A VC-Based Copyright Protection Scheme for Digital Images of Multi-Authorship

Shu-Fen Tu and Ching-Sheng Hsu

Abstract—**Digital watermarking is a technique for protecting intellectual property of digital information. However, when a work is created by multiple authors, digital watermarking may suffer some problems. When each author embeds his/her watermark, it is highly probable that the latter watermark will compromise the former one. Additionally, it is reasonable that no author can prove the ownership alone since all authors own the work jointly. In this paper, we will propose a copyright protection scheme, which is suitable for co-authored works and without drawbacks of digital watermarking. Our scheme integrates discrete cosine transform and visual cryptography to meet the requirement of robustness and security. The experimental results show that our scheme can resist some common attacks successfully.**

Index Terms—**Copyright Protection Scheme, Discrete Cosine Transform, Joint Ownership, Visual Cryptography.**

I. Introduction

Digital watermarking is a technique for protecting intellectual property of digital information. A signature, called a watermark, is embedded into a protected image. When piracy happens, the author can extract the watermark to prove his ownership. However, when a work is created by multiple authors, digital watermarking may suffer some problems. If each author embeds his/her watermark, it is highly probable that the latter watermark will compromise the former one. Some papers proposed different copyright protection schemes from watermarking, which is suitable for a co-authored work and without the drawback mentioned above [3]–[6], [8]. In those papers, anyone who participates in the creation can prove the ownership of the work by oneself. However, it is reasonable that none of the authors is allowed to prove the ownership alone since all authors own the work jointly. Therefore, when dealing with a co-authored work, we may need an appropriate copyright protection scheme to avoid such problems.

In this paper, we propose a copyright protection scheme for digital images of multi-authorship. Suppose there is a digital image created by multiple authors. At first, all authors have to pick a binary image to be an ownership statement. Then, a feature map, which represents the feature of the image, is extracted by means of discrete cosine transform (DCT). Applying the technique of visual cryptography (VC), each author is distributed a share, which is generated according to the feature map and the ownership statement. To prove the ownership of the image, all authors have to address their shares to reveal the ownership statement. Due to the security condition of visual cryptography, any malicious author, who wants to make the image of his/her own, cannot reveal the ownership statement with his/her share alone. To sum up, we integrate DCT and VC to meet the requirement of robustness and security in our scheme.

The rest of this paper is organized as follows. In section 2, we will introduce the concept visual cryptography for those readers, who are not familiar to it. Then, the proposed scheme is introduced in section 3. In section 4, we will demonstrate some experimental results to prove the robustness of our scheme. Finally, 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 [7]. 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, (Γ_{Qual}, Γ_{Forb}), which specifies how the secret is shared among the n participants. Suppose that there are two participants, *i.e.* $P = \{1, 2\}$. And suppose that the qualified set are all the subsets of P containing at least two participants and all remaining subsets of P are forbidden. Hence, the family of qualified sets is $\Gamma_{\text{Qual}} = \{\{1, 2\}\}$, and the family of forbidden sets is $\Gamma_{\text{Forb}} = \{\{1\}, \{2\}\}$. 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.

Generally, a VSS scheme (Γ_{Qual}, Γ_{Forb}, m)-VCS is constituted

Manuscript received March 22, 2007. This work was supported in part by a grant from National Science Council of the Republic of China under the project NSC 95-2221-E-034 -010.

Shu-Fen Tu is with the Department of Information Management, Chinese Culture University, Taipei, Taiwan (phone: +886-2-28610511 ext.35932; e-mail: dsf3@faculty.pccu.edu.tw).

Ching-Sheng Hsu is with Department of Information Management, Ming Chuan University, Taoyuan County, Taiwan. (e-mail: cshsu@mcu. edu.tw).

by two collections, C_0 and C_1, of $n \times m$ Boolean matrices. Let $X = \{i_1, i_2, \ldots, i_p\}$and M be an $n \times m$ Boolean matrix. Then we define a function OR(M, X) = $m_{i_1} \vee m_{i_2} \vee \ldots, \vee m_{i_p}$, where "$\vee$" denotes an logic OR operator and m_j denotes the jth row of matrix M. In addition, $w(V)$ represents the number of '1' within a vector V (*i.e.* the Hamming weight). If there exist the value $\alpha(m)$ and the set $\{(X, t_X)\}_{X \in \Gamma_{\text{Qual}}}$, a VSS scheme can be formerly defined as follows [1]:

Definition 1.1 (*contrast* property): If $X \in \Gamma_{\text{Qual}}$ and $V = \text{OR}(M, X)$, for any $M \in C_0$, the V satisfies $w(V) \le t_X - \alpha(m) \cdot m$; whereas, for any $M \in C_1$ it results that $w(V) \ge t_X$.

Definition 1.2 (*security* property): If $X \in \Gamma_{\text{Forb}}$, then the two collections of $p \times m$ matrices D_0 and D_1 obtained by restricting each $n \times m$ matrix in C_0 and C_1 ,respectively, to rows $i_1, i_2, \ldots, i_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The value $\alpha(m)$ is called relative difference, and the number $\alpha(m) \cdot m$ is referred to as the contrast of the image. The set $\{(X, t_X)\}_{X \in \Gamma_{\text{Qual}}}$ is called the set of thresholds, and t_X is the threshold associated to $X \in \Gamma_{\text{Qual}}$. The first property states that when participants belonging to a qualified set stack their transparencies, they can correctly recover the shared image. The second property implies that a forbidden set of participants cannot gain any information on the shared image.

To share a white (resp. black) pixel, we randomly choose one of the matrices in C_0 (resp. C_1) and distribute the m colors of the ith row of the selected matrix to the corresponding positions of share i. Generally, two collections of matrices C_0 and C_1 can be obtained from two $n \times m$ basis matrices M_0 and M_1, respectively. For example, the basis matrices for the 2-out-of-2 VSS scheme are as follows.

$$M_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix},\ M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{1}$$

Where '1' denotes black and '0' denotes white. The collections C_0 and C_1 are obtained by permuting the columns of the corresponding basis matrix (M_0 for C_0, and M_1 for C_1) in all possible ways; that is,

$$C_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\}, C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$

In practice, when we want to share a white (resp. black) pixel, we just randomly permute the columns of M_0 (resp. M_1) to get the desired matrix as if we randomly choose one of the matrices in C_0 (resp. C_1). There are many studies about how to design the basis matrices [1], [2], [7], [9], [10].

III. The Proposed Scheme

Our scheme is partitioned into two phases: the ownership registration phase and the ownership verification phase. The purpose of the first phase is to embed the ownership statement into the protected image virtually. Each author will get a share in the end. The aim of the second phase is to verify the ownership. Every author has to cooperate to reveal the ownership statement with their respective shares.

A. *Ownership Registration*

Assume that a gray-level image H is created by n authors, and a binary image W is an ownership statement. Let A denote the set of authors, where $A = \{a_1, a_2, \ldots, a_n\}$. Borrowed symbols from visual cryptography, we define Γ_{Qual} as the family of the qualified sets and Γ_{Forb} as the family of the forbidden sets. Each element of Γ_{Qual} represents the set of authors who can verify the ownership, and each one of Γ_{Forb} represents those who cannot verify the ownership. Since no author is allowed to verify the ownership alone, $\Gamma_{\text{Qual}} = \{A\}$ and $\Gamma_{\text{Forb}} = 2^A - \{\varnothing, A\}$ accordingly. In this phrase, the first job is to extract a feature map of H, and the second job is to generate n shares for each author according to the feature map. To extract the feature map of H, we divide H into blocks of 4×4 pixels and transform each block from spatial-domain to frequency-domain by DCT. Then, all DC coefficients of each DCT block are gathered to form the feature map.

After we get the feature map, the next step is to generate shares for each author by VC. Before we come to the main task, one more point of the rule of ownership verification must be clarified. Suppose that S is a subset of A. When verifying the ownership, we need to conform to the following rules:

1) If $S \in \Gamma_{\text{Qual}}$, each author of S can reveal the ownership statement via their respective shares with the feature map.
2) If $S \in \Gamma_{\text{Forb}}$, each author of S cannot reveal the ownership statement via their respective shares with or without the feature map.

To explain how to generate shares with feature map by VC, we add a virtual author f and define other symbols A', Γ_{Qual}', and Γ_{Forb}', where $A' = A \cup \{f\}$, $\Gamma_{\text{Qual}}' = \{X \cup \{f\} \mid X \in \Gamma_{\text{Qual}}\}$, and $\Gamma_{\text{Forb}}' = \Gamma_{\text{Forb}} \cup \{Y \cup \{f\} \mid Y \in \Gamma_{\text{Forb}}\}$. Note that the virtual author f can be seen as the one who holds the feature map. Then, we can find a VSS scheme for the access structure $\Gamma = (\Gamma_{\text{Qual}}', \Gamma_{\text{Forb}}')$. Suppose that M_0 and M_1 are the two $(n+1) \times m$ basis matrices for Γ, and let b denote the number of bit '1' of the first row of M_0 (or M_1). For each pixel p of W, we randomly retrieve m coefficients from the feature map, and let the b bigger ones become '1' and the others become '0'. Therefore, we can get an m-bit string s. According to s, we can split p as follows:

1) If p is white, rearrange the columns of M_0 randomly so that the first row is equal to s. Let M_0' denote the submatrix of the rearranged M_0 excluding the first row. Then, split p to n shares with M_0'.
2) If p is black, rearrange the columns of M_1 randomly so that the first row is equal to s. Let M_1' denote the submatrix of the rearranged M_1 excluding the first row. Then, split p to n shares with M_1'.

When each pixel of W is split, we can get n ownership shares O_i of W and distribute O_i to the author a_i, where $i = 1..n$.

For example, suppose H is created by two authors A and B. Taking the feature map of H into consideration, we can define the access structure as $\Gamma = (\{\{A, B, f\}\}, \{\{A\}, \{B\}, \{A, f\}, \{B, f\})$. As we have mentioned above, f can be seen as the one who holds the feature map. The VSS scheme for Γ is as follows:

$$M_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix},\ M_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \quad (2)$$

According to Eq. (2), for each pixel of W, we have to randomly retrieve four DC coefficients from the feature map, and let the bigger two values become bit ‘1’ and the others become bit ‘0’. Assume that the first pixel p of W is black and the sequence of the retrieved coefficients is (100, -20, 50, 200). Consequently, we can get a bit string $s = (1001)_2$. According to s, the columns of M_1 are permuted randomly so that the first row is equal to s. Assume that the permuted matrix is as follows:

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

Then, p is split to $(0011)_2$ and $(0101)_2$. After all pixels of W are split, we can get two shares for author A and B, respectively.

The following is the complete algorithm of ownership registration.

Algorithm 3.1 *Ownership Registration*

```
Input:  (1) A gray-level image $H$
        (2) An ownership statement $W$
        (3) A seed $K$ of the pseudo random number generator
        (4) The number of authors $n$
        (5) The $(n+1) \times m$ basis matrices $M_0$ and $M_1$
Output:     $n$ ownership shares $O_1, O_2, \ldots O_n$
Step 1: Divide $H$ into blocks of $4 \times 4$ pixels and compute the DC coefficients of each blocks.
Step 2: Let $b$ denote the number of bit ‘1’ of the first row of $M_0$.
Step 3: For each pixel $p$ of $W$, retrieve $m$ DC coefficients from $H$. Set the $b$ bigger values as bit ‘1’ and the others as bit ‘0’. Let $s$ denote the bit string.
Step 4: If $p$ is white (resp. black), randomly permute the column of $M_0$ (resp. $M_1$) so that the first row is equal to $s$.
Step 5: Distribute the bits of the second row to the last row of the permuted matrix to the $n$ ownership shares, respectively.
Step 6: Repeat step 4 to step 5 until each pixel of $W$ is split.
```

B. Ownership Verification

Once the protected image is distributed, the rights holder should be able to verify the copyright information to prove his/her ownership. If a gray-level image G is suspected to be a piracy copy, one can resolve the dispute about the ownership by revealing the ownership statement. Basically, the procedure of ownership verification is very similar to that of ownership registration. At first, we have to extract the feature map of G using the same method as shown in the procedure of ownership registration. Then, according to the number of authors, we can decide the appropriate VSS scheme, i.e. the matrix M_0 and M_1. According to M_0 and M_1 and the size of the ownership share, we can transform the feature map into a binary share. Simply speaking, each time we randomly retrieve m DC coefficients from the feature map, and let the b bigger ones become ‘1’ and the other become ‘0’, where m is the number of columns of the matrix and b is the number of bit ‘1’ of the first row of the matrix. Repeat the above procedure until we get a binary share, whose size is the same as the ownership share. Note that the seed of the pseudo random number generator here must be the same seed as we used in the phase of ownership registration. Finally, we can verify the ownership via performing the OR operation on all authors’ ownership shares and the binary share. If the ownership statement is revealed, we can prove that G is co-created by these authors.

The following is the complete algorithm of ownership verification.

Algorithm 3.2 *Ownership Verification*

```
Input:  (1) A gray-level image $G$
        (2) $n$ ownership shares $O_1, O_2, \ldots, O_n$
        (3) A seed $K$ of the pseudo random number generator
        (4) The $(n+1) \times m$ basis matrices $M_0$ and $M_1$
Output:     An ownership statement $W$
Step 1: Divide $H$ into blocks of $4 \times 4$ pixels and compute the DC coefficients of each blocks.
Step 2: Let $b$ denote the number of bit ‘1’ of the first row of $M_0$.
Step 3: For each $m$ pixels of an ownership share, randomly retrieve $m$ DC coefficients using the pseudo random number generator. Set the $b$ bigger values as bit ‘1’ and the others as bit ‘0’. Gather all the bits to form a binary share $S$.
Step 4: Perform the logic OR on $S$, $O_1, O_2, \ldots,$ and $O_n$ to reveal the ownership statement $W$.
```

IV. Experimental Results

In this section, we will demonstrate our scheme using the same example as shown in section 3.1. That is, there are two authors who co-create Fig. 1(a) of 512 × 512 pixels, and Fig. 1(b) is the binary ownership statement of 100 × 100 pixels. Eq. (2) is the 3 × 4 basis matrices to split the ownership statement into two shares, i.e. Fig. 1(c) and 1(d). Performing the logic OR on Fig. 1(c) and 1(d), we can see the ownership statement on Fig. 1(e). In this example, each pixel of the ownership statement will be expanded into four subpixels. Therefore, we can arrange the four subpixels as a 2 × 2 block. That is why the ratio of the width to height of Fig. 1(c) and 1(d) is 1 : 1.

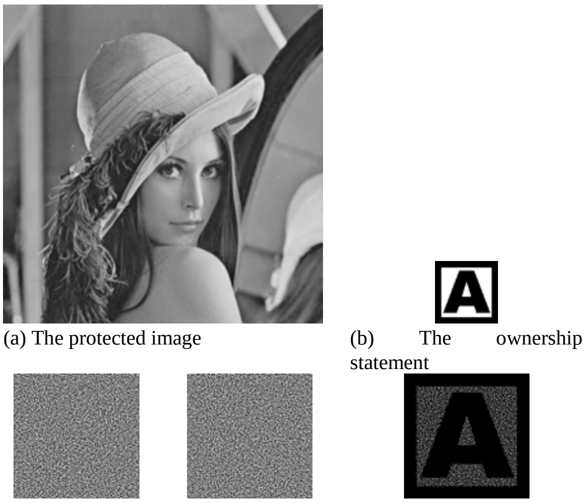
We simulate some common attacks on Fig. 1(a) using the software Adobe Photoshop version 7, and the parameters are listed in Table 1. We use the PSNR (peak signal-to-noise ratio) to represent the degree of attacks and list the PSNR value of each attack in Fig. 2. The following is the formula of PSNR:

$$PSNR = 10 \times \log \frac{255^2}{MSE} \quad (3)$$

and

$$MSE = \frac{1}{X \times Y} \sum_{i=1}^{X} \sum_{j=1}^{Y} \left(c_{i,j} - c'_{i,j} \right)^2 \quad (4)$$

where $c_{i,j}$ and $c'_{i,j}$ denote the original pixel and the changed pixel, respectively, and *X* and *Y* denote the height and width of the image, respectively. The lower the PSNR value is, the larger degree of attack is. Fig. 3(a) to 3(h) is the revealed ownership statements corresponding to Fig. 2(a) to 2(h). Observing Fig. 3, we can see that our scheme is robust enough against some common attacks.



(a) The protected image

(b) The ownership statement

(c) Share 1

(d) Share 2

(e) The revealed ownership statement

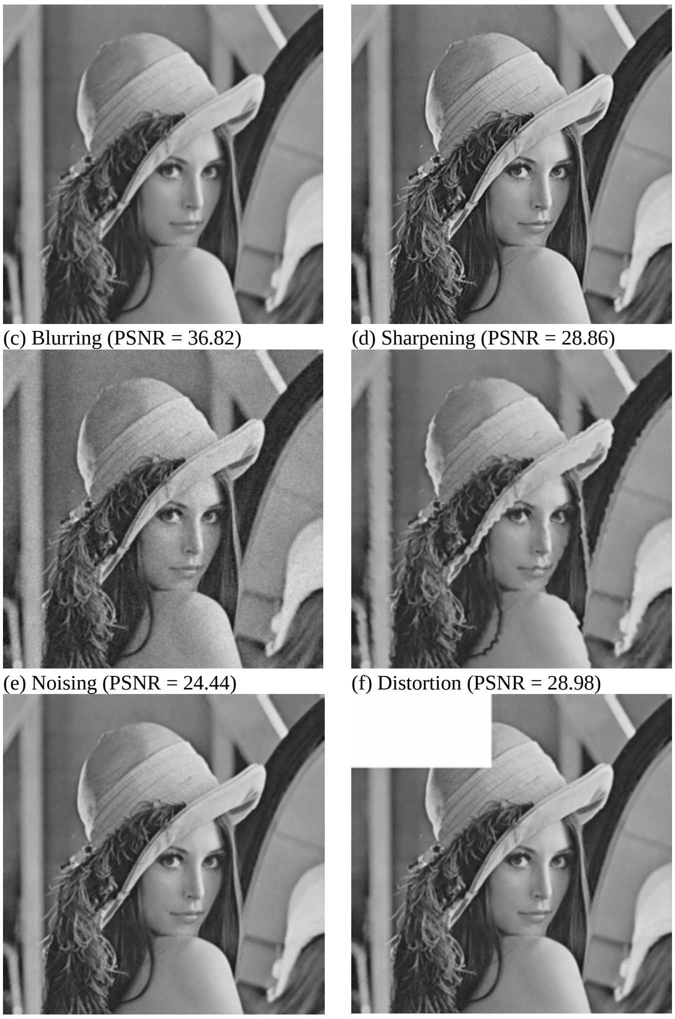
Fig. 1 The experimental results

TABLE I PARAMETERS OF ATTACKS

Attacks	Parameters (Adobe Photoshop version 7.0)
darkening	brightness: -30
lightening	brightness: +30
blurring	blur more
sharpening	sharpen more
noising	add noise: amount = 10%, distribution = uniform
geometric distortion	ripple: amount = 100%, size = large
cropping	erasing about 12% area of the image
JPEG	quality = 5, format option = baseline optimized

(a) Lightening (PSNR = 18.59)

(b) Darkening (PSNR = 18.59)



(c) Blurring (PSNR = 36.82)

(d) Sharpening (PSNR = 28.86)

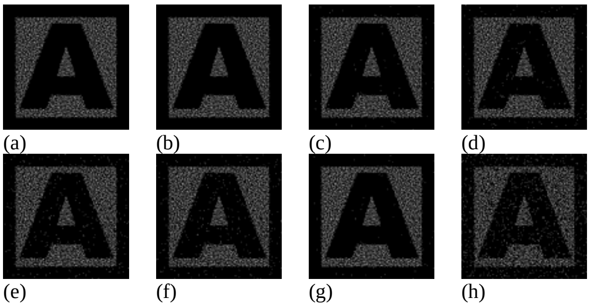
(e) Noising (PSNR = 24.44)

(f) Distortion (PSNR = 28.98)

(g) Jpeg (PSNR = 39.43)

(h) Cropping (PSNR = 15.58)

Fig. 2 Some common attacks on figure 1(a)



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 3 The revealed ownership statement

V. CONCLUSIONS

In this paper, we propose a copyright protection scheme for digital images of multi-authorship. It is reasonable that the proof of the ownership of a co-created image should be performed by all authors. In our scheme, we utilize the visual cryptographic method to split the ownership statement into *n* shares, each of which is held by an author privately. On the basis of the security condition of visual cryptography, we can prove that no author can gain any information about the ownership statement from his/her share. To prove the ownership, we just perform the logic OR operation on each author's ownership share to reveal the ownership statement. Hence, the operation of ownership verification is very simple. In addition, we utilize the discrete cosine transform to enhance the robustness of our scheme. Through the demonstration in section 4, we can see that our scheme is robust enough against some common attacks.

REFERENCES

[1] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Information and Computation*, 129(2), 1996, pp. 86–106.

[2] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," *Journal of Cryptology*, 12(4), 1999, pp. 261－289.

[3] 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, 2002, pp. 931－941.

[4] 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*, 50(3), 2002, pp. 133－140.

[5] 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.

[6] R. J. Hwang, "A digital image copyright protection scheme based on visual cryptography," *Tamkang Journal of Science and Engineering*, 3(2), 2000, pp. 97－106.

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

[8] S. F. Tu and C. S. Hsu, "A BTC-based watermarking scheme for digital images," *Information & Security: An International Journal*, 15(2), 2004, pp. 214－226.

[9] W. G. Tzeng and C. M. Hu, "A new approach for visual cryptography," *Designs, Codes and Cryptography*, 27, 2002, pp. 207－227.

[10] E. R. Verheul and H. C. A. van Tilborg, "Constructions and Properties of *k* out of *n* Visual Secret Sharing Schemes," *Designs, Codes and Cryptography*, 11, 1997, pp. 179－196.