Digital Watermarking Scheme with Visual Cryptography

Ching-Sheng Hsu and Shu-Fen Tu

Abstract—**The aim of this paper is to propose a novel digital watermarking scheme using visual cryptography. A binary image, called watermark, is split into two shares via a 2-out-of-2 visual secret sharing scheme. Then, one of the shares is embedded into the host image, and the other is held by the owner. When proving the ownership, the owner has to extract the embedded share and recover the watermark with his/her own share. Based on the security property of visual cryptography, our scheme can make sure that the two shares cannot leak any information about the watermark. Unlike other researchers' method, our scheme needs not a trust third party to avoid the multiple claming problem. Besides, the experimental results show that our scheme can resist most of common attacks.**

Index Terms—**digital watermarking, modular arithmetic, visual cryptography**

I. Introduction

With the coming era of Internet, more and more data are transmitted and exchanged on the networked systems to enjoy the rapid speed and convenience. However, in the cyberspace, the availability of duplication methods encourages the violation of intellectual property rights of digital data, such as document, image, audio, and video. Therefore, the protection of rightful ownership of digital data has become an important issue in recent years. Nowadays, researchers have proposed many techniques to protect the intellectual property rights for digital images. Digital watermarking, a kind of such techniques, is a method that hides a meaningful signature, or the so-called digital watermark, in an host image for the purpose of copyright protection, integrity checking, and captioning. When the rightful ownership of the image needs to be identified, the hidden watermark can be extracted for the ownership verification.

Recently, Chang et al. [2] proposed a copyright protection scheme, which utilizes visual cryptography and discrete cosine transformation (DCT) to satisfy the requirement of security and robustness. Essentially, their model comprises the ownership share construction and the watermark revelation phases. During the ownership share construction phase, the DC coefficients of different DCT blocks are extracted from the host image to form a master share, then an ownership share obtained by combining the master share and the watermark is constructed as a key to reveal the watermark without resorting to the original image. Since their method does not actually embed the watermark into the image, the host image will not be altered. However, they did not utilize the specialty of visual cryptography; namely decoding secrete visually. Besides, a trusted third party (TTP) is necessary to get a digital time-stamping signature for the ownership share to avoid the multiple claims problem. There are some similar schemes proposed by other researchers. Those schemes do not embed the watermark into the host image hence need a TTP as well [1, 3, 4, 8, 9].

In this paper, we propose a wavelet-based digital watermarking scheme, which can bring the specialty of visual cryptography into full play. Moreover, our scheme really embed the watermark into the host image hence need not a TTP. The rest of this paper is organized as follows. In section 2, visual cryptography is introduced to readers who are not familiar with it. Then, our scheme is explained in every detail and particular in section 3. The experimental results are given in section 4 to show the robustness and feasibility of our scheme. Finally, some discussions and conclusions are given in section 5.

II. Visual Cryptography

In 1994, a new cryptographic paradigm, called visual cryptography or visual secret sharing (VSS), was firstly introduced by Naor and Shamir [6]. It can encode a black-and-white secret image into n shares, which are printed on transparencies separately and distributed to n separate participants. Those who belong to a qualified set can see the secret image by stacking up their transparencies together. For example, in a k-out-of-n VSS scheme, the secret is visible only when at least k or more shares are stacked together. Hence VSS scheme is suitable for group secret sharing without the help of a computer. A VSS scheme is constructed for an access structure, $(\Gamma_{Qual}, \Gamma_{Forb})$, which specifies how the secret is shared among the n participants. Γ_{Qual} denotes the family of qualified sets, and Γ_{Forb} denotes the family of forbidden sets. Participants belonging to a qualified set can see the secret through stacking their transparencies together, and those belonging to a forbidden set cannot perceive any information from the stacked image. Take a 2-out-of-2 VSS scheme for example. There are two participants $\{1, 2\}$, and $\Gamma_{Qual} = \{\{1, 2\}\}$ and $\Gamma_{Forb} = \{\{1\}, \{2\}\}$.

Table 1 is an illustration of a 2-out-of-2 VSS scheme (Naor and Shamir 1995). There are six encryption rules for a white (resp. black) pixel. For each time of encoding a white (resp.

Manuscript received January 7, 2008.

Ching-Sheng Hsu is with the Department of Information Management, Ming-Chuan University, TAIWAN (phone: +886-3-350-7001 ext. 3741; fax: +886-3-359-3875; e-mail: cshsu@ mcu.edu.tw).

Shu-Fen Tu was with Department of Information Management, Chinese Culture University, TAIWAN. (e-mail: dsf3@faculty.pccu.edu.tw).

black) pixel, we randomly choose one of the encryption rules and split the pixel into two shares according to the selected rule. To decode the secret, we just stack the two shares to see the secret on the stacked result. Generally speaking, the encryption rules must satisfy the contrast and security condition. The contrast condition means that there must be a contrast between the stacked result of a white pixel and that of a black pixel if the shares come from a qualified set, while the security condition means that there must be no difference between the stacked result of a white pixel and that of a black pixel if the shares come from a forbidden set [5].

TABLE 1: AN ILLUSTRATION OF A 2-OUT-OF-2 VSS SCHEME

Secret Pixels	Encryption Rules		Stacked Results
	Share 1	Share 2	
□	■□ / □■	■□ / □■	■■
	■□ / □■	□■ / ■□	□□
	■□ / □■	■□ / □■	■□ / □■
	□■ / ■□	□■ / ■□	□■ / ■□
	■□ / □■	□■ / ■□	■□ / □■
	□■ / ■□	■□ / □■	□■ / ■□
■	■□ / □■	■□ / □■	■■
	■□ / □■	□■ / ■□	■■
	□■ / ■□	■□ / □■	■■
	□■ / ■□	□■ / ■□	■■
	■□ / □■	■□ / □■	■■
	□■ / ■□	■□ / □■	■■

III. THE PROPOSED SCHEME

The proposed scheme composes of two phases: the watermark embedding and watermark extraction. During the watermark embedding phase, a watermark is split into two shares by means of visual cryptography. Then, one of the two shares is embedded into the frequency domain of the host image, and the other is distributed to the owner. To prove the ownership, the owner has to address his/her share, extract the other share from the image and then combine these two shares to reveal the watermark. Based on the security condition of visual cryptography, we can make sure that the two shares cannot leak any information about the watermark.

A. Watermark embedding

Suppose that the host image H is a 512 × 512 gray-level image and that the watermark W is a 128 × 128 binary image. At first, a 2-level Haar wavelet transform is performed on H. Suppose that H' denotes H in frequency domain. Starting at an arbitrary point of H', we retrieve a rectangle T of size 256 × 256 to embed W and divide T into non-overlapping blocks of size 4 × 4. For each time of embedding a pixel of W, we split it into two shares using a 2-out-of-2 VSS scheme (see Table 1), where one is called the master share, and the other is called the ownership share. Then, the four wavelet coefficients of a block of T are modified according to the master share. Suppose that p (resp. c) denotes a pixel of share 1 (resp. a block of T). If p is black, c is modified into c' so that c' **mod** $R = (3/4) \times R$; otherwise, c is modified into c' so that c' **mod** $R = (1/4) \times R$, where R is a predefined modulus. The above procedure is illustrated by figure 1. Suppose that a white pixel of W is split into two shares as shown in figure 1. Since the coefficient 100 and 8 correspond to black pixel of the master share, they are modified to 98 and 13. The other two coefficients, -50 and 62, are modified to -38 and 55 since they correspond to white pixel of the master share.

In sum, the watermark is split into master share and ownership share. The master share is embedded into the host image, and the ownership share is distributed to the owner. After all pixels of W are processed, we can get the watermarked image. The following is the algorithm of watermark embedding.

Algorithm Embedding(c, R)

$r = |c| \bmod R$

$$\Delta(c) = c - \frac{c}{|c|} \cdot r$$

if $w = 1$ **then**

$d = (R - 1) \times (3/4)$

else

$d = (R - 1)/4$

$$c' = \Delta(c) + \frac{c}{|c|} \cdot d$$

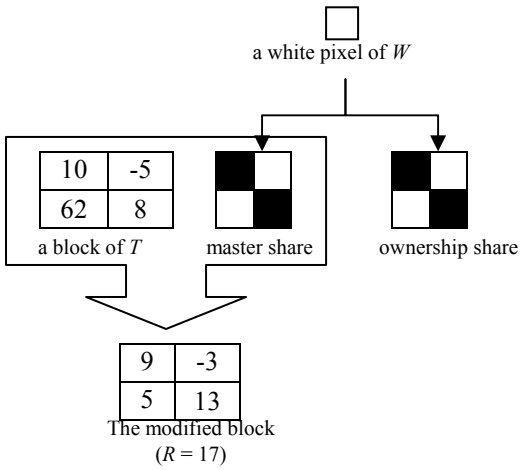


Fig. 1: An example of watermark embedding.

B. Watermark extraction

When the owner would like to prove the ownership, he/she has to extract the embedded master share to reveal the watermark with his/her share. Similarly, the first step is to perform a 2-level wavelet transform on the watermarked image and retrieve the rectangle T' of the same size and located at the same position. To extract the master share, we divide T' into non-overlapping blocks of size 4 × 4. Whenever a block is read in, it is transformed into a binary block according to the coefficients inside. If the coefficient c' modulo R is greater than a half of R, it represents black; otherwise, it represents white. By doing so, we can transform

T into a binary share, *i.e.* the master share. Stacking it with the ownership share, we can see the watermark on the stacked result. By stacking, we mean that perform the logic OR operation the two shares. Note that R must be the same as we used in the watermark embedding phase.

The complete algorithm of watermark extraction is shown below.

Algorithm Extracting(c', R)
  $r' = |c'| \bmod R$
  if $r' \geq (R-1)/2$ **then**
    $p' = 1$
  else
    $p' = 0$

IV. Experimental Results

Figure 2 is the watermark, which is embedded to Fig. 3(a), and Fig. 3(b) is the watermarked image. The watermark is split into the master share (Fig. 4(a)) and the ownership share (Fig. 4(b)), and the stacked result of the two shares is Fig. 4(c). In the experiment, we use PSNR (Peak Signal to Noise Ratios) to measure the quality of the watermarked image. The PSNR is computed as follows.

$$PSNR = 20 \log_{10}(255/MSE) \quad (1)$$

where

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (p_{i,j} - p'_{i,j})^2 \quad (2)$$

In Eq.(2), $p_{i,j}$ is the pixel of the host image, and $p'_{i,j}$ is that of the watermarked image. The larger the PSNR is, the more similar the watermarked image is to the host image. Generally speaking, human eyes cannot perceive the difference if PSNR is greater than 30. The PSNR of the watermarked image is 41.69, which means that human eyes almost cannot perceive the difference between it and the original image.

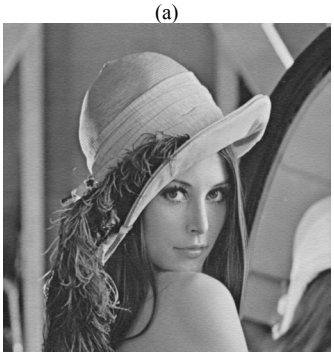
We simulate JPEG attack of various quality factors using Adobe Photoshop version 7. The extracted watermark is measured by the measurement NC (normalized correlation) as shown in Eq.(3).

$$NC = \frac{\sum_i \sum_j w_{i,j} w'_{i,j}}{\sum_i \sum_j w_{i,j}^2} \times \frac{\sum_i \sum_j \left(1 - w_{i,j}\right)\left(1 - w'_{i,j}\right)}{\sum_i \sum_j \left(1 - w_{i,j}\right)^2} \quad (3)$$

where $w_{i,j}$ is the pixel of the original watermark, and $w'_{i,j}$ is that of the extracted watermark. If NC is close to 1, the extracted watermark is similar to the original watermark. The extracted watermarks corresponding to different quality factors are shown in Fig. 5, and the numerical data, namely the PSNR of the watermarked image under attack and the NC of the extracted watermark, are shown in Table 2. The results show that our scheme is highly robust against the JPEG attack even the quality factor is low. Fig. 6 is the line chart of NC values corresponding to different JPEG quality factors. Observing Fig. 6, we can see that the quality of the extracted watermark does not decline sharply with the decreasing of the quality factors. We list the numerical data of other attacks in Table 1 as well. In sum, Table 1 shows that our scheme can resist most common attacks.

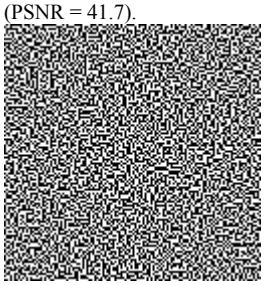
Fig 2: The binary watermark (64 × 64 pixels).

(a)

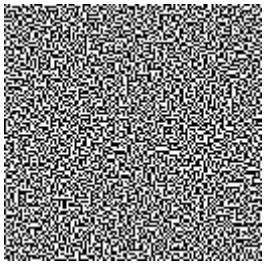


(b)

Fig. 3: (a) The original image (512 × 512 pixels); (b) The watermarked image (PSNR = 41.7).



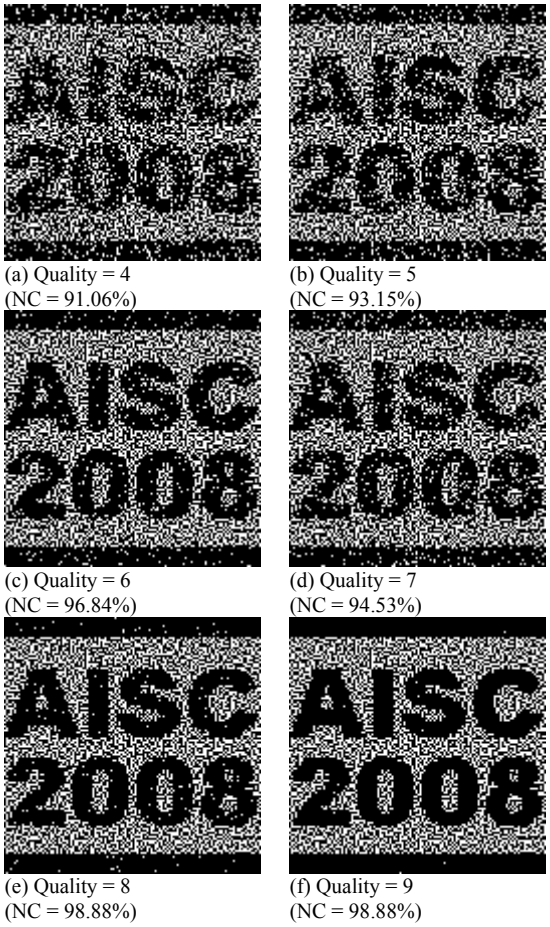
(a) Master share



(b) Ownership share

(c) Stacked result

Fig. 4: The corresponding shares (128 × 128 pixels) and stacked result of the watermark.



(a) Quality = 4 (NC = 91.06%)
(b) Quality = 5 (NC = 93.15%)
(c) Quality = 6 (NC = 96.84%)
(d) Quality = 7 (NC = 94.53%)
(e) Quality = 8 (NC = 98.88%)
(f) Quality = 9 (NC = 98.88%)

Fig. 5: Stacking results of the JPEG lossy compression attacks with various quality factors.

TABLE 2: EXPERIMENTAL RESULTS UNDER VARIOUS ATTACKS.

Attacks	PSNR (dB)	NC (%)
JPEG (quality = 1)	33.28	76.37
JPEG (quality = 2)	34.78	79.01
JPEG (quality = 3)	36.90	87.28
JPEG (quality = 4)	37.85	91.06
JPEG (quality = 5)	38.92	93.15
JPEG (quality = 6)	40.47	96.84
JPEG (quality = 7)	39.54	94.53
JPEG (quality = 8)	41.53	98.88
JPEG (quality = 9)	43.28	99.88
JPEG (quality = 10)	45.46	100.0
Lighting (+40)	16.09	99.90
Darkening (–40)	16.10	99.87
Blurring	36.60	80.30
Sharpening	36.66	82.03
Noise (5%)	30.21	80.55
Ripple	29.10	82.13

Note: (1) The PSNR values are computed from the watermarked image and the attacked images. (2) The NC values are measured between the stacking results with and without attacks.

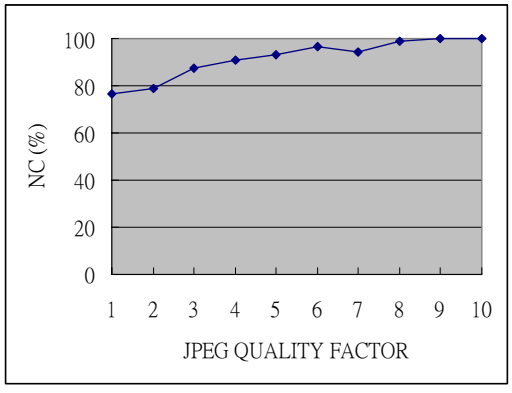


Fig 6: The watermark detection performance under JPEG lossy compression attacks.

ACKNOWLEDGMENT

This work was supported in part by a grant from the National Science Council of the Republic of China under the project NSC 96-2221-E-130-018.

REFERENCES

[1] C. C. Chang, K. F. Hwang, and Y. Lin, "A proof of copyright ownership using moment-preserving," *Proceedings of The 24th Annual International Computer Software and Application Conference* (COMPSAC 2000), Taipei, Taiwan, 25-28 October 2000, pp. 198-203.

[2] C. C. Chang, J. Y. Hsiao, and J. C. Yeh, "A colour image copyright protection scheme based on visual cryptography and discrete cosine transform," *Imaging Science Journal*, vol. 50, no. 3, 2002, pp. 133-140.

[3] C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods", *Optical Engineering*, vol. 44, no. 7, 2005, 077003.

[4] C. S. Hsu and Y. C. Hou, "An image size unconstrained ownership identification scheme for gray-level and color ownership statements based on sampling methods," *Journal of Systems and Software*, vol. 79, no. 8, 2006, pp. 11301140.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol. 129, no. 2, 1996, pp. 86-106.

[6] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology-EUROCRYPT '94*, LNCS 950, Springer-Verlag, 1995, pp. 1-12.

[7] R. J. Hwang, "A digital image copyright protection scheme based on visual cryptography," *Tamkang Journal of Science and Engineering*, vol. 3, no. 2, 2000, pp. 97-106.

[8] S. F. Tu and C. S. Hsu, "A BTC-based watermarking scheme for digital images," *Information & Security: An International Journal*, vol. 15, no. 2, 2004, pp. 214-226.

[9] S. F. Tu and C. S. Hsu, "A digital rights management approach for gray-level images," *Pattern Recognition and Image Analysis, Lecture Notes in Computer Science (LNCS)*, vol. 3687, 2005, pp. 3947.