A Digital Image Watermarking Scheme Based on Visual Cryptography

Amir Houmansadr[*], Shahrokh Ghaemmaghami[**]
[*] Electrical Engineering Department, Sharif University of Technology, Azadi St., Tehran, Iran
[**] Electronic Research Center, Sharif University of Technology, Azadi St., Tehran, Iran
Emails: houmansadr@mehr.sharif.edu, ghaemmag@sharif.edu

Abstract

An image watermarking scheme based on the visual cryptography is proposed in this paper. The owner's mark which can be a visible logo is split into two share-images using a visual secret sharing scheme. One of the shares is embedded into the host image whereas the other is kept as the system's secret-key to be used in the watermark detection process. In case the inserted watermark is a visible logo, the mark's existence can be verified just by the human's eye. Experimental results show that the proposed scheme is robust against major watermarking attacks.

Keywords: digital image watermarking, visual cryptography.

Introduction

The extreme development of internet has made the transmission, distribution and access to digital media very convenient. So, media producers are more frequently dealing with illegal and unauthorized usage of their productions.

Over the last two decades, digital watermarking has been addressed as an effective solution to safeguard copyright laws and an extensive effort has been made to design robust watermarking algorithms [1]. Basically, a digital watermark is an invisible mark that is inserted into a digital media such as audio, image, or video to identify illegal distributions of copyright protected digital media and also lawbreaking customers. A digital watermark must have special features to achieve functionalities desired. The embedded mark should be robust enough against various watermarking attacks, while keeping the perceived quality of the host signal unchanged (the imperceptibility requirement). Watermarking attacks consist of deliberate attacks made maliciously to remove or change the mark sequence by lawbreakers, unintentional modifications caused by coding and compression that are made to the digital media prior to transmission and/or storage, and errors occurred during the transmission of the media through the networks.

In this paper, we propose a novel image watermarking scheme, based on the concept of visual cryptography. A digital watermark (which can be the visible logo of the owner) is split according to a visual secret sharing scheme [2], [3]. One of the shares is inserted into the image and the other serves as the detection key.

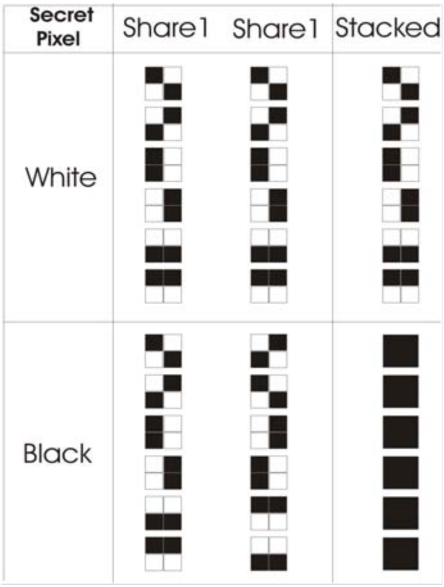
In section 1, we describe the concept of visual cryptography. Sections 2 and 3 explain the proposed watermark insertion and detection schemes, respectively. Section 4 is dedicated to experiments and discusses the experimental results.

1. Visual Cryptography

In 1979, *Blakley* and *Shamir* developed the concept of *secret sharing* independently [4], [5]. A secret sharing scheme shares a secret into a number of shares so that the cooperation of a predetermined group of shareholders reveals the secret whereas the secret reconstruction is impossible for any unauthorized set of shareholders. Visual cryptography is a kind of secret sharing in which the secret reconstruction can be done only by the human visual system [2]. This is why it is also called visual secret sharing (VSS).

Many VSS schemes have been proposed from which we consider the (2,2) VSS scheme proposed by Naor *et al.* in [2], [3]. According to the algorithm, each pixel of the binary-valued secret image is expanded into 2*2 pixels, as shown in table 1. To share a white pixel of the secret image, one row from the first 6 rows of table1 is chosen randomly. Similarly, the two shares of a black pixel are determined by a random selection from the 6 last rows of table 1. As a result, an M*N pixels secret image is expanded into two 2M*2N pixels share-images.

Table 1 A (2x2) VSS scheme using 2x2 subpixels.


Secret Pixel
Share1
Share1
Stacked
White
Black

Considering security of the method, presence of only one share image reveals nothing about the corresponding secret image, i.e., each 2*2 pixels block of one share-image may correspond to either a white pixel or a black pixel of the secret image. As table 1 shows, stacking the shares of a black secret pixel results in 4 black subpixels, whereas only 2 black subpixels is gained by stacking shares of a white secret pixel. So, secret image is revealed to human eyes by stacking the shares without performing any cryptographical computations.

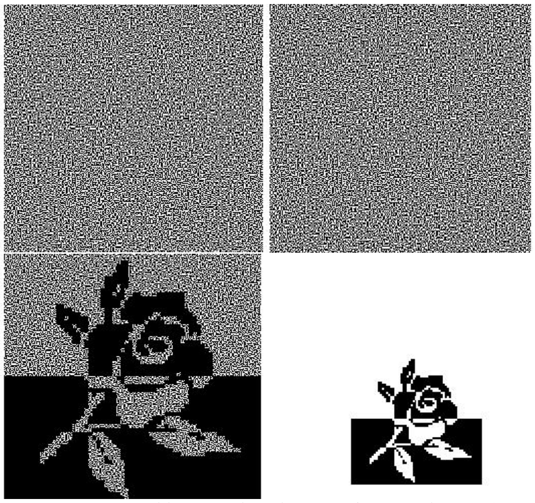


Figure 1 Stacking two share images of a secret image. (Top-left) first share, (top-right) second share, (bottom-left) stacked shares without reduction and (bottom-right) reducing stacked image which is the same as split secret image (fig. from [1]).

Figure 1 shows the result of superimposing the share-images of a secret image. Original secret image can be obtained using a simple reduction algorithm from the superimposed image.

In the next sections, the mentioned (2,2) VSS scheme is utilized in the proposed watermarking algorithm.

2. Watermark Insertion Scheme

In this section, we describe the proposed watermark insertion algorithm which exploits the mentioned (2,2) VSS.

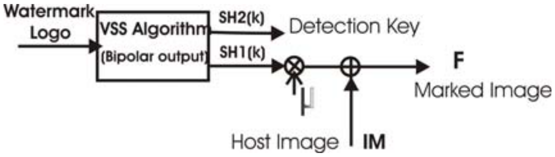


Figure 2 Block diagram of the proposed watermark insertion scheme.

Fig. 2 shows the block diagram of the watermark embedding algorithm which is performed in the spatial domain of the host image. We transform the watermark (binary logo) and all the shares from binary (0,1) to signed format (-1,+1), which leads an approximately zero-mean pseudo-random watermark sequence, so we can proceed with the detection process in a correlation-based manner. Accordingly, white and black pixels are represented by 1 and -1, respectively. The watermark, which can be the visible logo of the owner, is split into two pseudo-spread spectrum shares according to the mentioned VS scheme. One of the gained shares is then added to the host image to obtain the watermarked image as below:

$$F = IM + \mu * SH1 \tag{1}$$

where *SH1* is the first share of the mark , *IM* is the digital host image, *F* is the watermarked image, and μ is a parameter defining the mark's power which must be chosen so that the best trade off between watermark robustness and watermark imperceptibility is made. We set μ equal to two in our simulations. Fig. 3 compares an image watermarked using the proposed watermarking scheme and the unwatermarked host image. As shown, the watermark in the marked image is imperceptible.

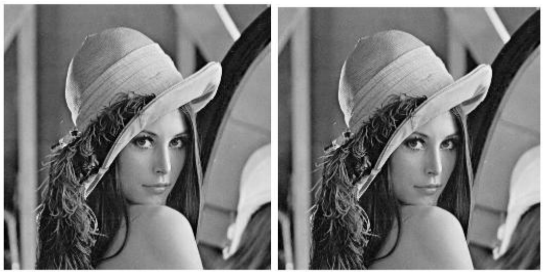


Figure 3 Imperceptibility of the proposed method. (Left) original image and (right) watermarked image.

3. Watermark Detection Scheme

Though watermark detection can be performed in an informed structure (by using the unwatermarked host image at the detector), the blind detection scheme is explained in this paper. The block diagram of the watermark detecting algorithm is depicted in fig. 4. The inserted mark is a high frequency pseudo-spread spectrum sequence. So, we get the received image passed through a high-pass filter (HPF) in order to weaken the low frequency components which more correspond to the unwatermarked host image. To gain a binary valued image, the filtered image is hard limited by comparing every pixel to a threshold, TH, as:

$$F_{HL}(i,j) = \begin{cases} 1 & if \quad F_F(i,j) > TH \\ -1 & otherwise \end{cases} \tag{2}$$

where $F_F\ (i,j)$ is the (i,j)-th pixel of the filtered image and $F_{HL}\ (\ i\ ,\ j\ )$ is the (i,j)-th pixel of the hard-limited image. We set threshold *TH* equal to the mean luminance of the input image.

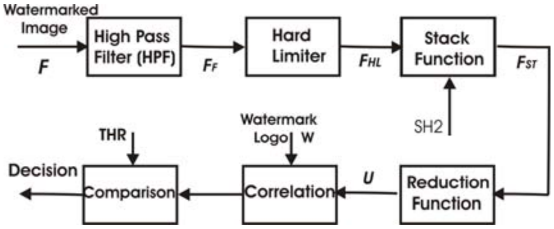


Figure 4 Block Diagram of the Detection Algorithm

The resulted image gets *Stacked* to the second share of the watermark, which was kept private as the detection key of the watermarking system. Stack function acts as the reverse of (2,2)-VSS scheme used in the watermark insertion algorithm and resembles *stacking* images printed on two transparent sheets. The stack function returns a 2M*2N pixels image whose (i,j)-th pixel is:

$$F_{ST}(i,j) = \min(F_{HL}(i,j), SH2(i,j)) \tag{3}$$

Pixels of F_{HL} and SH2 only take two values 1 and -1, representing white and black pixels respectively. As a result, only the two values 1 and -1 are allocated to the pixels' values of the gained image F_{ST}. If a black pixel is stacked to another pixel, a black pixel is obtained, whereas a white pixel is gained only if two white pixels are stacked.

The last block before evaluating the correlation is the reduction function, which returns an M*N-pixels image whose (i,j)-th pixel is given as:

$$U(i,j) = \begin{cases} 1 & if \quad L(i,j) > 0 \\ -1 & otherwise \end{cases} \tag{4}$$

where:

$$\begin{aligned} L(i,j) = F_{ST}(2i-1, 2j-1) + F_{ST}(2i-1, 2j) \\ + F_{ST}(2i, 2j-1) + F_{ST}(2i, 2j) \end{aligned} \tag{5}$$

The reduction block decides whether the secret pixel corresponding to each 2*2 block of F_{ST} is a black pixel or a white pixel, according to the last column of table 1. Due to the fact that watermarked image F contains the first share of the logo, running the stack function and the reduction function using the two 2M*2N-pixels images F_{HL} and the second share of the logo SH2 produces an M*N-pixels image which is highly correlated by the watermark logo.

The watermark can be detected due to the correlation between the gained image and the watermark. The last block of the watermark detection scheme of fig. 4 computes the correlation between this image and the inserted watermark, as:

$$\rho = \frac{U \bullet W}{\sqrt{E(U) * E(W)}} \tag{6}$$

where W is the logo, U is the stacked image passed through the reduction function and E(X) computes the energy of image X. By comparing this correlation coefficient to a threshold, THR, it is decided whether the watermark W exists in the image *F* or not.

However, the presence of the watermark can be investigated just by the human eyes without any mathematical computation. Fig. 5 illustrates the resulted image after reduction in the detection process besides the original watermark logo.

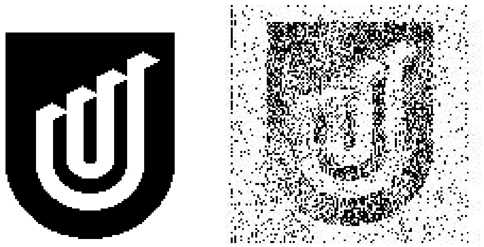


Figure 5 (Left) watermark and (right) detected mark (logo from [1])

The detection algorithm discussed above is a blind detection scheme. Substituting the high-pass filter in fig.4 by an image subtractor and using the host image, IM, transforms the detection scheme to informed structure. This leads better robustness to various watermarking attacks, however the original unwatermarked image is needed at the detector.

4. Experimental Results

We simulated the proposed watermark insertion and detection schemes and investigated the effect of various attacks on the watermarking system. We examined different high pass filters of order 21 to find the optimum filter that is to maximize the ratio of correct detection (correlation coefficient ρ, in case of genuine watermark logo) to false detection (correlation coefficient ρ for an irrelevant watermark logo). The maximum ratio was about 8.3 for different watermark logos, which gained by using the HPF whose frequency response is shown in fig. 6.

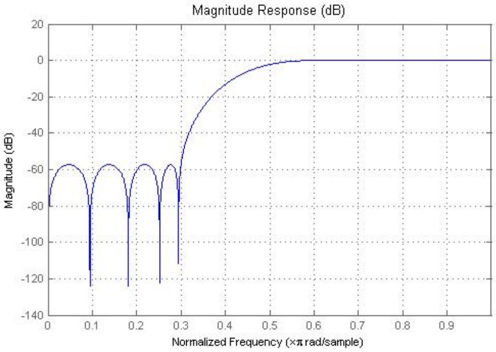


Figure 6 Frequency response of the HPF used in the detection scheme.

The threshold THR in the detection scheme should be properly selected to minimize the false alarm ratio (detecting a watermark in an unwatermarked image or denying the watermark in a watermarked image). We set THR equal to 0.12 based on certain experiments. We also surveyed the effect of different attacks on the watermark detection.

JPEG Compression acts as a low-pass filtering, which zeros out frequency components. We marked different images using the proposed scheme, and then performed JPEG compression with various quality factors, Q, on the marked images. Subsequently, we verified the existence of the watermark in the compressed images by evaluating the correlation coefficient as in (6). Table 2 depicts decrement of the correlation coefficient of the JPEG compressed watermarked image over the typical uncompressed correlation coefficient. A "Y" in the last row of the table indicates that the watermark's existence is successfully detected, whereas an "N" shows that watermark is not detected due to the performed watermarking attack.

Table 2 Decrement of the correlation coefficient and the detection status after JPEG compression with various quality factors (Q).

Quality factor	90	80	70	60
Decrement of ρ (%)	29	61	71	75
Detection Status	Y	Y	Y	N

The high impact of the JPEG compression on the watermark detection is due to the fact that JPEG compressor eliminates high frequency components of the watermarked image, which more correspond to the high-frequency inserted watermark.

Cropping can be taken as the dual of the JPEG compression, which zeros out spatial components of the image. Because of its structure, the proposed scheme is quite robust to the cropping attack, if spatial synchronization is made. Table 3 shows decrement of the correlation coefficient of the cropped watermarked image to the typical watermarked correlation coefficient, for both cases with and without performing synchronization.

Table 3 Decrement of the correlation coefficient and the detection status after image cropping, with respect to the availability of synchronization.

Cropping Percentage		10	20	30	40	50
Synch.	Decrement of ρ (%)	6	13	8	11	13
	Detection Status	Y	Y	Y	Y	Y
No Synch.	Decrement of ρ (%)	36	43	57	55	75
	Detection Status	Y	Y	Y	Y	N

The effect of *Image Rotating* on the proposed watermarked image is also taken as a watermarking attack. By performing spatial synchronization (rotating the detection key by a value equal to what is applied to the marked image), the correlation value shows up to 4% decrement for various rotation angels. However, the scheme is fragile to rotation if no synchronization is made.

Changing the aspect ratio (AR) of the watermarked image, which is the image's height to width ratio, has a little impact on the correlation coefficient. Table 4 illustrates the effect of changing the aspect ratio of a 256*256 pixels watermarked image on the detection process.

Table 4 Decrement of the correlation coefficient and the detection status after changing the AR of a 256*256 pixels watermarked image.

New Size (pixels)	256*128	256*64	512*256
Decrement of ρ (%)	14	6	26
Detection Status	Y	Y	Y

The high robustness of the proposed scheme to geometrical attacks, in the presence of synchronization, is due the VSS scheme's robustness to this kind of distortions. Fig. 7 illustrates the reconstructed secret image by the VSS scheme, if the shares are geometrically distorted.

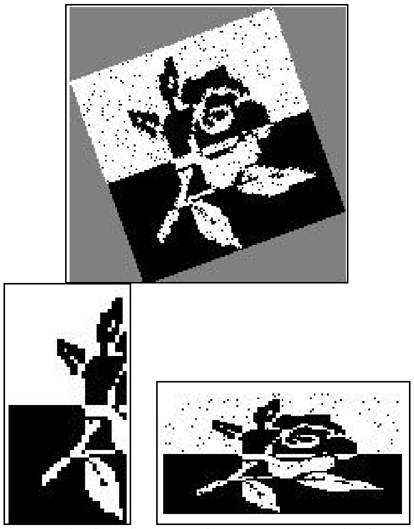


Figure 7 Retrieving the secret image (watermark) from its geometrical distorted shares. (Top) image rotating, (bottom-left): image cropping and (bottom-right): changing the aspect ratio.

We also investigated the robustness of the scheme to image scaling. We low-pass filtered the watermarked image using a four-tap filter, prior to downsampling by R, in each direction. The resulting image is upsampled before calculation of the correlation coefficient. Table 5 shows the decrement of the correlation coefficient of scaled image compared to that of the original watermarked image. In case no filtering is performed, prior to downsampling, the scheme shows a higher degree of robustness.

Table 5 Decrement of the correlation coefficient and the detection status after image scaling, with and without filtering prior to downsampling.

Scaling Ratio (R)		2	4	8	16
No Filtering	Decrement of ρ (%)	39	37	20	43
	Detection Status	Y	Y	Y	Y
With Filtering	Decrement of ρ (%)	65	64	65	77
	Detection Status	Y	Y	Y	N

The utilized VSS scheme is simple, if the computational complexity is considered. As a result, the proposed watermark insertion and detection schemes are fast and do not need a high amount of computational capabilities.

It must be again mentioned that selection of the parameter μ in (1) makes a tradeoff between imperceptibility and robustness of the watermarking system to different attacks. We chose μ equal to 2 in the simulations, where a higher value for μ (up to 5) could result in a higher robustness to the surveyed attacks, especially the JPEG compression process. Also, if the host image is present at the detector, an informed watermark detection scheme leads higher robustness to different watermarking attacks.

Conclusions

In this paper, we have proposed a new watermarking algorithm for digital images. The proposed scheme is simple and is based on the concept of visual cryptography, which is performed in the spatial domain of the host image. Digital mark to be embedded in the host image is one of the shares of the owner's mark (that can be a visible logo), whereas the other share is utilized as a detection key in the detection process. Watermark detection can be performed in both informed and blind structures, depending on the host image's presence at the detector. The detection algorithm relies on the fact that stacking images, containing corresponding shares of the logo, make a high correlation to the logo that is also detectable by the human eyes.

Acknowledgment

This project is partly supported by the Iran Telecommunication Research Center (ITRC).

References

[1] J. S. Pan, H. C. Huang and L. C. Jain, *Intelligent Watermarking Techniques*, World Scientific Publishing Co. Pte. Ltd., Singapore, 2004.

[2] M. Naor, and A. Shamir, "Visual Cryptography", *Advances in Cryptology – Eurocrypt'94 Proceeding, LNCS* Vol. 950, Springer-Verlag, 1995, pp. 1-12.

[3] M. Naor and A. Shamir, "Visual Cryptography II: Improving the Contrast Via the Cover Base", Cambridge Workshop on Protocols, 1996.

[4] A. Shamir, "How to Share a secret", *Communications of the ACM,* vol. 22, 1996, pp.612-613.

[5] G. Blakley, "Safeguarding cryptographic keys", in: *Proceedings of National Computer Conference*, 48, AFIPS Press, New York, 1979