Proceedings of the 2010 International Conference on Wavelet Analysis and Pattern Recognition, Qingdao, 11-14 July 2010

A NEW ROBUST COPYRIGHT PROTECTION SCHEME FOR DIGITAL IMAGE BASED ON VISUAL CRYPTOGRAPHY

YI-BO XING, JUN-HUI HE

School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China
E-MAIL: yibo.xing@mail.scut.edu.cn, hejh@scut.edu.cn (correspondence author)

Abstract

In this paper, a new digital image copyright protection scheme based on visual cryptography is proposed. Based on a more detailed feature classification in the discrete wavelet transform domain, an expanded codebook is used to improve the security of the current related schemes. Moreover, there is no need to modify the original image to be protected, which providing an obvious advantage when the image itself does not give permission for alteration. Experimental results show that the proposed scheme is robust against many common image processing attacks, such as JPEG compression, noise addition, cropping, rotation, scaling.

Keywords:

Discrete wavelet transform; visual cryptography; copyright protection; digital watermarking; robustness

1. Introduction

With the extensive use of digital media, including images, videos and sound clips, which could be easily copied or changed, how to protect the copyright of them has become an important issue. Robust digital watermarking techniques may be used for image copyright protection by embedding a specialized watermark into an image, which will be extracted to verify its copyright. A successful watermarking-based image copyright protection scheme usually requires not to make a perceptible change in the image to be protected, and should be able to withstand many common image processing attacks without leading to ambiguity in verification.

In general, there exist two major kinds of watermarking schemes: spatial domain watermarking and frequency domain watermarking. In order to embed a watermark, the spatial domain watermarking technique modifies the pixel values of an image, for instance, replacing the least significant bits (LSBs) of the pixels chosen in a specific order with watermark bits. In the frequency watermarking scheme, an image is first decomposed into frequency domain with discrete Fourier transform (DFT), discrete cosine transform (DCT) or discrete wavelet transform (DWT), etc. Then the frequency coefficients are used for watermark-embedding. Frequency domain based methods have been demonstrated by many researches to have better robustness.

Naor and Shamir [1] first introduced the technique of visual cryptography in 1994. In a (k, n) threshold scheme, the secret image is divided into n shadow images, and any k $(k \leq n)$ shadow images of them can be used to restore the original image by stacking together. A $(2, 2)$ scheme as an example is shown in Figure 1(a)-1(c). Visual cryptography has been utilized in image watermarking for copyright protection. Hwang [2] and Tai [3] both proposed their watermarking schemes, in which the watermark is revealed by stacking image shares together and is verified by human visual system (HVS) directly. However, the two spatial domain based schemes need to modify the original image and suffer from their weakness of withstanding image attacks.

Recently, a DCT-based watermarking technique is proposed by Huang [4], but the robustness of the scheme was not so satisfactory. By combining the visual secret sharing scheme with Torus-automorphism [6], Chang [5] proposed an image intellectual property protection scheme for gray-level images. In Chang's scheme, the Torus-automorphism technique was used to generate a secret image as a feature and to retrieve the potential public image from a suspect image. However, as Heieh and Huang mentioned in [7], Chang's scheme may be vulnerable to JPEG compression. With the use of DWT, Heieh's scheme is robust against JPEG compression and does not modify the original image so hardly can it cause any loss of the image detail.

In [8], Lou presented a copyright protection scheme, which will be denoted by the LTL scheme (named after the authors Der-Chyuan Lou, Hao-Kuan Tso and Jiang-Lung

978-1-4244-6529-3/10/$26.00 ©2010 IEEE

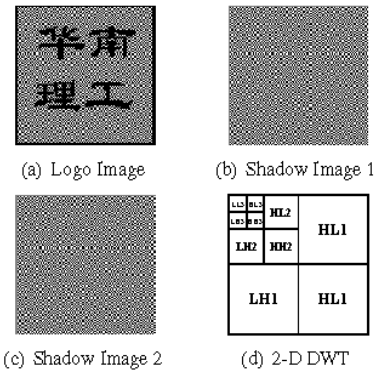


Figure 1. In a $(2, 2)$ visual cryptography scheme, the logo image (a) can be recovered by stacking two shadow images (b) and (c) together. (d) illustrates a three level 2-D discrete wavelet transform.

Liu) in this paper. In the LTL scheme, an image is decomposed by 2-D three-level DWT (as illustrated in Figure 1(d)). By comparing the frequency coefficients of the low sub-band and those of the middle sub-band, a unique feature of the image is generated. A well-designed codebook together with a secret key are then applied to generate a secret image share based on the watermark bits. In order to verify the copyright of a suspect image, a public image share is first generated with the use of the same codebook and secret key, then the watermark will be extracted by applying XOR between the public share and the secret share.

Although Chen [9] demonstrated that the LTL scheme has a major defect of ambiguity, making someone can maliciously claim the copyright of almost any image, the LTL scheme showed high robustness against many common attacks. Park [10] proposed a scheme (referred as the PYY scheme, which is named after the authors Geum-Dal Park, Eun-Jun Yoon and Kee-Young Yoo) trying to fix the flaw. However, in the codebook used in the PYY scheme (see Table 2),public blocks corresponding to watermark bit 0 and 1 differ from each other, which make Park's scheme require both the suspected image and the original watermark to extract the watermark used for verification. Moreover, by analyzing the codebook used in the PYY scheme, someone may also maliciously claim the copyright of an image, which will be analyzed in detail later in Section 2.

This paper presents a new image copyright protection method. Compared with the LTL scheme, a more detailed feature classification is used in our proposed approach. With an expanded codebook based on visual cryptography, a secret image and the corresponding public image are generated according to the watermark bits and a random sequence controlled by a secret key. The secret image should be registered to CA. The watermark will be recovered by performing XOR operation between the secret image and the public image during verification process.

Table 1. The codebook used in LTL's scheme

■=0 □=1

Feature Value	Computing mod (sety, 4)	Watermark bits □		XOR	Watermark bits ■		XOR
		Public Block	Secret Block		Public Block	Secret Block	
$F(i,j)=0$	0	■□	□■	□□	■□	■□	■■
	1	□■	■□	□□	□■	□■	■■
	2	■■	□■	□■	■■	■■	■■
	3	□□	■□	□■	□□	□□	■■
$F(i,j)=1$	0	□■	■□	□□	□■	□■	■■
	1	■■	□■	□■	■■	■■	■■
	2	□□	■□	□■	□□	□□	■■
	3	■□	□■	□□	■□	■□	■■

The rest of this paper is organized as follows. In Section 2, we first briefly review the LTL scheme and the PYY scheme. The security analysis of them is then given. Section 3 describes our proposed scheme in detail. Experimental results and analysis are given in section 4. We conclude our work in the last section.

2. Related Work

2.1. Review of the LTL scheme

The LTL scheme consists of mainly two phases: the secret image generation and watermark extraction. The procedure of the secret image generation is described as follows.
Input: An image I to be protected, a watermark W, a secret key K, a codebook C given in Table 1.
Output: A secret image S.
Step 1: Decompose image I using three-level DWT, and then extract the coefficients of the low sub-band L (LL3) and those of the middle sub-band M (HL3, LH3 or HH3).
Step 2: Compute the new coefficient values using the following equation:

$$L_{new}(i,j) = L(i,j) + n \times (L(i,j) - M(i,j)) \qquad (1)$$

where n is a normally distributed random bit sequence controlled by the secret key K.
Step 3: The feature values of the image I are generated according to the equation (2).

$$F(i,j) = \begin{cases} 0, & \text{if } L_{new}(i,j) > L(i,j) \\ 1, & \text{if } L_{new}(i,j) \leq L(i,j) \end{cases} \qquad (2)$$

Step 4: The secret image is then generated by looking up the codebook C according to the feature values $F(i,j)$ and bits of watermark W.
Step 5: Register the secret image S to CA, keep the selected sub-bands and the secret key K secretly for watermark extraction.

The procedure of the watermark extraction is described as follows.

Input: A suspect image I', a secret image share S, a secret key K, a codebook C given in Table 1.
Output: An extracted watermark W'.
Step 1: Decompose the suspect image I' using three-level DWT, and then extract the coefficients of the low sub-band L' (LL3) and those of the middle sub-band M' (HL3, LH3 or HH3).
Step 2: Calculate the new coefficient values using the following equation:

$$L'_{new}(i,j) = L'(i,j) + n \times (L'(i,j) - M'(i,j)) \quad (3)$$

where n is the same bit sequence as used in the equation (1), which controlled by the secret key K.
Step 3: The feature values of the suspect image I' are generated as follows:

$$F'(i,j) = \begin{cases} 0, & \text{if } L'_{new}(i,j) > L'(i,j) \\ 1, & \text{if } L'_{new}(i,j) \leq L'(i,j) \end{cases} \quad (4)$$

Step 4: Generate the public image by looking up the codebook C shown in Table 1 according to $F'(i,j)$. Note that the pixels on a specific position of each F' value are the same despite the pixel values of the potential watermark may vary.
Step 5: Extract the expanded watermark W_{temp} by performing XOR operation as follows

$$W_{temp} = P \oplus S \quad (5)$$

Step 6: Reduce the size of the expanded watermark and obtain the final extracted watermark of the same size as the original watermark.

$$W'(i,j) = \begin{cases} 1, & \text{if } \sum_m^m \sum_n^{n+1} W_{temp}(m,n) \geq 1 \\ 0, & \text{if } \sum_m^m \sum_n^{n+1} W_{temp}(m,n) < 1 \end{cases} \quad (6)$$

Chen [9] observed that the magnitude relationships between the DWT coefficients of the low sub-band and those of the middle/high sub-band are almost fixed. In other words, the feature value F in the LTL scheme is basically monotonous since $L(i,j) \geq M(i,j)$ for most images. The feature value of the image to be protected is determined only by the secret key K. This implies that if someone intentionally uses the same secret key to generate a public image share, the copyright of other images could be illegally claimed since the same watermark will be extracted from almost any images. This hypothesis has been proved by the experimental results provided in [9], suggesting that the LTL scheme fails to meet the security requirements of a copyright protection scheme.

2.2. Review of the PYY scheme

In order to fix the flaw of the LTL scheme, the PYY scheme used the average of a cover image to calculate the feature value. As a result, during both the secret image generation phase and watermark extraction phase, the **Step 3** has been changed to :

Table 2. The codebook used in PYY's scheme

■=0 □=1

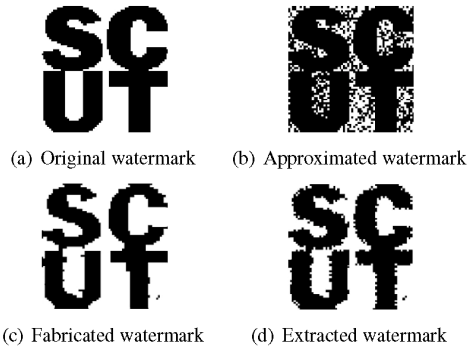
Feature Value	Computing mod ((x, y), 3)	Watermark bit is □		XOR	Watermark bit is ■		XOR
		Public Block	Secret Block		Public Block	Secret Block	
$F(x,y)=0$	0	□	■	□	■	■	■
	1	□	■	□	■	■	■
	2	■	□	□	■	■	■
$F(x,y)=1$	0	■	□	□	■	■	■
	1	□	■	□	■	■	■
	2	■	□	□	■	■	■

$$Aver = TP/NP$$
$$F(i,j) = \begin{cases} 0, & \text{if } L_{new}(i,j) > Aver \\ 1, & \text{if } L_{new}(i,j) \leq Aver \end{cases} \quad (7)$$

where that TP stands for the total coefficient value of L and NP stands for the number of coefficients in L. After the feature value is generated, a new code book (shown in Table 2) is introduced in **Step 5**.

As we can see that one of the major difference between the codebook used in LTL scheme and codebook used in PYY scheme is that, in LTL scheme, the public block column remains the same though the watermark bit changes, however, the public block column changes in PYY scheme. It means that during the watermark extraction phase in PYY scheme, the original watermark is still required to choose which the public block column should be used. We can see that if the watermark bit is black, the public block bits are all black, while half of the public block bits are black if the watermark bit is white. Also, **Step 6** of the watermark extraction phase in the LTL scheme will not be conducted since the codebook generates only one bit for each watermark bit naturally.

Suppose this scenario, a third one other than the owner wanted to maliciously claim the ownership of the protected image. Firstly by performing the XOR operation between the secret image share S (given as a input) and a all-black image share, a approximated watermark may be retrieved since nearly 75% bits of the public image share are black according to the codebook (Table 2). This percentage could be much more higher if the black-to-white ratio in the watermark is greater than 1. As shown in Figure 2, we firstly use the PYY scheme to embed the watermark "SCUT" (shown in Figure 2(a)) into the protected image "Lena", then at the watermark extraction phase, we pretend that we do not know the watermark and by performing the XOR operation between the secret image share S and a all-black image share, the approximated watermark is shown in Figure 2(b). Then we use a common erosion operation to clarify the watermark (shown in Figure 2(c)) and claim this fabricated watermark is the original watermark that we embedded earlier. Using this fabricated watermark as a parameter to perform



(a) Original watermark (b) Approximated watermark

(c) Fabricated watermark (d) Extracted watermark

Figure 2. Flaw of PYY scheme

the watermark extraction phase, the extracted watermark is still highly recognizable (shown in Figure 2(d)). Thus, the copyright of the protected image is maliciously claimed.

3. The Proposed scheme

In the proposed scheme, an expanded codebook is used to replace the codebook used in the LTL scheme. In order to avoid the security flaw in the LTL scheme, a different algorithm is also introduced to generate the feature values of the image to be protected. The procedure of the secret image generation is described as follows.

Input: A image I to be protected, a watermark W, a secret key K, a codebook C given in Table 3.

Output: A secret image S.

Step 1: Decompose the image I using three-level DWT, and then extract the coefficients of the low sub-band L (LL3).

Step 2: Compute the average coefficient value of L. Let TP denote the total coefficients value of L and NP denote the number of coefficients in L.

$$Aver = TP/NP \tag{8}$$

Step 3: Compute a matrix $\mathbf{V}$ to evaluate the weight of every coefficient by the following equation:

$$V(i,j) = \lfloor 2 \times L(i,j)/Aver \rfloor \tag{9}$$

where $\lfloor x \rfloor$ denote the nearest integer less than or equal to x.

Step 4: The feature values of the image I are generated as follows:

$$F(i,j) = \mod (V(i,j), 4) \tag{10}$$

Step 5: Use the secret key K to permute the feature value sequence, and generate the secret image S by looking up the codebook C (Table 3) according to the feature values $F(i,j)$ and the bits of the watermark W.

Step 6: Register the secret image S to CA, keep the selected sub-bands and the secret key K secretly for watermark extraction.

Table 3. The codebook used in our scheme

■=0 □=1

Feature Value	Computing mod (grey, 4)	Watermark bit is □ Public Block	Watermark bit is □ Secret Block	XOR	Watermark bit is ■ Public Block	Watermark bit is ■ Secret Block	XOR
F(x,y) = 0	0	■□	□■	□□	■□	■□	■■
	1	□■	■□	□□	□■	□■	■■
	2	■■	□□	□■	■■	■■	■■
	3	□□	■■	□■	□□	□□	■■
F(x,y) = 1	0	□■	■□	□□	□■	□■	■■
	1	■■	□□	□■	■■	■■	■■
	2	□□	■■	□■	□□	□□	■■
	3	■□	□■	□□	■□	■□	■■
F(x,y) = 2	0	□■	■□	□□	□■	□■	■■
	1	■□	□■	□□	■□	■□	■■
	2	□■	■■	□■	□■	□■	■■
	3	■□	□□	□■	■□	■□	■■
F(x,y) = 3	0	■□	□■	□□	■□	■□	■■
	1	□■	■■	□■	□■	□■	■■
	2	■□	□□	□■	■□	■□	■■
	3	□■	■□	□□	□■	□■	■■

The procedure of the watermark extraction is described in the following:

Input: A suspect image I', a secret share S, a secret key K, a codebook C.

Output: An extracted watermark W'.

Step 1 $\sim$ **Step 4** are the same as those in the secret image generation phase. Note that I in the secret image generation phase is replaced by I' while feature value of the image I' is generated as $F'(i,j)$.

Step 5: Use the secret key K to permute the feature sequence, and generate the public image P by looking up the codebook C (Table 3) according to the feature values $F'(i,j)$.

Step 6: Extract the expanded watermark W_{temp} by performing XOR operation as given in the equation (5).

Step 7: Reduce the size of the extracted watermark as described in the equation (6).

4. Experimental results

To test the robustness of the proposed scheme, the standard gray-level "Elaine" image and "Boat" image (512×512), which may be the protected image, and a watermark (64×64 (Figure 2(a)) were used in our experiments. We applied Photoshop CS2 to simulate different attacks. Accuracy ratio (AR) defined in the equation (11) was used to evaluate the similarity between the original watermark and the extracted watermark.

$$AR = CB/NB \tag{11}$$

where NB is the number of pixels in the original watermark and CB is the number of the correct pixels in the extracted watermark. And the peak signal to noise ratio (PSNR) defined in the equation (12) was used to evaluate the quality of the attacked image.

$$\begin{aligned} PSNR &= 10\log_{10} 255^2/MSE \text{ (dB)} \\ MSE &= \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (X_{i,j} - X'_{i,j})^2 \end{aligned} \tag{12}$$

where $X_{i,j}$ is the value of original image while $X'_{i,j}$ is the value of attacked image.

(a) Distorted boat image, PSNR=15.40

(b) Extracted watermark, AR=0.85

Figure 4. Liquefy attack

In order to test the robustness of the proposed scheme against JPEG compression , we compressed the protected image with different quality factor by Photoshop CS2 and then the watermark was extracted. As we can see from Figure 3, though a very low quality factor was chosen during JPEG compression, the watermark could be extracted successfully by using our proposed scheme.

When we added 20% salt and pepper noise into the protected image, as a result, the PSNR of the image reduced to 12.46. But the accuracy ratio of the extracted watermark reached 0.92 (see Figure 3).

We cropped $1/64$, $1/32$, $1/16$ and $1/8$ of the protected image, then extracted the watermark and calculated the ARs. The results were also shown in Figure 3. The letters in the watermark was still recognizable when we cropped up to 1/8 of the protected image.

In order to test the rotation attack, we rotated the protected image with several small angle varying from $1°$ to $6°$. The experimental results given in Figure 3 showed that the proposed scheme was effective when the rotation angle was less than $6°$. The challenge could be more severe when the rotation angle goes up.

Then we scaled the protected image down to a very tiny block. The most extreme situation we tested was that a 512×512 protected image was scaled down to 16×16 and then re-scaled back to 512×512. Experimental data demonstrated that the proposed scheme was very robust against scaling attack. Though the re-scaled image was almost unidentifiable, the extracted watermark was acceptable and the accuracy ratio was equal to 0.88.

Finally, We used the "Boat" image as the protected image, and the "Liquefy" tool in Photoshop to produce a distorted image (Figure 4(a)), which was hard to recognize with a PSNR of only 15.40. Then our proposed scheme was used to extract the watermark. As a result, the extracted watermark was recognizable with an accuracy ratio of 0.85 (Figure 4(b)).

5. Conclusions

Based on visual cryptography, a new digital image copyright protection scheme, which need not to modify the image to be protected, is presented in this paper. With the use of a new method of feature classification and an expanded codebook, the security of our scheme is better compared to the LTL and PYY schemes. Experimental results showed that the proposed scheme was robust against many common image processing attacks, especially the scaling operations.

Acknowledgments

This work is supported by the Fundamental Research Funds for the Central Universities under Grant No. 2009ZM0039.

References

[1] M. Naor and A. Shamir. Visual cryptography. In *Proc. of the Workshop on the Theory and Application of Cryptographic Techniques (Advances in Cryptology - EUROCRYPT'94)*, volume 950 of *LNCS*, pages 1–12, 1995.

[2] R. junn Hwang. A digital image copyright protection scheme based on visual cryptography. *Tambang Journal of science and Engineering*, 3:97–106, 2000.

[3] G.-C. Tai and L.-W. Chang. Visual cryptography for digital watermarking in still images. In *Proc. of the 5th Pacific Rim Conference on Multimedia - Advances in Multimedia Information Processing (PCM 2004*, volume 3332 of *LNCS*, pages 50–57, 2005.

[4] S. C. Huang and C. F. Wang. The image watermarking technique using visual secret sharing strategy. In *Proc. of the Eighth International Conference on Intelligent Systems Design and Applications (ISDA 2008)*, volume 2, pages 190 –195, 2008.

[5] C.-C. Chang and J.-C. Chuang. An image intellectual property protection scheme for gray-level images using visual secret sharing strategy. *Pattern Recognition Letters*, 23(8):931–941, 2002.

[6] G. Voyatzis and I. Pitas. Applications of toral automorphisms in image watermarking. In *Proc. of the International Conference on Image Processing (ICIP 1996)*, volume 2, pages 237–240, 1996.

[7] S.-L. Hsieh and B.-Y. Huang. A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformation. In *Proc. of International Computer Symposium (ICS 2004)*, pages 661–666, 2004.

[8] D.-C. Lou, H.-K. Tso, and J.-L. Liu. A copyright protection scheme for digital images using visual cryptography technique. *Computer Standards & Interfaces*, 29(1):125–131, 2007.

[9] T.-H. Chen, C.-C. Chang, C.-S. Wu, and D.-C. Lou. On the security of a copyright protection scheme based on visual cryptography. *Computer Standards & Interfaces*, 31(1):1–5, 2009.

[10] G.-D. Park, E.-J. Yoon, and K.-Y. Yoo. A new copyright protection scheme with visual cryptography. In *Proc. of the Second International Conference on Future Generation Communication and Networking Symposia (FGCNS 2008)*, pages 60–63, 2008.

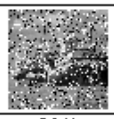
JPEG Compression				
Quality factor	60	40	20	10
Extracted watermark				
PSNR(dB)	35.8642	34.0551	33.7838	31.7998
AR	0.99902	0.9978	0.99586	0.99683
Noise addition				
Noise ratio	2%	5%	10%	20%
Extracted watermark				
PSNR(dB)	22.5128	18.4779	15.458	12.4617
AR	0.9843	0.9665	0.96973	0.92993
Cropping				
Cropping ratio	1/64	1/32	1/16	1/8
Extracted watermark				
PSNR(dB)	21.5789	19.4	16.7174	13.7035
AR	0.97021	0.94092	0.90869	0.81226
Rotation				
Rotation angle	1°	2°	4°	6°
Extracted watermark				
PSNR(dB)	21.7016	18.3389	15.0702	13.9775
AR	0.94653	0.9043	0.84375	0.80371
Scaling				
Re-scaled back from	128 × 128	64 × 64	32 × 32	16 × 16
Extracted watermark				
PSNR(dB)	30.6849	27.2569	20.921	18.8819
AR	0.99536	0.98218	0.93091	0.88623

Figure 3. Experimental results of common image processing attacks