(V)$ represents the variance of input pixel x in the vertical direction, $E(DL)$ means the variance of pixel x in the left diagonal, and $E(DR)$ indicates the variance of pixel x in the right diagonal, respectively.

Afterward, the four variances are used to measure the gradient $\nabla g(x)$ of the input pixel x, which is defined as

$$\nabla g(x) = \sqrt{E(H)^2 + E(V)^2 + E(DL)^2 + E(DR)^2}. \tag{5}$$

Subsequently, we regard the input pixel x as an edge point if $\nabla g(x) > T$; otherwise, we label the input pixel x as the non-edge point. Here, the parameter T is a threshold defined by the user.

2.2. Chen et al.'s scheme

The main idea of Chen et al.'s scheme (Chen et al., 2005) is to apply the discrete wavelet transformation (DWT) technique to obtain the t-level LL subband of the copyright image. A verification key is generated by the t-level LL subband and the logo image. There are three roles in their method: the Signer, the Verifier, and Trusted Authority (TA). The signer takes the responsibility for constructing the signature of the host image, the verifier can be anyone who wants to check the ownership of the host image, and TA is the trusted third party. Pub_SK is the public key of the signer and Pri_SK is the corresponding private key while Pub_TAK is the public key of TA and Pri_TAK is the corresponding private key. The signing procedure consists of four phases: t-level wavelet transformation, polarity table construction, verification key generation, and digital signature signing.

Phase 1: t-level wavelet transformation

In the first phase, the signer decomposes a gray-level copyright image C of $H_c \times W_c$ pixels by discrete wavelet transformation. The decomposed wavelet transformation has four subbands LL_1, LH_1, HL_1, and HH_1. The subband LL_1 containing the major energy of the image is the lowest-frequency component in level one. The signer further applies the wavelet transformation to decompose LL_1 into subbands LL_2, LH_2, HL_2, and HH_2. Repeat the decomposition on the lowest-frequency subband t times, we have the lowest-frequency subband LL_t of $H_t \times W_t$ pixels in the t-level wavelet transformation,

$$LL_t = \{LL_t(i,j) | 0 \leqslant i \leqslant H_t, 0 \leqslant j \leqslant W_t\}. \tag{6}$$

Here, $LL_t(i,j)$ means the pixel value located in ith row and jth column of subband LL_t.

Phase 2: Polarity table construction

The signer subsequently constructs a polarity table P by comparing each pixel $LL_t(i,j)$ of LL_t with an average value avg as follows:

$$p_{i,j} = \begin{cases} 0, & \text{if } LL_t(i,j) < avg \\ 1, & \text{if } LL_t(i,j) \geqslant avg \end{cases}, \tag{7}$$

where $P = \{p_{i,j} | p_{i,j} \in (0,1),\ 0 \leqslant i \leqslant H_t,\ 0 \leqslant j \leqslant W_t\}$, and avg is the average value of all pixels in subband LL_t.

Phase 3: Verification key generation

The signer then applies a seed s to randomly permute (Hsu and Wu, 1998, 1999) the logo image L to prevent geometric distortions. Let L' be the permuted logo image. Next, the signer can obtain the verification key K by computing:

$$K = P \oplus L'. \tag{8}$$

Note that the security of Chen et al.'s scheme is based on the seed s and the verification key K.

Phase 4: Digital signature signing

Finally, the signer generates the partial signature DS by encrypting the security parameters (s, K, t, H_0, W_0) with its private key as follows:

$$DS = \mathrm{Sign}_{\mathrm{Pri\_}SK}(s, K, t, H_0, W_0), \tag{9}$$

where $\mathrm{Sign}_{\mathrm{Pri\_}SK}(\cdot)$ is the digital signature function with the private key Pri_SK. The signer then sends DS to the trusted authority TA to have it authorized. After TA authenticates the validity of the host image and accepts the signing request, it constructs the other partial signature TS as follows:

$$TS = TM_{\mathrm{Pri\_}TAK}(DS), \tag{10}$$

where $TM_{\mathrm{Pri\_}TAK}(\cdot)$ is the timestamp function with TA's private key Pri_TAK. Afterwards, (DS, TS) is the signature of the protected copyright image O.

Once a dispute arises, the verifier can utilize TA's public key Pub_TAK to verify TS and apply the signer's public key Pub_SK to check the validity of DS. Subsequently, the verifier can verify the ownership of the protected copyright image by the singing procedure.

3. The proposed scheme

Our scheme consists of two procedures: the signing procedure and the verification procedure. The signing procedure details how signers retrieve the significant features of the host image and combine them with an authorized logo to generate effective certificates. The second one discusses how the verifiers check the copyright of the protected image. There are three roles in our scheme: the Signer, the Verifier, and Trusted Authority (TA). The signer takes the responsibility for constructing the verification information of the host image, the verifier can be anyone who wants to check the ownership of the host image, and TA is responsible for generating the certificate of the protected image for the signer. The details of these two procedures are presented in Sections 3.1 and 3.2, respectively.

3.1. The signing procedure

The signing procedure is composed of five phases: Scaled image generation phase, Edge map generation phase, Logo permutation phase, Verification map generation phase, and Certificate generation phase. The block diagram of the procedure is shown in Fig. 2. We subsequently describe the details of these phases as follows.

Phase 1: Scaled image generation

Assume that the protected host gray-level image O has $N \times N$ pixels.

Step 1: The signer divides O into 8×8 non-overlapping blocks o_i's; namely, $O = \{o_1, o_2, \ldots, o_{(N/8)\times(N/8)}\}$.

Step 2: The signer then calculates a mean value m_i of each block o_i, for $i = 1,2,\ldots,(N/8) \times (N/8)$. By collecting all the mean values m_i's, the signer can obtain a scaled image with $(N/8) \times (N/8)$ pixels which represents the reduction of the host image O.

Phase 2: Edge map generation

Here, Sobel technology (Kazakova et al., 2004) is used to detect the edge features of the scaled image. Suppose the eight pixels a, b, c, d, e, f, g, and h are the neighboring of m_i in the scaled image, for $i = 1,2,\ldots,(N/8) \times (N/8)$.

Step 1: First, the signer has to figure out the variances of the four directions, as depicted in Fig. 1b–e, of each m_i by applying the Eqs. (1)–(4).

Step 2: Subsequently, the signer computes the gradient $\nabla g(m_i)$ of m_i by Eq. (5),

$$\nabla g(m_i) = \sqrt{E(H)^2 + E(V)^2 + E(DL)^2 + E(DR)^2}.$$

Step 3: According to $\nabla g(m_i)$, the signer is able to classify m_i into two distinct types: edge point and smooth point. If $\nabla g(m_i) \geqslant T$, m_i is regarded as an edge point; otherwise, it is a smooth one.

Step 4: According to Eq. (11), the signer generates an edge map $E = \{m_i' | i = 1, 2, \ldots, (N/8) \times (N/8)\}$ from the scaled image, where m_i' is 1 if m_i is an edge point; otherwise, m_i' is 0.

$$m_i' = \begin{cases} 0, & \text{if } \nabla g(m_i) < T \\ 1, & \text{if } \nabla g(m_i) \geqslant T \end{cases}. \tag{11}$$

Phase 3: Logo permutation

The signer then applies Torus Automorphism mechanism (Chang et al., 2002d) to scramble the logo image with a seed s. Assume that the permuted logo image L is in a size of $(N/8) \times (N/8)$ pixels.

Phase 4: Verification map generation

Next, the signer applies the exclusive-or operation on the edge map E and the permuted logo image L to create a verification map V as follows:

$$V = E \oplus L. \tag{12}$$

Phase 5: Certificate generation

Step 1: The signer then sends a request for certification to TA along with the verification map V, the image size N, the threshold T, the signer's identity ID_{signer}, and the permuting seed s in a secure channel.

Step 2: After TA receives and accepts the request, it generates a certificate for the host image by computing

$$h_{TA} = H_{TA}(V||N||T||ID_{\text{signer}}||s||t), \tag{13}$$

where $H_{TA}(\cdot)$ is the one-way hash function, t is the timestamp generated by TA, and "||" denotes concatenation.

Step 3: Afterward, TA publishes the certificate h_{TA}, timestamp t, and the hash function $H_{TA}(\cdot)$ on its bulletin board.

An example of how to construct the verification map

Assume that Fig. 3a is the protected host gray-level image O of 6×6 pixels, Fig. 3b is the permuted logo L, and the threshold $T = 200$. To simplify the procedure, we divide O into 2×2 non-overlapping blocks instead of 8×8 non-overlapping blocks. Next, we calculate the mean value m_i for each 2×2 block to generate the scaled image shown in Fig. 3c. For instance, the marked mean value 163 in Fig. 3c is computed by the marked block with pixels 163, 162, 163, and 163 in Fig. 3a, i.e. $(163 + 162 + 163 + 163)/4 = 163$. Subsequently, by applying Eqs. (1)–(4) to this marked value, we have four variances $E(H) = 12$, $E(V) = -156$, $E(DL) = 110$, and $E(DR) = 126$. By Eq. (5), we then have the following gradient

$$\nabla g(163) = \sqrt{12^2 + (-156)^2 + 110^2 + 126^2} = 229.$$

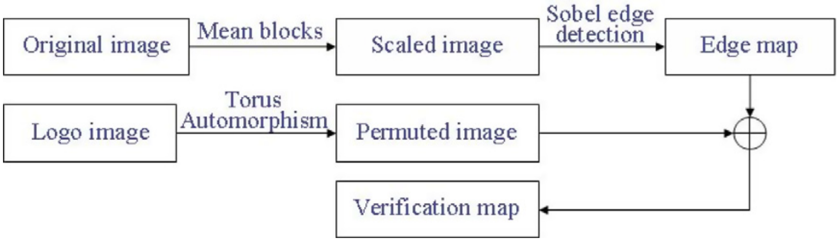
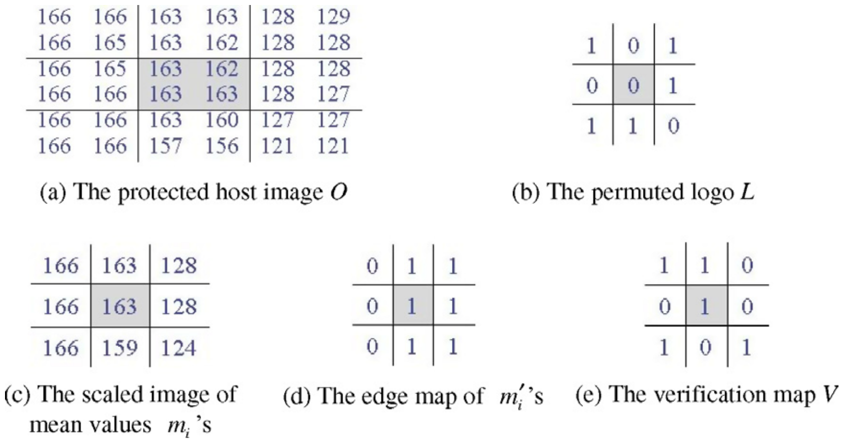


Fig. 2. The block diagram of our signing procedure.



166	166	163	163	128	129
166	165	163	162	128	128
166	165	163	162	128	128
166	166	163	163	128	127
166	166	163	160	127	127
166	166	157	156	121	121

(a) The protected host image O

1	0	1
0	0	1
1	1	0

(b) The permuted logo L

166	163	128
166	163	128
166	159	124

(c) The scaled image of mean values m_i's

0	1	1
0	1	1
0	1	1

(d) The edge map of m_i''s

1	1	0
0	1	0
1	0	1

(e) The verification map V

Fig. 3. The example of the signing procedure.

Since $\nabla g(163) = 229 > T$, the marked value in Fig. 3d must be ‘1’ by Eq. (11), i.e. it is an edge point. And then we can complete the edge map E as shown in Fig. 3d.

According to Eq. (12), the mark component can be determined by applying the exclusive-or operation to the marked values of E and L; namely, $1 = 1 \oplus 0$. In this way, we are able to finish the verification map V as depicted in Fig. 3e.

3.2. The verification procedure

While the verifier receives the protected image along with the information $\{V, N, T, ID_{\text{signer}}, s\}$ and queries the copyright of the image, the verifier can perform this procedure to prove the validity of the copyright. The flowchart of this procedure is shown in Fig. 4. The verification procedure also consists of four phases: Certificate verification phase, New scaled image generation phase, New edge map generation phase, and Logo permutation phase. The details of these phases are described as follows.

Phase 1: Certificate verification

Step 1: The verifier first acquires h_{TA}, t, and $H_{TA}(\cdot)$ from TA's bulletin board.

Step 2: Next, the verifier uses $\{V, N, T, ID_{\text{signer}}, s\}$ and t to compute the following,

$$h^*_{TA} = H_{TA}(V||N||T||ID_{\text{signer}}||s||t). \tag{14}$$

Step 3: The verifier then compares the computation result h^*_{TA} with h_{TA}. If they are not the same, the verifier destroys the information; otherwise, the verifier is convinced that the information $\{V, N, T, ID_{\text{signer}}, s\}$ is valid.

Phase 2: New scaled image generation

The verifier performs the scaled image generation phase in the signing procedure to obtain a scaled image.

Phase 3: New edge map generation

The verifier executes the edge map generation phase in the signing procedure to acquire an edge map E'.

Phase 4: Logo permutation

Step 1: Subsequently, the verifier generates a scrambled map L' by computing

$$L' = E' \oplus V. \tag{15}$$

Step 2: Adopting Torus Automorphism mechanism, the verifier therefore can retrieve a visible logo L^* by re-permuting the scrambled map L' with seed s.

Step 3: Finally, the verifier can visually recognize the retrieved logo L^* and validate the ownership of the test image.

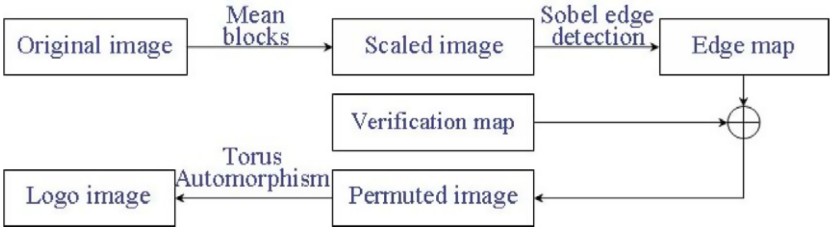


Fig. 4. The block diagram of our verification procedure.

4. Experimental results and analyses

We subsequently conducted several simulations to demonstrate the practicability of our scheme and compared other related schemes with ours in terms of requirements in Sections 4.1 and 4.2, respectively.

4.1. Experimental results

We applied the peak-signal to noise rate (*PSNR*) to measure the image quality of an attacked image. The formula of *PSNR* is described as follows:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\text{dB}. \tag{16}$$

On the other hand, the mean square error (*MSE*) of an image with $H \times W$ pixels is defined as

$$MSE = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(o_{ij} - \tilde{o}_{ij})^2, \tag{17}$$

where o_{ij} is the original pixel value and $\tilde{o}_{ij}$ is the processed pixel value.

Besides, we utilized the accuracy rate AR to evaluate the robustness of a copyright protection scheme for a specific attack. The accuracy rate AR was defined as

$$AR = \frac{CP}{NP}, \tag{18}$$

where NP is the number of pixels of the logo image and CP is the number of correct pixels in the logo image that is retrieved from the attacked image. Furthermore, the average accuracy rate AAR is used to estimate the practicality of a copyright protection scheme for common attacks, which is defined as

$$\text{AAR} = \left(\sum AR\right)/NT, \tag{19}$$

where NT is the number of examined attacks.

4.1.1. Applying attacks to the nature images

The test image 'Lena' and the logo image shown in Fig. 5a and b were used in the simulations. To begin with, we performed several signal processing attacks and geometric transformation attacks on the test image 'Lena' to demonstrate the robustness of our scheme. Under these attacks, the retrieved logo images are still recognizable even though the quality of the attacked image has been seriously distorted.

Attack 1. Blurring
We applied the Gaussian blurring on the test image 'Lena' with two pixels radius, and the *PSNR* value of the attacked image is reduced to 29.3 dB.
Attack 2. Cropping
We applied quarter cropping and surround cropping on the test image 'Lena', and the *PSNR* values of the attack images are decreased to 23.5 dB and 9.41 dB, respectively.

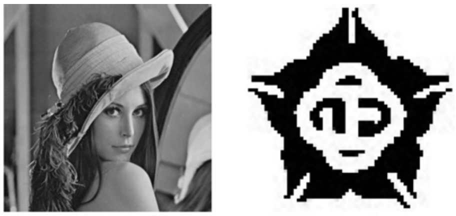

(a) Test image 'Lena' (512×512 pixels)
(b) Logo image (64×64 pixels)

Fig. 5. Test image 'Lena' and logo image.

Attack 3. JPEG lossy compression
We compressed the test image 'Lena' by JPEG with compression rate 13.12%. And, the *PSNR* value of the attacked image is 37.42 dB.
Attack 4. Noising
We applied Gaussian noising on the test image 'Lena' with 7% noise and 23.28 dB *PSNR* value.
Attack 5. Rotation
We rotated the test image 'Lena' by 2° and then resized the processed image to 512 × 512 pixels. The *PSNR* value is down to 14.6 dB.
Attack 6. Scaling
We reduced the size of the test image 'Lena' from 512 × 512 pixels to 128 × 128 pixels. Subsequently, we amplified the size of 'Lena' from 128 × 128 pixels to 512 × 512 pixels again. The *PSNR* value is 29.85 dB.
Attack 7. Sharpening
We sharpened the test image 'Lena' so that the *PSNR* value is reduced to 28.86 dB.
Attack 8. Print-photocopy-scan
We first printed the test image 'Lena' by a 1200dpi laser printer and then scanned the printed image using a 256 gray-level scanner by 300dpi. Subsequently, we resized the scanned image to 512 × 512 pixels. The *PSNR* value is reduced to 19.3 dB.
Attack 9. StirMark
We performed the StirMark attack on the test image 'Lena' with default parameters. The *PSNR* value is decreased to 17.7 dB.
Attack 10. UnZign
We applied the UnZign attack on the test image 'Lena' with default parameters. The *PSNR* value of the attacked image is 25.63 dB.
Attack 11. BPM attack
We performed the BPM attack on the test image 'Lena' by the following procedure:

(a) Divide 'Lena' into non-overlapping blocks with 4 × 4 pixels;
(b) Train a codebook containing 256 codewords by LBG algorithm (Linde et al., 1980);
(c) Match the minimum distortion codeword to replace the original blocks. The *PSNR* value of replaced image is reduced to 30.89 dB.

Fig. 6 illustrates the images under above-mentioned attacks, the corresponding *PSNR* values, and the retrieved logo image with its accuracy rate at $T = 200$. Based on the human visual system (HVS) characteristics, our retrieved logo images are recognizable and beneficial to protect copyright from various attacks.

The accuracy of the proposed scheme is shown in Table 1. The averages of accuracy rates are larger than 91.6% under different thresholds T's. Without loss of generality, a proposed method is said to be robust enough while its accuracy rate achieves 85%. That is, the new scheme is secure and resistant to malicious attacks.

Moreover, we used other gray-level nature images as test images to demonstrate the robustness of our scheme. As shown in Fig. 7a and b, we can raise threshold T to achieve desirable robustness for complex images. For the type of smooth images, we can obtain satisfactory robustness under different threshold T's as demonstrated in Fig. 7c and d. Our scheme still outperforms Chen et al. (2005) in most cases.

4.1.2. Application of our scheme to medical images

Subsequently, we adopted three medical images 'CT', 'MRI', and 'US' as the test images. Fig. 8a is our scaled image from medical image 'CT' while Fig. 8b is Chen et al.'s polarity table generated from the same test image. The edge maps E's constructed by Sobel with different thresholds are listed in Fig. 8c–h, respectively. From the extracted significant features shown in Fig. 8c–h, it can be discovered that our novel scheme is able to describe the essential outline of the scaled image. In comparison

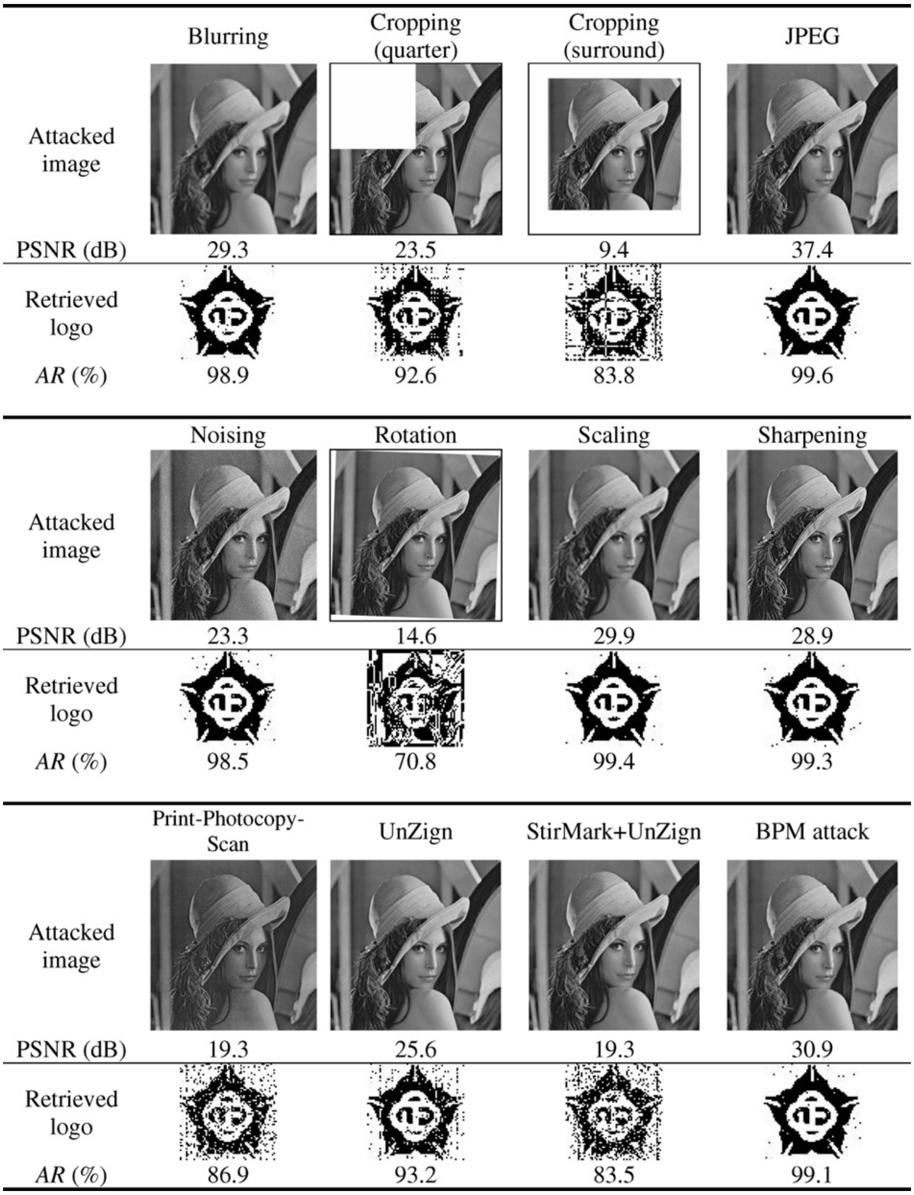
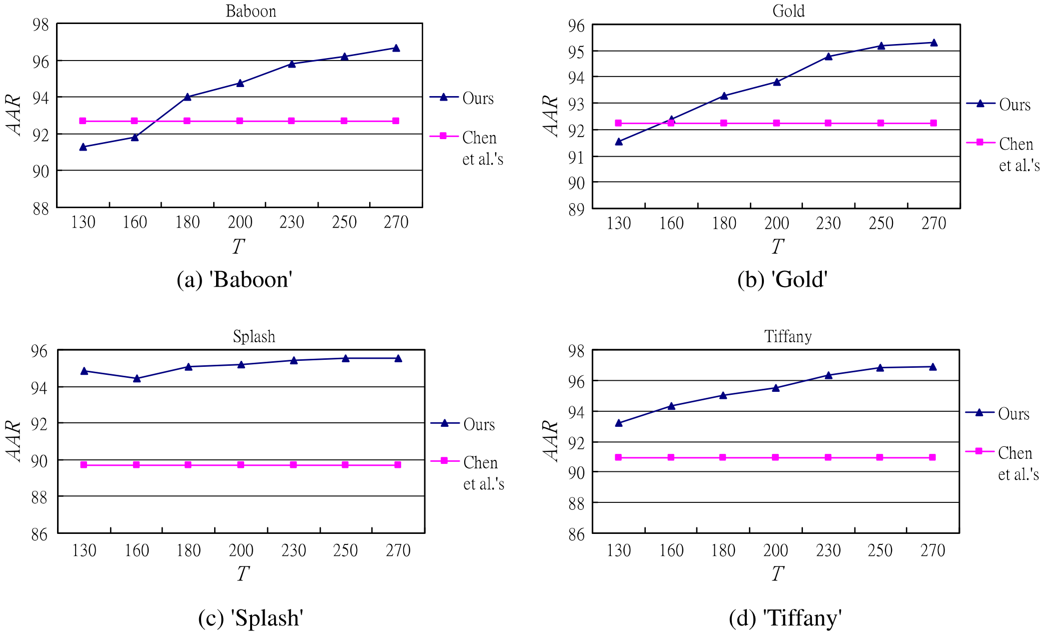


Fig. 6. The attacked images, the corresponding *PSNR* values, and the retrieved logo image with its accuracy rate at $T = 200$.

Table 1
The accuracy rate under various attacks

	PSNR (dB)	Ours					
		$T = 160$	$T = 180$	$T = 200$	$T = 230$	$T = 250$	$T = 270$
Blurring	29.3	98.6	98.4	98.9	98.7	98.8	99.1
Cropping (quarter)	23.5	91.4	91.9	92.6	93.5	94.1	94.8
Cropping (surround)	9.4	82.5	83.2	83.8	84.2	84.3	85.2
JPEG	37.4	99.4	99.5	99.6	99.6	99.6	99.6
Noising	23.3	98.5	98.9	98.5	98.8	99.2	99.1
Rotation	14.6	71.1	70.5	70.8	72.4	72.5	72.9
Scaling	29.9	99.4	99.5	99.4	99.6	99.4	99.5
Sharpening	28.9	99.1	99.3	99.3	99.3	99.4	99.3
Print-photocopy-scan	19.3	85.8	86.2	86.9	86.8	87.4	88.1
UnZign	25.6	92.8	93	93.2	93.5	93.7	94.9
StirMark + UnZign	19.3	81.4	82.1	83.5	83.7	83.9	84.6
BPM attack	30.9	99	99	99.1	99.1	99.3	99.4
AAR		91.6	91.8	92.1	92.4	92.6	93.0



(a) 'Baboon'

(b) 'Gold'

(c) 'Splash'

(d) 'Tiffany'

Fig. 7. The comparisons between Chen et al.'s scheme ([Chen et al., 2005) and ous in the AAR's for nature images.

with Chen et al.'s scheme, Fig. 8c–h present characteristics of the scaled image more effectively than Fig. 8b does.

The scaled medical images of 'MRI' and 'US' generated by Sobel are illustrated in Fig. 9a and d, respectively, while the edge maps from these scaled images are shown in Fig. 9c and f. Furthermore, the polarity tables of the same images constructed by Chen et al.'s scheme are shown in Fig. 9b and e. According to the human visual system characteristics, Fig. 9c and f described the contours more significant than Fig. 9b and e did. What is more, the average accuracy rates AAR's versus different thresholds using medical images 'CT', 'MRI', and 'US' are illustrated in Fig. 10. Undoubtedly, our proposed method outperformed Chen et al.'s scheme in all cases. That is, our scheme is more suitable for protecting lossless medical images than Chen et al.'s.

4.2. More discussions

In this subsection, we discuss how to adjust the threshold to obtain high AAR's and demonstrate that our scheme can meet the requirements of copyright protection mechanisms.

4.2.1. How to adjust the threshold

According to the experimental results, we know that threshold T is a critical factor for determining the robustness of the retrieved logo image. When we adopt a large threshold T in simulation, the average accuracy rate (AAR) can be raised, because the edge points refined by a large threshold are the most outstanding in the host image. Even though we apply signal processing operations (such as blurring, JPEG compression, and noising) and

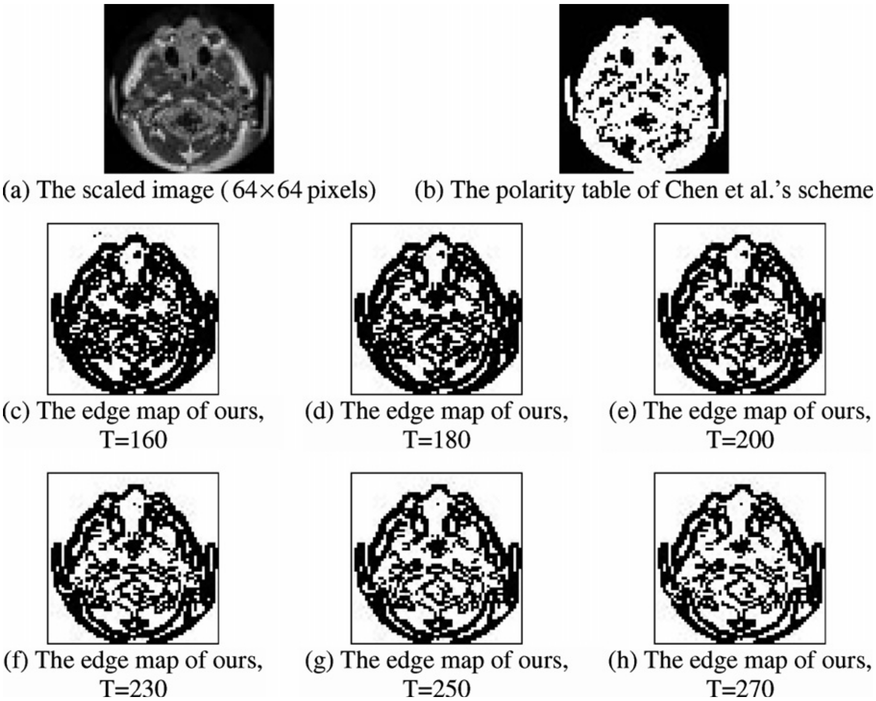

(a) The scaled image (64×64 pixels)
(b) The polarity table of Chen et al.'s scheme
(c) The edge map of ours, T=160
(d) The edge map of ours, T=180
(e) The edge map of ours, T=200
(f) The edge map of ours, T=230
(g) The edge map of ours, T=250
(h) The edge map of ours, T=270

Fig. 8. The extracted feature between Chen et al.'s scheme and ours.

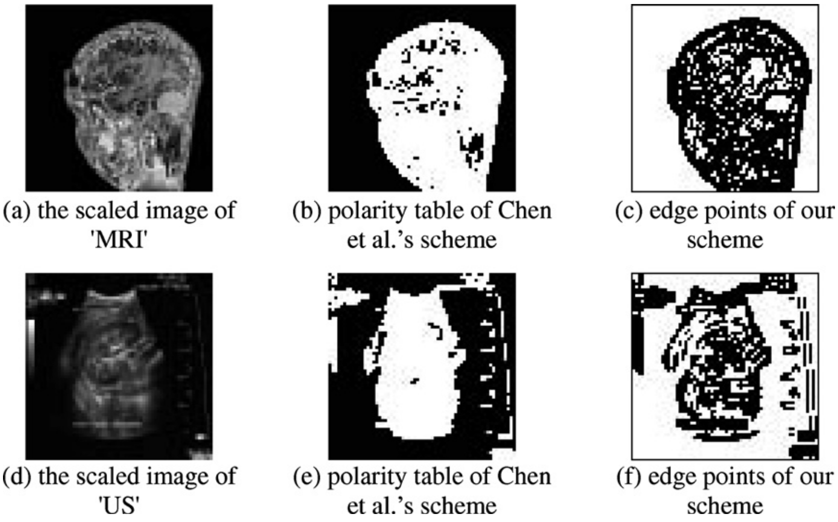
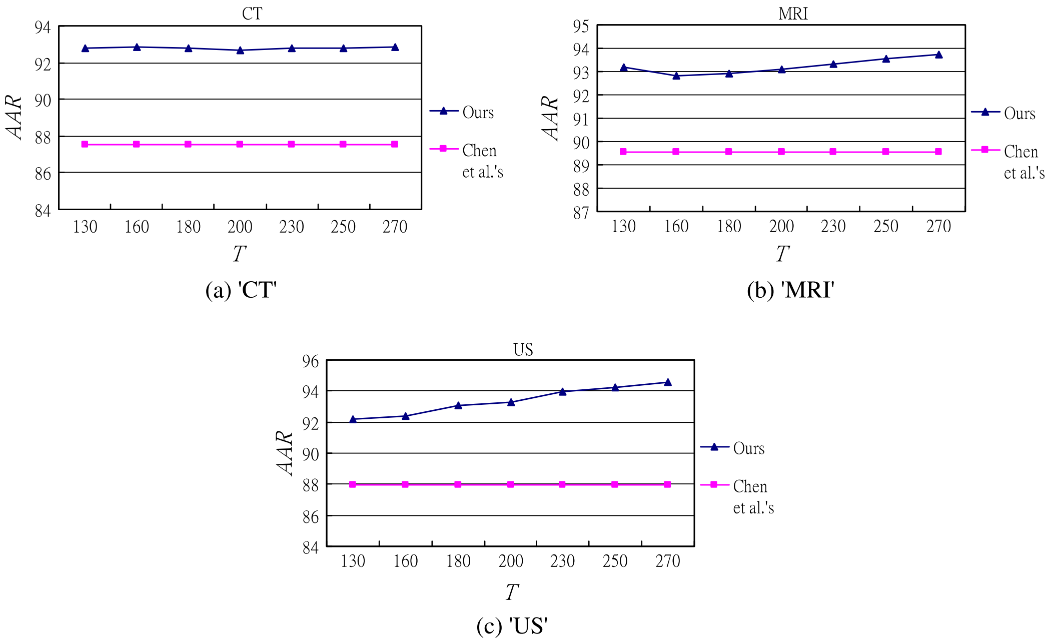

(a) the scaled image of 'MRI'
(b) polarity table of Chen et al.'s scheme
(c) edge points of our scheme
(d) the scaled image of 'US'
(e) polarity table of Chen et al.'s scheme
(f) edge points of our scheme

Fig. 9. The extracted feature between Chen et al.'s scheme and ours at $T = 130$.

geometric transformations (such as cropping, rotation, and scaling) to the host image, these significant features can still be preserved. Nevertheless, this case is only suitable for the rough test images. If we use the smooth test images such as 'Splash' and 'Tiffany' in the experiment, we must lower the threshold; otherwise, most significant points will be filtered out. That is, with a large threshold, the edge map E of a smooth test image cannot stand for the integrity of the host image.

Thus, the following conclusions can be derived. When using a rough test image, we raise the threshold to obtain high AAR's. For a smooth test image, we decrease the threshold, so that the significant features of the host image can be preserved in the edge map. Although we must tune down the threshold in this condition, we still can acquire better AAR's than Chen et al.'s scheme (see Fig. 7c and d).

According to the simulation results, we suggest the threshold $T > 180$ for rough test images (see Fig. 7a and b). Our scheme obtains at least 93% AAR under this threshold. For smooth test images, we propose the threshold $T = [130, 160]$ as shown in Fig. 7c and d and the medical images. If $T = [130, 160]$, then our scheme not only



(a) 'CT'

(b) 'MRI'

(c) 'US'

Fig. 10. The comparisons between Chen et al.'s scheme and ours in the AAR's for medical images.

preserves the outstanding features of the host image in the edge map but also possesses high AAR's.

4.2.2. Discussions on the performance

Performance comparisons between the well-known traditional watermarking schemes and ours are listed in Table 2. Our scheme not only inherits the advantages of Chen et al.'s scheme but also possesses the efficiency better than that of other related schemes. Subsequently, we demonstrate that our scheme can achieve the requirements of copyright protection mechanism as follows.

4.2.2.1. Robustness. From the experimental results, the extracted logos of the attacked images are still visually recognizable after we impose Attacks 1–11 to the test images. That is to say, our scheme is able to resist various attacks. Furthermore, our scheme provides satisfied average accuracy rate AAR's, as described in Table 1, Figs. 7 and 10. Hence, we conclude that our scheme can meet this requirement.

4.2.2.2. Unambiguity. Simulation results show that our scheme possesses high AAR's so that the verifier can unambiguously recognize the ownership of the extracted logo from the attacked image as illustrated in Fig. 6. Consequently, our scheme is able to meet this requirement.

4.2.2.3. Security. We assume that no one can apply a hash function to generate the same hash values with distinct input parameters. After TA confirms the parameters V, N, T, ID_{signer}, s, and t, it generates the certificate of the protected image by Eq. (13). Once a dispute occurs, the verifier can acquire the parameters from a bulletin board maintained by TA and then prove the ownership of the protected image to others. If, an intruder wants to convince others that the ownership of the host image belongs to him/her, he/she has to forge a set of parameters so that the hash value of these fake parameters is the same as h_{TA} generated by Eq. (13). Without the loss of generality, this attempt is computation infeasible. That is, the security of our scheme is based on the difficulty of breaking the one-way hash function.

4.2.2.4. Transparency. As illustrated in Fig. 2, the signing procedure of our scheme does not modify any pixels of the host image. Hence, the protected host image O is lossless after the verification map generation phase. Accordingly, our scheme can meet the lossless requirement. This makes our scheme suitable for medical images, artistic images, and valuable images.

4.2.2.5. Multiple watermarking. Excluding the logo depicted in Fig. 5b, the signer can utilize other logo images and the original image O to construct different verification maps. Afterward, the signer has to request TA to generate the certificate of the novel logos by certificate generation phase. Consequently, the verifier can repeat the verification procedure to retrieve multiple logos from the same protected image. This attempt allows a protected image have multiple ownerships. Thus, our scheme can preserve the requirement.

4.2.2.6. Public verification. As described in Section 3.2, with public information: V, N, T, ID_{signer}, and s, the verifier is able to construct a scaled image and then figure out the detected edge map E'. Next, the verifier can extract a logo L^* by utilizing the exclusive-or operation and Torus Automorphism mechanism. Through the extracted logo, the verifier can visually recognize the ownership of the host image. So our scheme can preserve this requirement.

Table 2
The performance comparison in terms of traditional well-known watermarking schemes and the proposed scheme

	CCC Chang et al. (2002c)	Cox et al. (1997)	Barni et al. (2001)	Chen et al. (2005)	Ours
Lossless	No	No	No	Yes	Yes
Suitability for medical image	No	No	No	No	Yes
Multiple logos	Yes	Yes	No	Yes	Yes
Publicly verifiable	No	No	No	Yes	Yes
Watermark domain	Spatial domain	Frequency domain	Frequency domain	Frequency domain	Spatial domain
Copy attack resistance	Yes	No	No	Yes	Yes
Counterfeit attack resistance	Timestamp	No	No	Timestamp	Timestamp
Extraction/detection	Extraction	Detection	Detection	Extraction	Extraction
Visual recognizable logo	Yes	No	No	Yes	Yes
Robustness	Compression Blurring Sharpening Rotation Repainted	Compression Blurring Scaling Print-photocopy-scan Cropping	Compression Cropping	Compression Blurring Scaling Noising Print-photocopy-scan Cropping Sharpening Rotation BPM attack StirMark attack UnZign attack	Compression Blurring Scaling Noising Print-photocopy-scan Cropping Sharpening Rotation BPM attack StirMark attack UnZign attack

4.2.2.7. Time consumption. As shown in Section 3.1, we retrieve the significant features of protected image from the spatial domain rather than the frequency domain. Namely, our scheme does not apply DCT and DWT mechanisms to the signing procedure. The average running time for retrieving significant features in the new method is 0.003 s while that in DWT mechanisms is 0.111 s. This indicates that the new scheme outperforms other DWT based methods in the signing procedure. Moreover, we sign the verification map using the one-way hash function instead of the public cryptosystem (Sutherland, 1996). Our scheme therefore is able to reduce the time consumption for generating the certificate by 0.1% in comparison with Chen et al.'s scheme (Chen et al., 2005). Hence, our scheme can meet this requirement.

4.2.2.8. Blindness. By applying the exclusive-or operation to the edge map extracted from the protected image and the verification map, the verifier can obtain a logo. The verifier can subsequently visually recognize the ownership of the protected image as illustrated in the verification procedure. So our scheme allows the verifier to check the copyright of the protected image without referring to the original image. Hence, our scheme is able to meet the blindness requirement.

5. Conclusions

How to retrieve significant features from a protected image is an important issue for copyright protection mechanisms. Our scheme utilizes Sobel to retrieve the edge characteristic of the protected image in order to generate a verification map. Using this map, people then can publicly verify the copyright of a protected image without needing the original image. Moreover, this novel approach allows image owners to adjust the strength of watermarks through a threshold to enhance robustness. Since our scheme uses the one-way hash function to sign the verification map of the protected image, instead of the public cryptosystem, the time consumption in constructing the certificate can be reduced by 0.1% compared with Chen et al.'s scheme. Moreover, our scheme does not apply DWT or DCT transformation, so it requires less computation load in the signing procedure than conventional copyright protection schemes. Furthermore, simulation results show that our scheme possesses higher AAR's than other schemes. In other words, our scheme can resist various signal processing and geometric transformation attacks. In particular, it preserves the lossless requirement, making it suitable for medical and artistic images.

References

Armstrong, J.R., Gray, G.F., 2000. VHDL Design: Representation and Synthesis. Prentice Hall.

Barni, M., Bartolini, F., Piva, A., 2001. Improved wavelet-based watermarking through pixel-wise masking. IEEE Transactions on Image Processing 10 (5), 783–791.

Chang, C.C., Hsiao, J.Y., Yeh, J.C., 2002a. A color image copyright protection scheme based on visual cryptography and discrete cosine transform. Image Science Journal 50, 133–140.

Chang, C.C., Chuang, J.C., Chen, T.S., 2002b. Recognition of image authenticity using significant DCT coefficients quantization. Informatica 26 (4), 359–366.

Chang, C.C., Hwang, K.F., Hwang, M.S., 2002c. Robust authentication scheme for protecting copyrights of images and graphics. IEE Proceedings-Vision Image and Signal Processing 149 (1), 43–50.

Chang, C.C., Hsiao, J.Y., Chiang, C.L. 2002d. An image copyright protection scheme based on torus automorphism. In: Proceedings of the First International Symposium on Cyber Worlds, pp. 217–224.

Chang, C.C., Chuang, J.C., Lai, Y.P., 2004. Hiding data in multitone images for data communications. IEE Proceedings-Vision on Images and Signal Processing 151 (2), 137–145.

Chen, T.H., Horng, G., Lee, W.B., 2005. A publicly verifiable copyright-proving scheme resistant to malicious attacks. IEEE Transactions on Industrial Electronics 52 (1), 327–334.

Cox, I.J., Kilian, J., Leighton, F.T., Shamoon, T., 1997. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing 6 (12), 1673–1687.

DES encryption standard (DES). National Bureau of Standards (U.S.) 1997. Federal Information Processing Standards Publication 46. National Technical Information Service, Springfield, VA.

Hsu, C.T., Wu, J.L., 1998. Multiresolution watermarking for digital images. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing 45 (8), 1097–1101.

Hsu, C.T., Wu, J.L., 1999. Hidden digital watermarks in images. IEEE Transactions on Image Processing 8 (1), 58–68.

Kanopoulos, N., Yasanthavada, N., Baker, R., 1988. Design of an image edge detection filter using the sobel operator. IEEE Journal of Solid State Circuits 23 (2), 358–367.

Katzenbeisser, S., Petitcolas, F.A.P. 2000. Information hiding techniques for steganography and digital watermarking, Artech House, January.

Kazakova, N., Margala, M., Durdle, N.G. 2004. Sobel edge detection processor for a real-time volume rendering system. In: Proceedings of the 2004 International Symposium on Circuits and Systems, vol. 2. pp. II-913-16.

Kim, W.S., Hyung, O.H., Park, R.H., 1999. Wavelet based watermarking method for digital images using the human visual system. Electronics Letters 35 (6), 466–468.

Kundur, D., Hatzinakos, D., 1999. Digital watermarking for telltale tamper proofing and authentication. Proceedings of the IEEE 87 (7), 1167–1180.

Lin, C.Y., Chang, S.F., 2001. A robust image authentication method distinguishing JPEG compression from malicious manipulation. IEEE Transactions on Circuits and Systems of Video Technology 11 (2), 153–168.

Linde, Y., Buzo, A., Gray, R.M., 1980. An algorithm for vector quantizer design. IEEE Transactions on Communications 28 (1), 84–95.

Nikolaidis, N., Pitas, I., 2004. Benchmarking of watermarking algorithms. In: Pan, Jeng-Shyang, Huang, Hsiang-Cheh, Jain, Lakhmi C. (Eds.), Intelligent Watermarking Techniques. World Scientific, pp. 315–347, Chapter 11.

Qu, Y.D., Cui, C.S., Chen, S.B., Li, J.Q., 2005. A fast subpixel edge detection method using Sobel–Zernike moments operator. Image and Vision Computing 23 (1), 11–17.

Rivest, R., Shamir, A., Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21 (2), 120–126.

Sutherland, P., 1996. Applied Cryptography, Protocols, Algorithms, and Source Code in C Bruce Schneier, second ed. John Wiley & Sons Inc., USA, p. 15.