Digital image copyright protection scheme based on visual cryptography and singular value decomposition

Ming-Shi Wang
Wei-Che Chen, MEMBER SPIE
National Cheng Kung University
Department of Engineering Science
Tainan 701, Taiwan
E-mail: mswang@mail.ncku.edu.tw

Abstract. A digital image copyright protection scheme based on visual cryptography (VC) and singular value decomposition (SVD) techniques is proposed. In the proposed scheme, a master share is first constructed by applying SVD to a host image. Then, the master share is used together with a secret image to construct an ownership share, according to a two-out-of-two VC scheme. The secret image for ownership identification can be revealed by stacking the master share, and the ownership share. The proposed scheme embeds the secret image without modifying the host image. In addition, the hidden secret image can be extracted without resorting to the original host image and the aid of computers. Experimental results show that the proposed scheme, compared with existing schemes, achieves stronger robustness against several common attacks.
[DOI: 10.1117/1.2746906]

Subject terms: copyright protection; digital watermarking; visual cryptography; singular value decomposition.

Paper 060782RR received Oct. 8, 2006; revised manuscript received Dec. 21, 2006; accepted for publication Dec. 27, 2006; published online Jun. 12, 2007.

1 Introduction

Rapid growth of digital technology and wide availability of network access lead to efficient digital data acquisition, processing, transmission, and storage. One of the great advantages of digitized data is that it can make a lossless reproduction easily. However, this easy way of reproduction faces real threats, such as unauthorized copying and malicious tampering of digital data, because of the issues related to copyright protection. Therefore, these concerns have motivated work to develop efficient ways to deter users from illegally reproducing or misusing digital data. Digital watermarking techniques have attracted considerable attention as methods to protect the copyright of digital data. The watermark term is used to express the secret data embedded into original digital data, primarily for ownership proof purpose. An effective watermarking scheme should satisfy certain requirements, including transparency, robustness, security, and unambiguity. Depending on the application to be developed, the original data may or may not be used in the detection of watermarks. Considering the portability and availability of the original data, the oblivious (or blind) watermarking scheme without resorting to the original data is preferred.

A wide variety of image watermarking schemes has been proposed addressing many different application scenarios. Depending on the work domain in which the watermark is hidden, the watermarking schemes can be classified into two categories: spatial-domain watermarking schemes and frequency-domain watermarking schemes. In a spatial-domain watermarking scheme, the watermark is embedded by directly modifying the spatial characteristics, such as pixel values[1,2] and statistical traits.[3,4] In contrast, frequency-domain watermarking schemes first transform an image into frequency domains, such as discrete fourier transform (DFT),[5,6] discrete cosine transform (DCT),[7–9] and discrete wavelet transform (DWT).[10–13] The watermark is then embedded by altering the frequency coefficients. Since low and middle frequency coefficients are less likely to be affected by common signal processing than high frequency coefficients, the watermark is preferred embedded into the low and middle frequency coefficients.

Recently, singular value decomposition (SVD), which is one of the most useful numerical analysis techniques, was explored for watermarking.[14–17] The main property of SVD relevant to watermarking is that the singular values (SVs) of an image do not change significantly when a small perturbation is added to an image.

In 1995, Naor and Shamir proposed a revolutionary cryptographic structure called visual cryptography (VC) for the protection of secret messages.[18] This new cryptographic structure has two significant characteristics: 1. it provides a perfectly secure way to protect secret messages; and 2. the human visual system (HVS) can identify confidential messages directly without any computations when retrieving encrypted messages. Recently, numerous VC-based copyright protection schemes were proposed.[19–23] Wang, Tai, and Yu[19] proposed a VC-based repeating watermarking scheme in which the watermark embedding is done by adding some parts of the watermark into edge blocks of the host image to enhance the robustness of the scheme. However, their scheme needs to alter the host image to embed a watermark. A watermarking scheme based on torus automorphism and VC techniques was proposed by Chang and

Chuang,[20] in which a watermark is embedded without altering the host image. Nevertheless, the robustness of the scheme tends to decrease with the increase of the JPEG compression ratio.[21] In 2005, Lou, Shieh, and Tso[22] developed a copyright protection scheme based on chaos and VC techniques. However, their scheme does not provide the main characteristic of VC that uses the HVS to decrypt secret messages. The watermark is retrieved by performing an exclusive-or (XOR) operation between the shadow images. In 2005, Hsu and Hou[23] proposed a copyright protection scheme that employs sampling distribution of means (SDM) and VC to achieve the requirements of robustness and security. In their scheme, the secret message can be identified by the HVS directly without the aid of computers.

In this work, a novel copyright protection scheme based on VC and SVD is proposed. The proposed scheme first applies the SVD technique to create a master share from the host image. Then, the master share is used together with a secret image to construct an ownership share according to a two-out-of-two VC scheme. When the rightful ownership needs to be identified, the master share, generated from the image to be identified, and the ownership share are stacked to reveal the secret image without the aid of computers. The main advantages of the proposed scheme can be summarized as follows.

- The secret image is embedded without altering the host image, which is suitable for the application in which any modifications of images cannot be allowed, such as medical, satellite, and astronomical images.
- The secret image can be revealed without resorting to the original host image.
- The rightful ownership can be identified by HVS directly without the aid of computers.
- The security of the scheme is ensured by the properties of VC.
- The requirement of robustness is achieved, since the singular values (SVs) of an image have good stability. When a small perturbation is added to an image, its SVs do not change significantly.

The remainder of this work is organized as follows. In Sec. 2, the background of SVD and VC is briefly described. The proposed copyright protection scheme is introduced in Sec. 3. In Sec. 4, the experimental results are presented to demonstrate the performance of the proposed scheme. Conclusions are finally drawn in Sec. 5.

2 Preliminaries

Since VC and SVD techniques can be found in Refs. 18 and 24, this work gives only a brief overview as follows.

2.1 *Visual Cryptography*

In 1995, Naor and Shamir[18] introduced a two-out-of-two VC scheme for binary image encryption and distribution. The major property of VC is that it makes the hidden image decodable directly by the human eye without any computations. The scheme enables two participants to share the secret message. The secret information can be decrypted by stacking the two shares. Anyone who holds only one share is unable to reveal any information about the secret message. The concept of Naor and Shamir's VC scheme is briefly described as follows.

Table 1 The codebook of Naor and Shamir's scheme.

Pixels	White						Black					
Share 1	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□
Share 2	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□
Stacked results	■□	■□	■□	■□	■□	■□	■	■	■	■	■	■

By applying Naor and Shamir's scheme to a secret image of size $M \times N$ pixels, each pixel of the secret image is expanded to 2×2 subpixels, and two share images of size $2M \times 2N$ pixels are thus obtained. Table 1 shows the concept of the two-out-of-two VC scheme. According to the concept demonstrated in Table 1, if a pixel is white in the secret image, the corresponding subpixels in both share images are identical, and the stacked result contains two white subpixels and two black subpixels. On the contrary, if a pixel is black in the secret image, the corresponding subpixels in the first share image are complements to those in the same spatial positions within the second share image, and the stacked result consists of four black subpixels. Naor and Shamir's scheme is secure, since each 2×2 block of the two share images is randomly selected. Furthermore, anyone who holds only one share image is unable to reveal any information about the secret message.

2.2 *Singular Value Decomposition*

SVD is a fundamental technique used to diagonalize matrices in numerical analysis. It has been successfully applied to a variety of applications such as data compression, signal processing, and pattern analysis.[24,25] From the viewpoint of linear algebra, a discrete image can be regarded as a matrix of non-negative scalar entries. Let such an image be denoted by A and let A be a square image whose dimension is $N \times N$ and rank $=r$, $r \leq N$. The SVD of A is defined as

$$A = UDV^T = [u_1, u_2, \ldots, u_N] \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & 0 \\ & & \lambda_3 & \\ & 0 & & \ddots \\ & & & & \lambda_N \end{bmatrix} \times [v_1, v_2, \ldots, v_N]^T = \sum_{i=1}^{N} \lambda_i u_i v_i, \quad (1)$$

where the U and V components are $N \times N$ real unitary matrices whose column vectors are u_i's and v_i's, respectively. The D component is an $N \times N$ matrix with entry λ_i's (SVs), satisfying,

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > \lambda_{r+1} = \cdots = \lambda_N = 0.$$

Although the image matrix A is assumed to be a square matrix for convenience, other nonsquare images can be

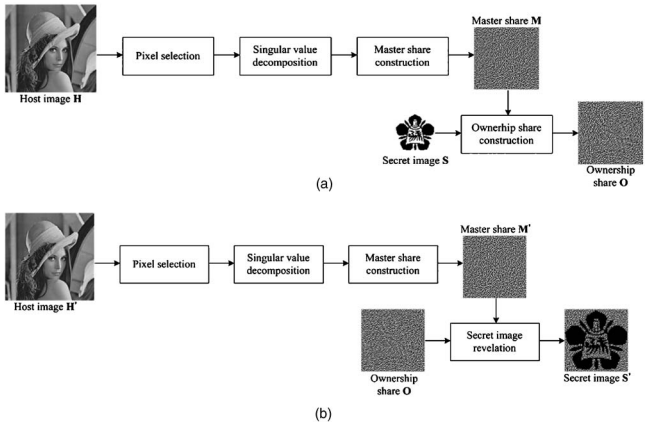

Fig. 1 An overview of the proposed copyright protection scheme. (a) The ownership share construction phase, and (b) the ownership identification phase.

processed in exactly the same way. The main property of SVD relevant to information hiding is that bigger SVs of an image have good stability.[14,15] In other words, the SVs do not change significantly when common image processing attacks are performed on an image.

3 Proposed Scheme

In this section, the proposed copyright protection scheme based on SVD and VC techniques is presented. The scheme can be divided into two phases: the ownership share construction phase and the ownership identification phase. An overview of the proposed scheme is shown in Fig. 1.

During the ownership share construction phase, as shown in Fig. 1(a), a list of pixel positions is first randomly selected from the host image. Then, the SVD is performed on a small window centered at each selected pixel position, and the largest SV of each window is utilized to construct a master share. Finally, an ownership share is constructed by using the master share and a secret image according to the VC technique, and the resultant ownership share should be registered to a certified authority (CA) for further authentication.

When a dispute over the rightful ownership of the host image arises, the ownership identification procedure should be performed to protect the owner's intellectual property. Accordingly, a master share is generated from the suspected image in the same way as in the ownership share construction phase. The hidden secret image can be revealed by stacking the generated master share and the ownership share kept by the CA. The ownership of the suspected image is therefore recognized. The workflow of ownership identification is shown in Fig. 1(b). In the following, details of the proposed scheme are described.

3.1 *Ownership Share Construction*

Assume that a copyright owner wants to embed a secret image $\mathbf{S}$ of size $N_1 \times N_2$ pixels into a gray-level host image $\mathbf{H}$ of size $M_1 \times M_2$ pixels for protecting his or her intellectual property. In the beginning, a pseudorandom number generator (PRNG) seeded with a private key PK is employed to select a list of pixel positions, $P=\{p_1, p_2, \ldots, p_{N_1 \times N_2}\}$, from the host image. Then, the SVD is performed on a window of size $W \times W$ pixels centered at each selected pixel position, and a sequence of SVs, $\Lambda=\{\lambda_1^1, \lambda_1^2, \ldots, \lambda_1^{N_1 \times N_2}\}$, consisting of the largest SV of each window, is thus acquired. To compute the threshold T, which is used for master share construction, all the SVs in Λ are first rearranged in a descending order to obtain a sorted sequence $\hat{\Lambda}=\{\hat{\lambda}_1^1, \hat{\lambda}_1^2, \ldots, \hat{\lambda}_1^{N_1 \times N_2}\}$. The threshold that can be utilized to acquire a balanced (0,1) share is determined by

$$T=\begin{cases} \hat{\lambda}_1^{(N_1 \times N_2+1)/2}, & \text{if } N_1 \times N_2 \text{ is odd} \\ \frac{1}{2}[\hat{\lambda}_1^{(N_1 \times N_2)/2} + \hat{\lambda}_1^{1+(N_1 \times N_2)/2}], & \text{if } N_1 \times N_2 \text{ is even} \end{cases}. \tag{2}$$

Assume that $\mathbf{M}$ is the master share of size $2N_1 \times 2N_2$ pixels. This master share is divided into nonoverlapping 2×2 blocks, $m_k (1 \le k \le N_1 \times N_2)$, in which each block can be generated according to the codebook, as illustrated in Table 2. For example:

if mod $(k,3)=0$

if $\lambda_1^k \ge T$ then $m_k = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

else $m_k = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$,

where 0 and 1 within block m_k represent a black pixel and a white pixel, respectively.

After performing the master share generation process, we can start to construct the ownership share $\mathbf{O}$. The ownership share of size $2N_1 \times 2N_2$ pixels is divided into nonoverlapping 2×2 blocks, o_k $(1 \le k \le N_1 \times N_2)$. Assume that s_k $(1 \le k \le N_1 \times N_2)$ denotes a pixel of the secret image $\mathbf{S}$. The generated master share $\mathbf{M}$ is utilized together with the secret image $\mathbf{S}$ to construct the ownership share $\mathbf{O}$ according to the codebook as shown in Table 2. For example:

Table 2 The codebook of the proposed scheme.

Feature	mod(k, 3)	White		Stacked result	Black		Stacked result
		Share M	Share O		Share M	Share O	
$SV_k \ge T$	0						
	1						
	2						
$SV_k < T$	0						
	1						
	2						

if $m_k = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

if $s_k = 1$ then $o_k = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

else $o_k = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Note that although the window size used for performing the SVD can be arbitrarily selected by the copyright owner, it is adequate, from our observations, to choose a window of size at least 31×31 pixels to achieve satisfactory robustness against various image processing attacks. The procedure of ownership share construction can be summarized by the following algorithm.

3.1.1 *Ownership share construction algorithm*

Input. A gray-level host image $\mathbf{H}$ of size $M_1 \times M_2$ pixels, a secret image $\mathbf{S}$ of size $N_1 \times N_2$ pixels, a window of size $W \times W$ pixels, a private key PK, and a codebook C.

Output. An ownership share $\mathbf{O}$ of size $2N_1 \times 2N_2$ pixels.

1. Select a list of pixel positions, $P = \{p_1, p_2, \ldots, p_{N_1 \times N_2}\}$, by using a PRNG seeded with the private key PK.
2. Perform the SVD on the window centered at each pixel position in P and a sequence of SVs, $\Lambda = \{\lambda_1^1, \lambda_1^2, \ldots, \lambda_1^{N_1 \times N_2}\}$, consisting of the largest SV of each window, is acquired.
3. Calculate the threshold T by using Eq. (2).
4. Construct a master share $\mathbf{M}$ by utilizing the sequence Λ and the threshold T according to the codebook C.
5. Create the ownership share $\mathbf{O}$ by mapping the master share $\mathbf{M}$ and the secret image $\mathbf{S}$ to the codebook C.

After the ownership share construction, the window size $W \times W$ pixels, the private key PK, and the codebook C must be kept secretly by the copyright owner. In addition, the resultant ownership share $\mathbf{O}$ should be registered to a CA for further authentication.

3.2 *Ownership Identification*

Assume that a dispute over the rightful ownership of the host image $\mathbf{H}'$ has arisen. To determine the rightful ownership of the suspected image, the copyright owner should provide the same window size, private key, and codebook used in the ownership share construction phase, so that the hidden secret image can be revealed after performing the ownership identification procedure. The procedure comprises two stages. The first stage is utilizing the host image $\mathbf{H}'$ to generate a master share $\mathbf{M}'$. The process of master share generation is the same as that used in the ownership share construction phase. The second stage is retrieving the secret image $\mathbf{S}'$ by using the master share $\mathbf{M}'$ and the ownership share $\mathbf{O}$ according to the VC technique. Since the secret image revelation is based on the VC technique, we can simply print the two shares, $\mathbf{M}'$ and $\mathbf{O}$, onto transparencies and then stack them together to reveal the secret image without the aid of computers. Moreover, with the aid of computers, we can perform the reduction process on the retrieved secret image $\mathbf{S}'$ to acquire a reduced secret image $\mathbf{S}''$, which is of the same size as the original one. The ownership identification procedure is described by the following algorithm.

Fig. 2 The host images and the secret image.

3.2.1 *Ownership identification algorithm*

Input. A suspected host image $\mathbf{H}'$ of size $M_1 \times M_2$ pixels, an ownership share $\mathbf{O}$ of size $2N_1 \times 2N_2$ pixels, a window of size $W \times W$ pixels, a private key PK, and a codebook C.

Output. A retrieved secret image $\mathbf{S}'$ of size $2N_1 \times 2N_2$ pixels and a reduced secret image $\mathbf{S}''$ of size $N_1 \times N_2$ pixels.

1. Select a list of pixel positions, $P' = \{p_1', p_2', \ldots, p_{N_1 \times N_2}'\}$, by using a PRNG seeded with the private key PK.
2. Perform the SVD on the window centered at each pixel position in P' and a sequence of SVs, $\Lambda' = \{\lambda_1'^1, \lambda_1'^2, \ldots, \lambda_1'^{N_1 \times N_2}\}$, consisting of the largest SV of each window, is acquired.
3. Calculate the threshold T' by using Eq. (2).
4. Generate a master share $\mathbf{M}'$ by utilizing the sequence Λ' and the threshold T' according to the codebook C.
5. Retrieve the secret image $\mathbf{S}'$ by stacking the master share $\mathbf{M}'$ and the ownership share $\mathbf{O}$.
6. Divide the retrieved secret image $\mathbf{S}'$ into nonoverlapping 2×2 blocks, s_k' $(1 \le k \le N_1 \times N_2)$.
7. Perform the reduction process to obtain a reduced secret image $\mathbf{S}''$ by the following rules:

$$s_k'' = \begin{cases} 1, & \text{if } \sum_i \sum_j s_k' \ge 2 \\ 0, & \text{if } \sum_i \sum_j s_k' < 2 \end{cases}. \tag{3}$$

4 Experimental Results

In this section, the performance of the proposed copyright protection scheme is demonstrated. The resistance of the proposed scheme to various distortions was studied in a series of experiments on gray-level images. Moreover, the evaluation results of two existing VC-based copyright protection schemes was provided for performance comparisons. Three gray-level images of size 512×512 pixels, called Lena, Airplane, and Barbara, were selected as the host images. A visually recognizable binary image of size 64×64 pixels was used as the secret image. Figures 2(a)–2(c) show the three host images, and the secret image is shown in Fig. 2(d). In addition, a window of

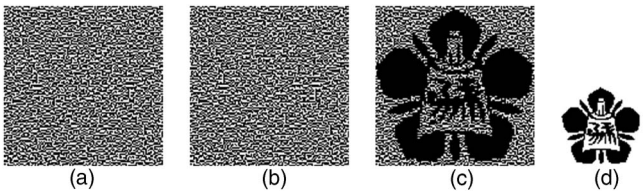

Fig. 3 Sample results of the proposed scheme: (a) master share, (b) ownership share, (c) revealed secret image, and (d) reduced secret image.

size 31×31 pixels was used to proceed all of the experiments. Figure 3 illustrates sample results obtained by applying the proposed scheme to Fig. 2(a). The master share and the ownership share are shown in Figs. 3(a) and 3(b), respectively. The revealed secret image, acquired by stacking Figs. 3(a) and 3(b), is shown in Fig. 3(c), and the reduced secret image is shown in Fig. 3(d).

For quantitative evaluation, two common similarity measurements, peak signal-to-noise ratio (PSNR) and normalized correlation (NC), were employed to evaluate the performance of the proposed scheme. The PSNR is used to measure the image quality and is defined as

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255^2}{\mathrm{MSE}} (\mathrm{dB}), \tag{4}$$

$$\mathrm{MSE} = \frac{1}{M_1 \times M_2} \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} \|\mathbf{H}_{i,j} - \mathbf{H}'_{i,j}\|^2, \tag{5}$$

where $\mathbf{H}_{i,j}$ stands for a pixel color of the original host image, $\mathbf{H}'_{i,j}$ represents a pixel color of the attacked image, and $M_1 \times M_2$ is the image size. The NC, used to measure the similarity between the original secret image and the reduced secret image, is defined as

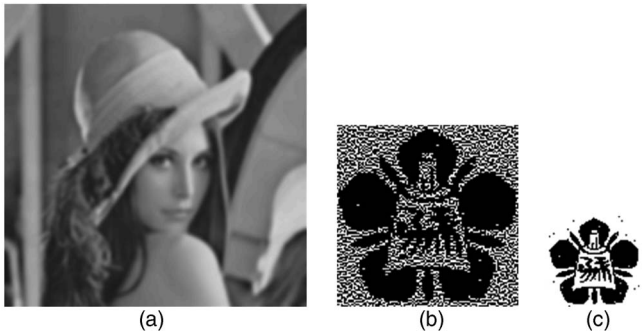

Fig. 4 Experimental results under blurring. (a) Blurred image (PSNR=25.65 dB), (b) revealed secret image, and (c) reduced secret image (NC=0.993).

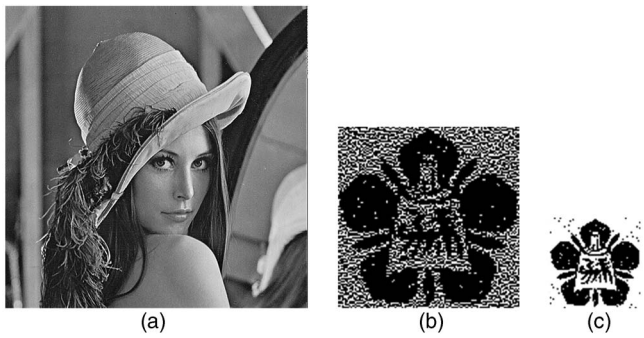

Fig. 5 Experimental results under sharpening. (a) Sharpened image (PSNR = 19.09 dB), (b) revealed secret image, and (c) reduced secret image (NC=0.972).

$$\mathrm{NC} = \frac{\sum_{i=1}^{N_1} \sum_{j=1}^{N_2} \overline{\mathbf{S}_{i,j} \oplus \mathbf{S}''_{i,j}}}{N_1 \times N_2}, \tag{6}$$

where $\mathbf{S}_{i,j}$ represents a pixel color of the original secret image, $\mathbf{S}''_{i,j}$ represents a pixel color of the reduced secret image, $\oplus$ denotes the XOR operation, and $N_1 \times N_2$ is the image size.

In the following experiments, the robustness of the proposed scheme against common image processing attacks is estimated, including blurring (Gaussian blur with a radius of 3 pixels), sharpening, median filtering (with a width of 11 pixels), histogram equalization, color reduction (reduced from 256 colors to 16 colors), noise addition (Gaussian noise with a variance of 30), JPEG lossy compression (with a compression factor of 50%), and rotation (3 deg to the right). The sample results obtained by performing the proposed scheme on the Lena image are shown in Figs. 4–11. The detailed evaluation results are shown in Table 3. Figures 4–11 demonstrate that the revealed secret images can be easily identified by human visual examination, even if the image quality of the original host image has been greatly degraded. In addition, most NC values listed in Table 3 are higher than 0.9. These high values demonstrate that the proposed scheme achieved satisfactory robustness against common image processing attacks.

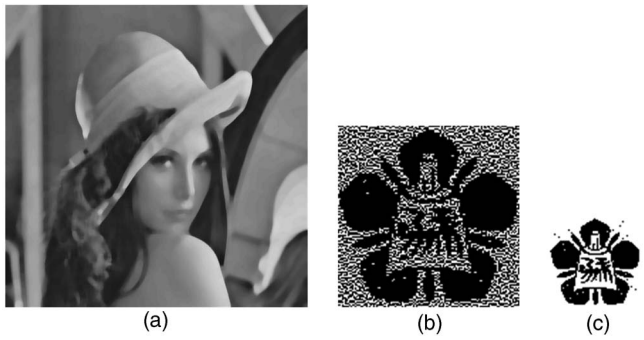

Fig. 6 Experimental results under median filtering. (a) Filtered image (PSNR=26.88 dB), (b) revealed secret image, and (c) reduced secret image (NC=0.993).

Fig. 7 Experimental results under histogram equalization. (a) Equalized image (PSNR=19.47 dB), (b) revealed secret image, and (c) reduced secret image (NC=0.976).

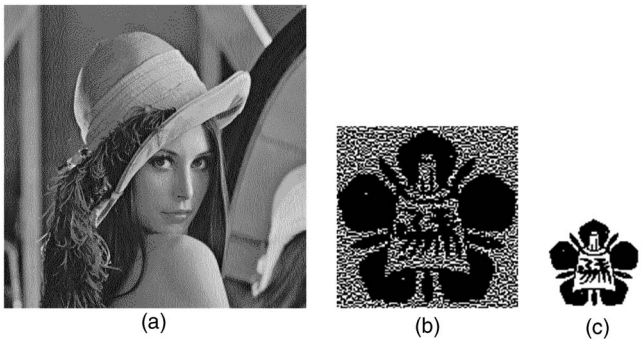

Fig. 8 Experimental results under color reduction. (a) Image with 16 colors (PSNR=15.82 dB), (b) revealed secret image, and (c) reduced secret image (NC=0.998).

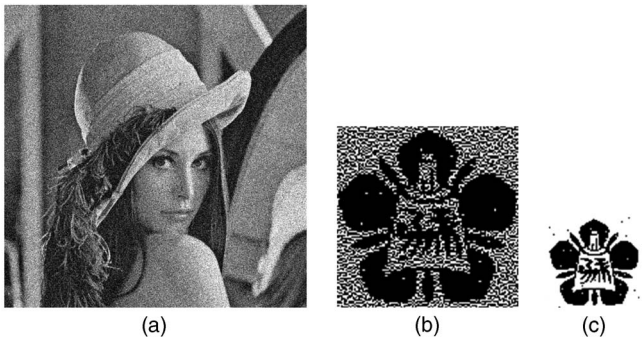

Fig. 9 Experimental results under noise addition. (a) Image with an addition of Gaussian noise (PSNR=18.83 dB), (b) revealed secret image, and (c) reduced secret image (NC=0.992).

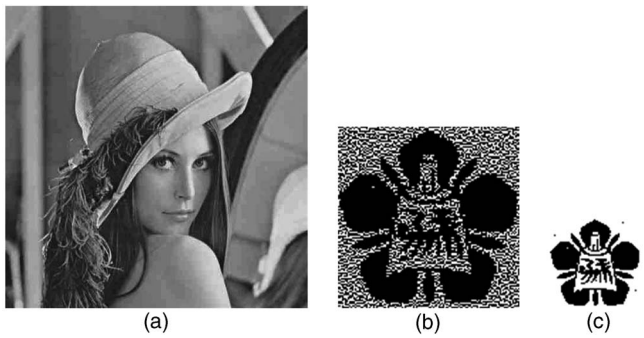

Fig. 10 Experimental results under JPEG compression. (a) Compressed image (PSNR=32.55 dB), (b) revealed secret image, and (c) reduced secret image (NC=0.997).

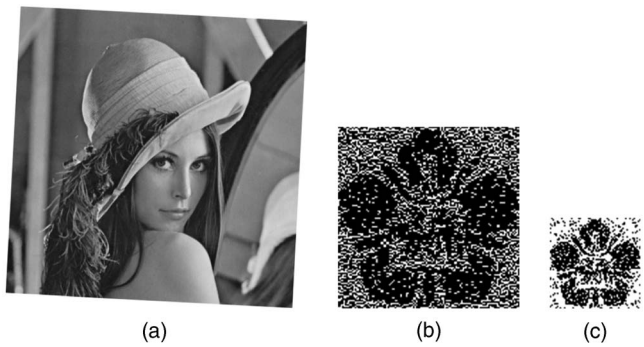

Fig. 11 Experimental results under rotation. (a) Image rotated 3 deg to the right (PSNR=13.07 dB), (b) revealed secret image, and (c) reduced secret image (NC=0.833).

Table 3 Evaluation results of the proposed scheme under various attacks.

	Lena		Airplane		Barbara	
Attacks	PSNR	NC	PSNR	NC	PSNR	NC
Blurring	25.65	0.993	23.96	0.988	23.03	0.991
Sharpening	19.09	0.972	18.98	0.981	13.63	0.971
Median filtering	26.88	0.993	23.40	0.977	23.00	0.988
Histogram equalization	19.47	0.976	11.95	0.902	18.27	0.985
Color reduction	15.82	0.998	18.47	0.998	15.33	0.995
Noise addition	18.83	0.992	19.04	0.986	18.87	0.995
JPEG	32.55	0.997	32.10	0.993	27.82	0.996
Rotation	13.07	0.833	14.56	0.872	12.49	0.828

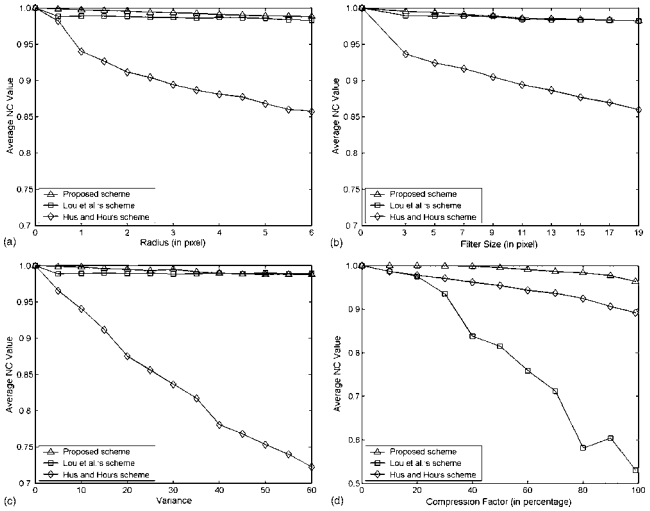

Fig. 12 NC curves of tested copyright protection schemes to common image processing attacks. (a) Gaussian blurring, (b) median filtering, (c) Gaussian noise addition, and (d) JPEG compression.

For performance comparisons, two copyright protection schemes, proposed by Lou, Shieh, and Tso,[22] and Hsu and Hou,[23] were implemented in this study. The three host images and the secret image, as shown in Fig. 2, were used for experiments. The results of performance comparisons are shown in Fig. 12. Figures 12(a)–12(d) show the NC curves under Gaussian blurring, median filtering, Gaussian noise addition, and JPEG compression, respectively. The comparison results, as shown in Figs. 12(a)–12(c) show that both the proposed scheme and Lou, Shieh, and Tso's scheme provide strong robustness against Gaussian blurring, median filtering, and Gaussian noise addition, while Hsu and Hou's scheme has a weak robustness to these attacks. Furthermore, the results in Fig. 12(d) show that the proposed scheme outperformed the other two schemes under JPEG compression. The NC values are all higher than 0.95, even if the host images have undergone JPEG compression with a compression factor of 99%. Experimental results indicate the efficiency and feasibility of the proposed copyright protection scheme for practical applications.

5 Conclusions

A copyright protection scheme for digital images based on visual cryptography and singular value decomposition is proposed. The proposed scheme first generates a master share from the host image by applying the SVD technique. The master share is then used together with a secret image to construct an ownership share according to the VC technique. For rightful ownership identification, the master share, generated from the suspected image, and the ownership share are stacked to reveal the secret image without the aid of computers.

In the proposed scheme, the copyright protection of digital images is achieved without modifying the host image, which is helpful for some special applications in which any modifications of images is not acceptable, such as the protection of medical images and astronomical images. Moreover, the hidden secret image can be revealed without the help of the original image. Experimental results demonstrate that the proposed scheme is quite robust against common image processing attacks, such as blurring, sharpening, color reduction, median filtering, noise addition, and JPEG lossy compression. Furthermore, the results show that the proposed scheme outperformed Lou, Shieh, and Tso,[22] and Hsu and Hou's[23] schemes under several common attacks.

Acknowledgments

The authors would like to thank the anonymous reviewers for their helpful and constructive suggestions that improved the quality of the work. This work was supported in part by the National Science Council of China under grant number NSC-95-2221-E-006-159-MY3.

References

1. M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. Image Process.* **11**, 585–595 (2001).
2. R. G. Van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proc. IEEE Int. Conf. Image Process.*, pp. 86–90 (1994).
3. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.* **35**, 313–336 (1996).
4. I. Pitas, "A method for signature casting on digital images," in *Proc. IEEE Int. Conf. Image Process.*, pp. 215–318 (1996).
5. C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale and translation resilient watermarking for images," *IEEE Trans. Image Process.* **10**, 767–782 (2001).
6. J. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Process.* **66**, 303–317 (1998).
7. C. T. Hsu and J. L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Process.* **8**, 58–68 (1999).
8. G. C. Langelaar and R. L. Lagendijk, "Optimal differential energy watermarking of DCT encoded images and video," *IEEE Trans. Image Process.* **10**, 148–158 (2001).
9. W. C. Chu, "DCT-based image watermarking using subsampling," *IEEE Trans. Multimedia* **5**, 34–38 (2003).
10. M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Trans. Image Process.* **8**, 783–791 (2001).
11. M. Tsai, K. Y. Yu, and Y. Z. Chen, "Joint wavelet and spatial transformation for digital watermarking," *IEEE Trans. Consum. Electron.* **46**, 241–245 (2000).
12. S. H. Wang and Y. P. Lin, "Wavelet tree quantization for copyright protection watermarking," *IEEE Trans. Image Process.* **13**(2), 154–165 (2004).
13. A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," *Pattern Recogn. Lett.* **26**(7), 1019–1027 (2005).
14. R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia* **4**, 121–128 (2002).
15. R. Sun, H. Sun, and T. Yao, "A SVD and quantization based semi-fragile watermarking technique for image authentication," in *Proc. Int. Conf. Signal Process.*, pp. 1592–1595 (2002).
16. C. C. Chang, P. Y. Tsai, and M. H. Lin, "SVD-based digital image watermarking scheme," *Pattern Recogn. Lett.* **26**, 1577–1586 (2005).
17. J. M. Shieh, D. C. Lou, and M. C. Chang, "A semi-blind digital watermarking scheme based on singular value decomposition," *Comput. Stand. Inter.* **28**, 428–440 (2006).
18. M. Naor and A. Shamir, "Visual cryptography," in *Proc. Advances Cryptol. EUROCRYPT94, LNCS 950*, pp. 1–12, Springer-Verlag, Berlin (1995).
19. C. C. Wang, S. C. Tai, and C. S. Yu, "Repeating image watermarking technique by the visual cryptography," *IEICE Trans. Fundamentals* **E83-A**(8), 1589–1598 (2000).
20. C. C. Chang and J. C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," *Pattern Recogn. Lett.* **23**, 931–941 (2002).
21. 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. Int. Computer Symp.*, pp. 661–666 (2004).
22. D. C. Lou, J. M. Shieh, and H. K. Tso, "Copyright protection scheme based on chaos and secret sharing techniques," *Opt. Eng.* **44**(11), 117004 (2005).

23. C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Opt. Eng.* **44**(7), 077003 (2005).
24. V. C. Klema, "The singular value decomposition: its computation and some applications," *IEEE Trans. Autom. Control* **25**(2), 164–176 (1980).
25. Z. Q. Hong, "Algebraic feature extraction of image for recognition," *Pattern Recogn.* **24**, 211–219 (1991).

Ming-Shi Wang received his BS degree in electronic engineering from Feng Chia University, Taichung, Taiwan, in 1977, his MS degree in electrical engineering from National Cheng Kung University, Tainan, Taiwan, in 1982, and his PhD degree in computation from UMIST, Manchester, United Kingdom, in 1992. Currently, he is an associate professor in Department of Engineering Science and the chief of the Division of Teaching and Research, Computer, and Network Center, both at National Cheng Kung University, Tainan, Taiwan. His major research interests are digital image processing, computer vision, content filtering, virtual reality, and grid computing.

Wei-Che Chen received his BS and MS degrees in engineering science from National Cheng Kung University, Tainan, Taiwan, in 1992 and 2003, respectively. He is currently pursuing his PhD degree at National Cheng Kung University, Tainan, Taiwan. His research interests include image processing, computer vision, and digital watermarking.