A Joint Ownership Protection Scheme for Digital Images Based on Visual Cryptography

Shu-Fen Tu[1] and Ching-Sheng Hsu[2]
[1]Department of Information Management, Chinese Culture University, Taiwan
[2]Department of Information Management, Ming Chuan University, Taiwan

Abstract: *When an image is created by multiple authors, it is reasonable that no single author monopolize the ownership. The ownership should be shared among these authors, and the ownership should be proved by a group of authors. In this paper, we propose a joint ownership protection scheme for co-authored images. Some of the authors or all of the authors can verify ownership. This scheme integrates discrete cosine transforms and visual cryptography to meet robustness and security requirements. The experimental results show this scheme successfully resists some common attacks.*

Keywords: *Joint ownership protection, visual cryptography, discrete cosine transform.*

Received January 2, 2010; accepted October 24, 2010

1. Introduction

Digital watermarking is a technique for protecting digital intellectual property. The procedure embeds a signature, called a watermark, in a protected image. When piracy occurs, the author can extract the watermark to prove ownership. However, when multiple authors create a work, digital watermarking may experience problems. If each author embeds his or her watermark, it is highly probable that a latter watermark will compromise a former one. Some papers proposed different methods than watermarking, suitable for a co-authored work and without the above-mentioned drawback [4, 6, 8, 10, 13, 16]. Their proposed scheme does not embed a watermark in the image. Instead, the scheme extracts a master share from the original image and compares it with a signature to generate a so-called "ownership share," which is the key belonging to the author(s) to prove ownership of the image. When proving ownership, authors can address their ownership shares to identify ownership. The merit of such methods is that the watermarks do not affect the quality of the original image and they don't destroy other existing watermarks. Every author can select his or her own signature and generate his or her own ownership share. No matter how many authors join the creation, a single author can verify ownership. However, all authors own the work jointly. Therefore, when dealing with a co-authored work, it is an important to prevent a single author from verifying ownership.

Another issue about ownership verification for co-authored works is that authors' contributions to the work may not be equal. Therefore, it is possible that different authors have different rights to prove the ownership. That is, some authors may be able to prove the ownership, but some may not. Boatoa *et al*. [3] and Wang *et al*. [17] proposed a hierarchical watermark system to handle ownership for multiple authors. Among these authors, a person, called a "super user," has absolute power to verify ownership. Other authors, called normal users, must together verify ownership. Such hierarchical authority structure is common in organizations. Therefore, such schemes provide valuable solutions to the ownership verification of co-authored works. However, such schemes cannot cope with non-hierarchical structures. In a non-hierarchical structure, it is possible to specify that some groups of authors can prove ownership together and some groups cannot. The necessity of a non-hierarchical structure may arise as well when the contributions of authors are not equal.

The aim of this paper is to propose a joint ownership protection scheme to handle the two issues mentioned above. The proposed scheme can prevent any single author from proving ownership alone and require all authors to join the process of ownership verification. In addition, if all authors reach an agreement on the rule of ownership verification, which specifies qualified and unqualified authors for proving ownership, this scheme can authorize qualified authors to prove the ownership jointly and put constraints on unqualified authors' actions for proving ownership. This scheme does not embed a watermark in a host image. Instead, the scheme generates ownership shares for each author according to the rules of the ownership verification. The generation of ownership shares is tied to the host image feature to meet robustness requirements. Qualified authors can prove ownership jointly via addressing their own shares. By contrast, it is

impossible for unqualified authors to conspire to prove ownership. Visual Cryptography (VC) and Discrete Cosine Transforms (DCT) are the main techniques employed in this scheme. Therefore, section 2 briefly introduces VC and DCT for readers unfamiliar with the two techniques. Then, section 3 goes into details about the scheme. Section 4 shows experimental results of the scheme. Finally, section 5 presents a discussion and conclusions.

2. Related Works

2.1. Discrete Cosine Transform

Existing algorithms for ownership protection schemes usually work either in the spatial domain or in a transformed domain. Spatial-domain techniques directly modify the pixel values of an image while frequency-domain techniques modify the values of some transformed coefficients, which may be computed by a DCT, a Fourier transform, a wavelet transform, etc., the readers may refer to Lee and Lee's paper [9] to find literature related to each domain. Because frequency-domain techniques are much more robust against compression and geometrical transformations than spatial-domain techniques, many studies of digital watermarking are based on frequency transformation techniques. In frequency-domain watermarking schemes, DCT is widely used for its good energy compaction capability. In addition, invisibility constraints are easier to impose when working in the DCT domain [7, 12]. Therefore, the proposed scheme works in the frequency domain and adopts DCT as the frequency transformation technique.

Equation 1 is the formula to transform an image into the frequency domain where N and M are respectively the width and height of an image, $f(x, y)$ denotes the pixel located at (x, y) and $F(u, v)$ denotes the transformed coefficient located at (u, v). Equation 2 is the formula to transform an image inversely from the DCT-domain into the spatial domain.

$$F(u,v)=\frac{2}{\sqrt{NM}}C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2M}\right] \quad (1)$$

Where $C(u),C(v)=\begin{cases}\sqrt{1/2}, u=0\\ 1, \text{otherwise}\end{cases}$.

$$f(x,y)=\frac{2}{\sqrt{NM}}\sum_{u=0}^{N-1}\sum_{v=0}^{M-1}C(u)C(v)F(u,v)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2M}\right] \quad (2)$$

When an image is transformed into the DCT-domain, the coefficient located at (0, 0) is called a DC coefficient, which represents an important image feature. The DCT technique (i.e., the two formulas above) can be applied to a whole image or an image block.

2.2. Visual Cryptography

In 1994, a new cryptographic paradigm, called Visual Cryptography or Visual Secret Sharing (VSS), was first introduced by Naor and Shamir [11]. VC 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 (or called (k, n)-threshold VSS scheme), the secret is visible only when at least k or more shares are stacked together. Therefore, a 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 n participants. Suppose there are two participants, i.e., $P=\{1, 2\}$. Further, suppose the qualified set is all the subsets of P containing at least two participants and all remaining subsets of P are forbidden. The family of qualified sets is $\Gamma_{Qual}=\{\{1, 2\}\}$, and the family of forbidden sets is $\Gamma_{Forb}=\{\{1\}, \{2\}\}$. 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, two collections, C_0 and C_1, of $n \times m$ Boolean matrices constitute a VSS scheme $(\Gamma_{Qual}, \Gamma_{Forb}, m)$-VCS. Let $X=\{i_1, i_2, \ldots, i_p\}$ and M be an $n \times m$ Boolean matrix. Then define a function OR $(M, X)=m_{i1} \vee m_{i2} \vee \ldots, \vee m_{ip}$, where "$\vee$" denotes an logic OR operator and m_j denotes the jth row of matrix M. In addition, $w(V)$ represents the number '1' within a vector V (i.e., the Hamming weight). If the value $\alpha(m)$ and the set $\{(X, t_X)\}_{X \in \Gamma Qual}$ exist, a VSS scheme can be formerly defined as follows [1]:

- *Definition 1.1 (contrast property)*: If $X \in \Gamma_{Qual}$ and V=OR(M, X), for any $M \in C_0$, V satisfies $w(V) \le t_X - \alpha(m) \cdot m$; whereas, for any $M \in C_1$, $w(V) \ge t_X$.
- *Definition 1.2 (security property)*: If $X \in \Gamma_{Forb}$, 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 that they contain the same matrices with the same frequencies.

The value $\alpha(m)$ is called the relative difference, and the number $\alpha(m) \cdot m$ is referred to as the contrast of the image. The set $\{(X, t_X)\}_{X \in \Gamma Qual}$ is called the set of thresholds, and t_X is the threshold associated to $X \in \Gamma_{Qual}$. 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 regarding the shared image.

To share a white (resp. black) pixel, 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 (or called (2, 2)-threshold VSS scheme) are as follows:

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

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 sharing a white (resp. black) pixel, just randomly permute the columns of M_0 (resp. M_1) to get the desired matrix as if randomly choosing one of the matrices in C_0 (resp. C_1). There are many studies about how to design the basis matrices [1, 2, 11, 14, 15].

3. The Proposed Schemes

The proposed scheme consists of two phases: the ownership registration phase and the ownership verification phase. In the first phase, each author obtains his or her own ownership share, which is generated according to the ownership statement and the feature of the protected image. This phase employs two techniques: DCT and VC. The former extracts the protected image feature, and the latter generates the shares. In the second phase, qualified authors have to cooperate to reveal the ownership statement with their respective ownership shares.

For convenience of explanation, section 3.1 first gives the definition of symbols. Then, sections 3.2 and 3.3 discuss the details of the proposed scheme.

3.1. Symbol Definition

H: The protected image
W: The ownership statement
n: Number of authors to create H
a_0: A virtual author
a_i: Author i, where $i = 1..n$.
A: The set of all authors, i.e., $A = \{a_1, a_2, \ldots, a_n\}$.
S_i: Share distributed to author i, where $i = 1..n$.
γ_{Qual} : A family of qualified author sets
γ_{Forb} : A family of forbidden author sets
Γ_{Qual} : A family of qualified sets of a VSS scheme
Γ_{Forb} : A family of forbidden sets of a VSS scheme
M_0: A white basis matrix of a VSS scheme
M_1: A black basis matrix of a VSS scheme

3.2. The Ownership Registration Phase

Two possible cases relate to ownership verification for multiple authors. The first case is that all authors must be involved in the ownership verification. No one can prove the ownership alone. The other case is that qualified authors may not cover all authors. Therefore, the ownership verification may be done by a portion of the authors. To clarify, this study uses the term "all-involved scheme" to indicate the scheme for case 1 and the term "general scheme" to indicate the scheme for case 2. In fact, case 1 can be seen as a special case of case 2 since only one set belongs to γ_{Qual}, and other possible subsets of A belong to γ_{Forb}. That is, $\gamma_{Qual} = \{A\}$ and $\gamma_{Forb} = 2^A - \{\varnothing, A\}$. Whether case 1 or 2, all authors need to coordinate a binary image as W. With the help of visual cryptography, the scheme splits W into n shares of for each author according to H. Before turning to a closer examination of how to split W according to H, one more point of the rule of ownership verification must be clarified. Suppose Z is a subset of A. When verifying ownership, authors need to conform to the following rules:

1. If $Z \in \gamma_{Qual}$, each author of Z can reveal the ownership statement via their respective shares with H but cannot reveal the ownership statement without H.
2. If $Z \in \gamma_{Forb}$, each author of Z cannot reveal the ownership statement via their respective shares with or without H.

To obey the above conditions, the scheme creates a virtual author a_0, which is a necessary role involved in the process of ownership verification. For an access structure $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ of a visual secret sharing, let $\Gamma_{Qual} = \{X \cup \{a_0\} \mid X \in \gamma_{Qual}\}$, and $\Gamma_{Forb} = \gamma_{Forb} \cup \{Y \cup \{a_0\} \mid Y \in \gamma_{Forb}\} \cup \gamma_{Qual}$. Qualified authors must cooperate with a_0 to prove ownership. The generation of shares has to be tied in with H; therefore, the virtual author a_0 is the one who holds the feature map of H. To extract the feature map of H, H is divided into blocks of 4×4 pixels and each block is transformed from spatial-domain to frequency-domain by DCT. Then, all DC coefficients of each DCT block are gathered to form the feature map.

Returning to share generation, suppose M_0 and M_1 are the two $(n+1)\times m$ basis matrices for Γ. Let b denote the number of bit '1' of the first row of M_0 (or M_1). For each pixel p of W, the process randomly retrieves m coefficients from the feature map; let the b bigger ones become '1' and the others become '0'. Thus, the process can get an m-bit string s. According to s, p is split 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, the process yields n shares S_i of W and distributes Si to the author a_i, where i=1..n. Take an all-involved scheme as an example. Suppose H is created by two authors and all authors have to join the ownership verification together. Therefore, $\gamma_{Qual}=\{\{a_1,a_2\}\}$ and $\gamma_{Forb}=\{\{a_1\},\{a_2\}\}$. Taking the feature map of H into consideration, the scheme defines the access structure as $\Gamma=(\{\{a_0, a_1, a_2\}\}, \{\{a_1\}, \{a_2\}, \{a_0, a_1\}, \{a_0, a_2\})$. The VSS scheme for Γ is as follows:

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

According to equation 2, for each pixel of W, the process must 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, the process yields a bit string $s=(1001)_2$. According to s, the columns of M_1 are permuted randomly so the first row is equal to s. Assume 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, the scheme produces 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 of M × N pixels
2. An ownership statement W of X × Y pixels
3. A seed K of the pseudo random number generator
4. The number of authors n
5. The (n +1) × m basis matrices M_0 and M_1
Output: n ownership shares S_1, S_2, …S_n
Step 1: Divide H into blocks of 4 × 4 pixels and compute the DC coefficients of each block.
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 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.

3.3. The Ownership Verification Phase

Once the protected image is distributed, the rights holder should be able to verify the copyright information to prove his or her ownership. If a gray-level image G is suspected to be a pirated copy, the dispute about the ownership can be resolved by revealing the ownership statement. The procedure of ownership verification is very similar to that of ownership registration. First, 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, 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, transform the feature map into a binary share. Each time m DC coefficients are randomly retrieved from the feature map. The b bigger ones become '1' and the others 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 a binary share is obtained that has the same size as the ownership share. Note that the seed of the pseudo random number generator here must be the same seed used in the ownership registration phase. Finally, verify the ownership via performing the OR operation on all authors' ownership shares and the binary share. If the ownership statement is revealed, G is co-created by these authors. Following is the complete algorithm of ownership verification.

Algorithm 3.2 Ownership Verification
Input: 1. A gray-level image G
2. n ownership shares S_1, S_2, …, S_n
3. A seed K of the pseudo random number generator
4. The (n +1) × m basis matrices M_0 and M_1
Output: An ownership statement W
Step 1: Divide H into blocks of 4 × 4 pixels and compute the DC coefficients of each block.
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, S_1, S_2, …, and S_n to reveal the ownership statement W.

4. Experimental Results

This section demonstrates the all-involved and general scheme using Figure 1-a as the protected image and Figures 1-b and 1-c as the ownership statements for case 1 and case 2, respectively. The experiment simulates some common attacks on Figure 1-a using Adobe Photoshop version 7, and the parameters are listed in Table 1. The PSNR (peak signal-to-noise ratio) represents the degree of attacks and Figure 2

lists the PSNR value of each attack. The following is the formula of PSNR:

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

and

$$MSE = \frac{1}{M_1 \times M_2} \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} (c_{i,j} - c'_{i,j})^2 \quad (4)$$

Where $c_{i,j}$ and $c'_{i,j}$ denote the original pixel and the changed pixel, respectively, and $M_1$and M_2 denote the height and width of the image, respectively. The lower PSNR value is the larger degree of the attack. This study measures the robustness as follows:

$$NC = \frac{\sum_{i=1}^{N_1} \sum_{j=1}^{N_2} \overline{w(i,j) \oplus w'(i,j)}}{N_1 \times N_2} \times 100\% \quad (5)$$

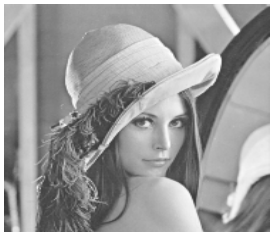
Where $w_{i,j}$ is the pixel of the original ownership statement, and $w'_{i,j}$ is the pixel of the revealed ownership statement. If NC is close to 1, the revealed ownership statement is similar to the original one.

a. The protected image (512 × 512 pixels).

b. The ownership statement for case 1 (100 × 100 pixels).

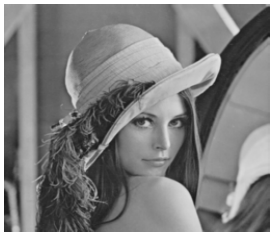
c. The ownership statement for case 2 (100 × 100 pixels).

Figure 1. The experimental images.



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).

Figure 2. Some common attacks on Figure 1-a.

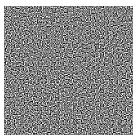
Table 1. Parameters of attacks.

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
Darkening	brightness: −30

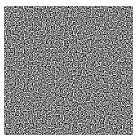
4.1. All-Involved Scheme

This subsection implements the example mentioned in section 3.2. That is, γ_{Qual}={{a_1, a_2}} and γ_{Forb}={{a_1}, {a_2}}. Equation 4 is the 3×4 basis matrices to split the ownership statement into two shares (i.e., Figures 3-a and 3-b). Performing the logic OR on Figures 3-a and 3-b and the binary share of Figure 1(a) reveals the ownership statement on Figure 3-c. In this example, each pixel of the ownership statement is expanded into four subpixels. The four subpixels are rearranged as a 2×2 block. This is why the ratio of the width to height of Figures 3-a and 3-b is 1: 1.

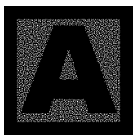
Figure 4 lists the ownership statements generated from the attacked images of Figure 2 and their corresponding NC values. Note that the NC values are computed between the revealed ownership statement and Figure 3-c rather than between the revealed ownership statement and Figure 1-b. Figure 4 shows that the all-involved scheme is robust enough against common attacks.



a. Share 1

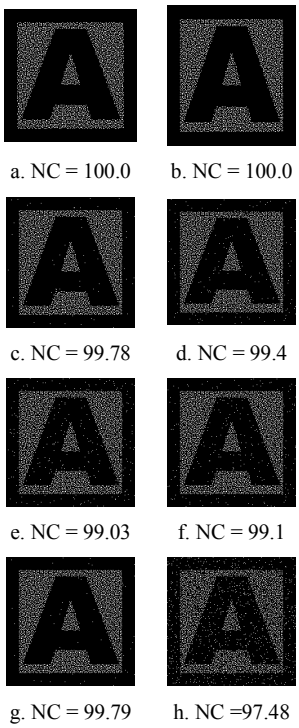


b. Share 2



c. The stacked result

Figure 3. The two shares and stacked result.



a. NC = 100.0 b. NC = 100.0

c. NC = 99.78 d. NC = 99.4

e. NC = 99.03 f. NC = 99.1

g. NC = 99.79 h. NC =97.48

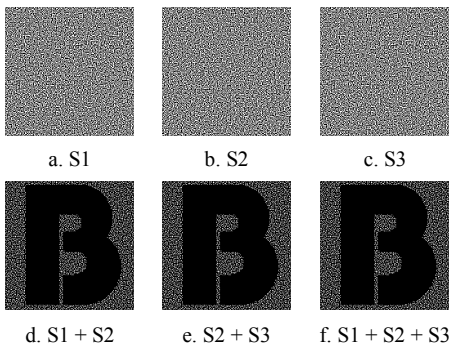
Figure 4. The revealed ownership statements.

4.2. General Scheme

Suppose there are three authors and that $\gamma_{Qual}=\{\{a_1, a_2\}, \{a_2, a_3\}, \{a_1, a_2, a_3\}\}$ and $\gamma_{Forb}=\{\{a_1\}, \{a_2\}, \{a_3\},\{a_1, a_3\}\}$. Authors 1 and 2, authors 2 and 3, or all authors together can prove ownership; however, authors 1 and 3, or any single author cannot prove ownership. The basis matrices for this scheme are as follows:

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

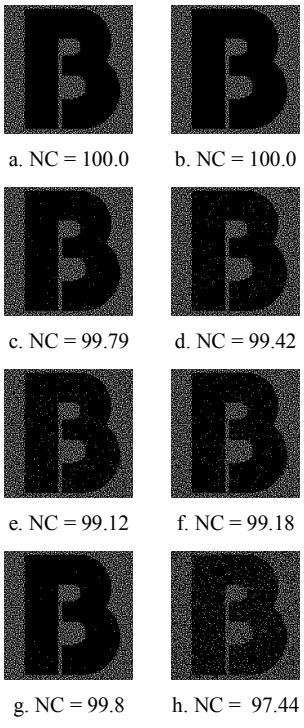
Figures 5-a to 5-c are the three authors' shares, and Figures 5-d to 5-f are the stacked results corresponding to each qualified set. Figures 6 to 8 are the revealed ownership statements corresponding to each qualified set and generated from those attacked images of Figure 2. Figures 6 to 8 and those NC values listed in the figures show that the revealed ownership statements are clear enough to prove ownership.



a. S1 b. S2 c. S3

d. S1 + S2 e. S2 + S3 f. S1 + S2 + S3

Figure 5. The three shares and stacked results.



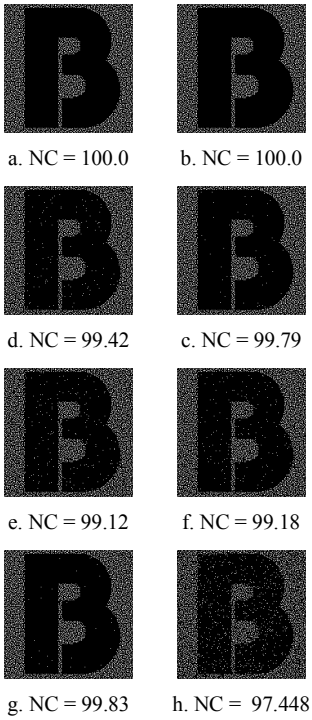
a. NC = 100.0 b. NC = 100.0

c. NC = 99.79 d. NC = 99.42

e. NC = 99.12 f. NC = 99.18

g. NC = 99.8 h. NC = 97.44

Figure 6. The revealed ownership statements of the qualified set $\{a_1, a_2\}$.



a. NC = 100.0 b. NC = 100.0

d. NC = 99.42 c. NC = 99.79

e. NC = 99.12 f. NC = 99.18

g. NC = 99.83 h. NC = 97.448

Figure 7. The revealed ownership statements of the qualified set $\{a_2, a_3\}$.

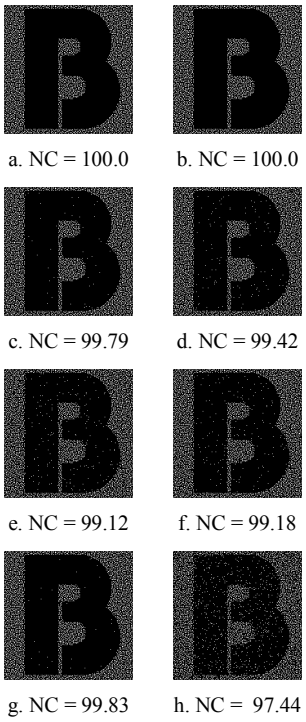


Figure 8. The revealed ownership statements of the qualified set $\{a_1, a_2, a_3\}$.

5. Discussions and Conclusions

Most existing digital watermarking schemes are not suitable for a digital image created by multiple authors. When a digital image is created by multi-authors, it is reasonable that all authors should involve in the proof of the ownership. To put it more precisely, no one can prove the ownership alone. Instead, every author should prove the ownership all together. Sometimes, the importance of each author is not equal. That is, some authors have major contributions to the creation, and others have minor contributions. Therefore, a digital watermarking scheme for digital images of co-authorships is necessary. Even more important is a digital watermarking scheme, which can assign different right of proof to each author according to the degree of contributions.

This paper proposes a copyright protection scheme for digital images with multi-authorship based on visual cryptography. If a digital image is created by n authors, we can utilize a suitable VSS scheme to split the ownership statement into n shares according to the feature of the protected image, and each of which is held by an author privately. On the basis of the security condition of visual cryptography, we can ensure that no author can gain any information about the ownership statement from his or her own share. To prove ownership, we perform the logic OR operation on each author's ownership share and the feature map of the protected image to reveal the ownership statement. Therefore, the operation of ownership verification is very simple.

Regarding to the robustness of the proposed scheme, the feature map of the proposed scheme is generated according to the DC coefficients of each DCT blocks of the protected image. In section 4, we simulate two cases: one is the all-involved scheme, and the other is the general scheme. As shown in the experimental results, we can see that our scheme is robust enough against some common attacks for the two cases. So far as we know, there are no researches related to a watermarking scheme for digital images of multi-authorship. Although Boatoa *et al.* [3] and Wang *et al.* [17] proposed a watermarking scheme for a co-authored digital image, their schemes cannot handle general cases. In their scheme, the right to prove the ownership is hierarchical. One of the authors has absolute power to prove the ownership. That is, he/she can prove the ownership alone. The other authors have to prove the ownership all together. Basically, a hierarchical scheme is a special case of a general scheme; therefore, our method can handle a hierarchical structure as well. In summary, we propose a watermarking scheme for digital images of multi-authorship. Our scheme can handle any cases of proof of ownership. Besides, the proposed scheme is robust enough against some common attacks.

Due to the nature of the traditional VC scheme, the size of the decoded image is unavoidably larger than the original image. In the future, we will introduce a probability-based model to solve this problem. That is, the size of the decoded image will be the same as that of the original image. Moreover, we will apply the proposed scheme to electronic voting.

Acknowledgements

This work was supported in part by a grant from the National Science Council of the Republic of China under the projects NSC 96-2221-E-034-016-MY2 and NSC 97-2221-E-130-019-.

References

[1] Ateniese G., Blundo C., De-Santis A., and Stinson D., "Visual Cryptography for General Access Structures," *Information and Computation*, vol. 129, no. 2, pp. 86-106, 1996.

[2] Blundo C., De-Santis A., and Stinson D., "On the Contrast in Visual Cryptography Schemes," *Journal of Cryptology*, vol. 12, no. 4, pp. 261-289, 1999.

[3] Boatoa G., Natalea F., Fontanarib C., and Melgani F., "Hierarchical Ownership and Deterministic Watermarking of Digital Images Via Polynomial Interpolation," *Signal Processing: Image Communication*, vol. 21, no. 7, pp. 573-585, 2006.

[4] Chang C. and Chuang J., "An Image Intellectual Property Protection Scheme for Gray-Level Images Using Visual Secret Sharing Strategy,"

Pattern Recognition Letters, vol. 23, no. 8, pp. 931-941, 2002.

[5] Chang C., Hsiao J., and Yeh J., "A Colour Image Copyright Protection Scheme Based on Visual Cryptography and Discrete Cosine Transform," *Imaging Science Journal*, vol. 50, no. 3, pp. 133-140, 2002.

[6] Chang C., Hwang K., and Lin Y., "A Proof of Copyright Ownership Using Moment-Preserving," *in Proceedings of 24th Annual International Computer Software and Application Conference*, Taiwan, pp. 198-203, 2000.

[7] Hernández J., Amado M., and Pérez-González F., "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a Structure," *IEEE Transactions on Image Processing*, vol. 9, no. 1, pp. 55-68, 2000.

[8] Hwang R., "Digital Image Copyright Protection Scheme Based On Visual Cryptography," *Tamkang Journal of Science and Engineering*, vol. 3, no. 2, pp. 97-106, 2000.

[9] Lee C. and Lee Y., "An Adaptive Digital Image Watermarking Technique for Copyright Protection," *IEEE Transactions Consumer Electronics*, vol. 45, no. 4, pp. 1005-1015, 1999.

[10] Lou D., Tso H., and Liu J., "A Copyright Protection Scheme for Digital Images Using Visual Cryptography Technique," *Computer Standards and Interfaces*, vol. 29, no. 1, pp. 125-131, 2007.

[11] Naor M. and Shamir A., "Visual Cryptography," *in Proceedings of Advances in Cryptology-EUROCRYPT, Lecture Notes in Computer Science*, Berlin, pp. 1-12, 1995.

[12] Tao B. and Dickinson B., "Adaptive Watermarking in the DCT Domain," *in Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, Germany, pp. 2985-2988, 1997.

[13] Tu S. and Hsu C., "A BTC-Based Watermarking Scheme for Digital Images," *Information and Security, An International Journal*, vol. 15, no. 2, pp. 216-228, 2004.

[14] Tzeng W. and Hu C., "A New Approach for Visual Cryptography," *Journal of Designs, Codes and Cryptography*, vol. 27, no. 3, pp. 207-227, 2002.

[15] Verheul E. and Van-Tilborg H., "Constructions and Properties of *k* out of *n* Visual Secret Sharing Schemes," *Journal of Designs, Codes and Cryptography*, vol. 11, no. 2, pp. 179-196, 1997.

[16] Wang M. and Chen W., "A Hybrid DWT-SVD Copyright Protection Scheme Based on K-Means Clustering and Visual Cryptography," *Computer Standards and Interfaces*, vol. 31, no. 4, pp. 757-762, 2009.

[17] Wang F., Yen K., Jain L., and Pan J., "Multiuser-Based Shadow Watermark Extraction System," *Journal of Information Sciences*, vol. 177, no. 12, pp. 2522-2525, 2007.

Shu-Fen Tu is an associate professor in Department of Information Management at Chinese Culture University in Taiwan. She received the BS degree in management information system from National Cheng-Chi University, Taiwan in 1996, the MS degree in information management from National Chi-Nan University, Taiwan in 1998, and the PhD degree from the Institute of Information Management, National Central University, Taiwan in 2005. From 1998 to 1999, she was a software engineer of the Syscom Group Co., Taiwan. From February 2005 to July 2005, she was an assistant professor of Department of Information Management, Chaoyang University of Technology, Taiwan. From 2005 to 2008, she was an assistant professor of Department of Information Management, Chinese Culture University. Her current research interests include steganography, secret sharing, and applications of computational intelligence.

Ching-Sheng Hsu got his BA degree from the Department of Information Management, National Cheng-Chi University, Taiwan, in 1994, MA degree from the Institute of Information Management, National Chi-Nan University, Taiwan, in 1998, and PhD degree from the Institute of Information Management, National Central University, Taiwan, in 2005. From 1998 to 1999, he was a software engineer at the Syscom Group Co, Taiwan, where his work focused on the Web-based stock trading systems. From 2000 to 2004, he was a part-time lecturer of the National Open University, Taiwan. From 2004 to 2011, he was an assistant professor of Department of Information Management, Ming Chuan University. Currently, he is an associate professor of Department of Information Management, Ming Chuan University. His current research interests include digital watermarking and information hiding, visual cryptography, optimization algorithms, and intelligent computer-assisted learning and testing systems.