A Novel Visual Secret Sharing Scheme without Image Size Expansion

Nazanin Askari, Cecilia Moloney, H.M. Heys
Electrical and Computer Engineering
Memorial University of Newfoundland
St. John's, Canada
Email: {nazanin.askari, cmoloney, hheys} @mun.ca

***Abstract*—Over the past few years, increasing concern about the privacy of information shared in computer systems has increased interest in data security. Visual cryptography is a secure secret sharing scheme that divides secret images into shares which on their own reveal no information of the original secret image. Recovery of the secret image can be performed by superimposing the shares. Hence, the process does not require any special software or hardware for cryptographic computations. However, loss of resolution and contrast, and also the image size expansion which results in the need for storage space, are resulting problems and have been the focus of many researchers. In this paper, we propose a novel visual secret sharing scheme without image size expansion. Compared to other schemes of visual cryptography, our perfectly secure scheme not only does not have pixel expansion, but also provides a high quality recovered image.**

I. Introduction

Increasing access to the Internet and information resources has a great impact on our everyday lives and is making humans more dependent on computer systems and networks. This dependency has brought many threats to information security. Thus, a number of studies have been done by researchers to protect secret information and data in a system. Cryptography is a well-known approach to protecting data information by writing it in secret codes and transmitting in a secure way. Visual cryptography is a cryptographic method that can be applied as a technique allowing multiple entities to share the information required to reveal a secret image.

The visual secret sharing (VSS) scheme, introduced by Naor and Shamir in 1994 [1], is a type of secret sharing scheme which can split the secret information into *n* shares and recover them by superimposing the shares. In VSS, the secret to be hidden is a black and white image and each share is comprised of groups of black and white subpixels used to recover a pixel of the secret image. It is assumed that a white pixel in a share is transparent and a black pixel is opaque so that superimposing shares can result in recovering the secret image. Since the shares are selected randomly, it is impossible to get any information about the secret images from shares individually or even subsets of the total shares. An advantage of VSS is that, unlike other cryptography techniques, this secret recovery does not need difficult computations. The secret information can easily be recovered with enough shares and requires human vision instead of special software or hardware devices.

Naor and Shamir proposed a (*k*, *n*) VSS scheme and assumed that the image or message is a collection of binary 1's and 0's displayed as black and white pixels respectively. According to their algorithm, the secret image is turned into *n* shares and the secret is revealed if any *k* of the shares are stacked together. So the image remains hidden if fewer than *k* shares are stacked together [2].

Image contrast and the number of subpixels of the shares are two main parameters in visual cryptography schemes [3]. The number of subpixels represents expansion of the image and should be as small as possible. In Naor and Shamir's visual secret sharing scheme (traditional VSS), each pixel in the secret image is mapped into an $m \times l$ block in each share, so the shortcoming of traditional VSS is that the shares and the recovered secret image are $m \times l$ times larger than the original secret image. Moreover, the recovered image is poor in contrast since only black pixels are perfectly reconstructed while all the white pixels turn into half black and half white pixels. Therefore the secret image can be hard to interpret.

In this paper we propose a novel visual secret sharing scheme without image size expansion. Compared to traditional VSS, the advantage of our scheme is that the secret image and all the share images have the same size. Compared to other VSS schemes that do not have expansion, our scheme results in a less noisy recovered image. Our method splits the secret image into the same size share images and recovers the secret image with good contrast by stacking them together with the logical XOR operation.

The rest of this paper is organized as follows: in Section 1, related work is reviewed. Section II introduces the proposed scheme in detail. The experimental results are demonstrated in Section III, and conclusions are presented in Section IV.

II. Related Work

The basic idea of visual cryptography can be illustrated with the traditional 2-out-of-2 scheme. In the (2, 2) scheme, every secret pixel of the image is converted into two share images and recovered by simply stacking two shares together. This is equivalent to using the OR operation between the shares. In this scheme, 4 subpixels are generated from each pixel of the secret image in a way that 2 subpixels are white and 2 are black. The subpixels for each share are

selected randomly. When a pixel from the original image is white, one of the six possible combination of patterns are randomly selected to encode the pixel into 2 shares. Table 1 demonstrates an example showing a part of Naor and Shamir's encoding process. It is easy to see that knowing only one share value does not reveal the other share nor any information of the secret image pixel. However superimposing both shares reveals the corresponding binary secret image.

Many studies have been done on applying visual cryptography to support grayscale and color images [4][5], while some researchers have focused on image size expansion and contrast degradation. Ito et al. [6] introduced a (*k*, *n*) VSS scheme which prevented size expansion by a probabilistic method. They represent each pixel in the secret image as a black or white pixel in the share images and the secret image can be revealed by stacking the shares together. In 2004, Yang et al. [7] proposed a similar probabilistic method called ProbVSS for binary and grayscale images. In [8], the authors presented a multiple image secret sharing without pixel expansion based on Chou's [9] method. In this scheme a block of four pixels are designed in a way that if a block has 2 to 4 black pixels, it is seen as a black block and if it contains 0 to 1 black pixels, it is known as white block. Chen et al. [10] proposed a multiple level visual secret sharing scheme (MLVSS). This scheme divides a secret image into several blocks called secret blocks and generates share blocks according to the density of the black pixels in a secret block.

Although these earlier works succeeded in preventing size expansion, they still have significant problems such as a leakage of the secret information [10] and poor quality of the reconstructed secret image [6][8].

TABLE I
A PART OF NAOR AND SHAMIR'S VSS SCHEME

Pixel	Probability	Share1	Share2	After Stacking
White	1/6			
	1/6			
Black	1/6			
	1/6			

III. PROPOSED SCHEME

A. Description of Scheme

To overcome the shortcomings of previous schemes, this section introduces a novel visual secret sharing scheme without pixel expansion. Our scheme is constructed as a (2, 2) scheme but can be easily extended to the schemes developed in earlier studies, such as the (*k*, *n*) VSS scheme. The block selection, mapping process and encoding process are the three steps in in the scheme and are described as follows.

At first, the image is divided into a number of blocks with 2×2 pixels. We call the block in the secret image a secret block, and the block in the share image a share block. In Table II, we define the name of each block model with each block model composed of four pixels. The next step is to categorize the secret blocks: if the secret block contains 1 black pixel (3 white pixels) or 3 black pixels (1 white pixel), they are randomly mapped to one of the 3 secret block candidates illustrated in Table III. Otherwise, no mapping process is required. In the encoding process, 8 patterns of share blocks are available for each secret block, with all the share blocks comprised of 0, 2, or 4 black pixels.

TABLE II
BLOCK MODELS OF THE IMAGE

bbbb	bbbw	bbwb	wbbb	bwbb	bbww	bwbw	wbwb
wwbb	bwwb	wbbw	wwbw	wwwb	bwww	wbww	wwww

TABLE III
ALL THE POSSIBLE PATTERNS

Secret Blocks	Candidate Blocks

Shares are created by randomly selecting one of the 8 possible share blocks as the first share block and then selecting the second share block in a way such that the reconstructed secret block is obtained by stacking the first and the second share together using the XOR operation (where the XOR of two pixels with the same colour is black and two pixels of different colour is white). As a result, the secret image, share images and reconstructed image have the same size and the recovered secret blocks differ only slightly from the original secret blocks; Thus the visual quality of the recovered images are slightly degraded over the original images.

B. Example

For the first step, assume that the *bbbw* case from Table II is selected as a secret block. As this block has 3 black pixels and one white pixel, one of the *bbww*, *bbbb* and *bwbw* models should be randomly selected from Table III. In the mapping processs, suppose that the *bbww* is selected as a secret block for the encoding process. According to Table IV, 8 possible

combinations of share blocks exist for share1 and share2 to produce the recovered secret blocks. One of the patterns will be selected randomly to create the shares for the secret block. As indicated in Table IV, stacking the two shared blocks with the XOR operation results the recovered secret block which is a *bbww* model.

C. Security and Recovered Image Quality

Security is the primary issue in visual secret sharing schemes. As shown in [1], the traditional (2, 2) scheme is perfectly secure since a forbidden set of participants cannot gain any information about the original secret image by inspecting one of the shares. Hence, share images should be indistinguishable in the sense that they contain the same share blocks with the same probability and frequency regardless of the distribution of pixels in the original secret image. In the encoding process of our proposed VSS scheme, each block of the secret image is randomly encoded into one of 8 pairs of share blocks. Since each share block is equally likely to occur for any original secret image block, no information of the secret image can be gained by examining only one share. Hence, our proposed scheme is secure.

Another important characteristic of VSS schemes is contrast [11]. Good contrast reflects the clear distinguishing of regions of white and black in an image. Traditional VSS, for example, is known to have poor contrast since the white pixels become blocks of subpixels that are only 50% white while being 50% black. For our proposed scheme, all blocks of pixels in the original secret image which are all white, all black, or 50% white / 50% black are all perfectly recovered when the shares are stacked, resulting in the preservation of the contrast in the original secret image. Only in the cases where blocks with one black or one white subpixel are mapped into blocks with 2 black and 2 white subpixels is there any effect on the contrast due to error. For such blocks, one of the 4 subpixels in the recovered block will be in error when compared to the original secret image, while the remaining 3 subpixels remain correct. In our proposed scheme, it can be shown that, assuming randomly distributed pixels blocks in the original secret image, 12.5% of the pixels in the recovered image are in error.

In order to explore the issue of contrast and pixels errors, an experiment was conducted on four different VSS schemes. In the experiment, we have computed the number of black and white pixels for a secret image (halftoned Lena) and the reconstructed image after applying different visual secret sharing schemes. As well, we have compared the pixels of the recovered image and the original image. The results are shown in Table V. Note that: 1) the total number of pixels in the recovered image in the traditional VSS scheme is four times the original image, reflective of the expansive nature of the scheme; 2) the fraction of black pixels is substantially different from the original image for all schemes except in our proposed scheme, indicating significant degradations in contrasts for these schemes; and 3) the fraction of pixels in error in the recovered secret image is smallest for our proposed scheme, supporting the argument that our scheme has low noise compared to other schemes.

IV. Experimental Results

In order to check the feasibility of the proposed scheme and also compare the results in our approach with previous approaches, we have implemented the traditional VSS scheme, Chen's MLVSS scheme, Chou's scheme and our proposed scheme. Figure 1(a) and 1(b) show two images used as secret images in our experiment, one grayscale known as Lena and a binary image of a fingerprint, with the size of 512×512 pixels and 784×1132 pixels respectively. For the grayscale image, digital halftoning (using the Floyd-Steinberg algorithm) is used for the purpose of converting the grayscale images into a black and white image [12]. Once we have a binary image, then the visual cryptography technique can be applied.

Figure 1(a) is the Lena image after halftoning and Figure 1(b) is the original binary image of the fingerprint. Figure 1(c) and (d) are the results obtained by applying Naor and Shamir's VSS on these two secret images. As it is expected, the expansion factor is 4, so the recovered image sizes are 1024×1024 and 1568×2264, respectively. Since the white pixels are not fully recovered, the superimposed images look darker and covered by random noise like a mist that can affects the image quality. Note that the recovered images from this scheme have been scaled down to the same size as other images for printing purposes. Figure 1(e) and (f) are the results when MLVSS scheme is applied. Since each secret block that consists of 3 or 4 white pixels appears as a half white and half black secret blocks, some information may be lost in the reconstructed secret images. Moreover, we have discovered this scheme reveals some secret information on shares and is not secure. Figure 1(g) and (h) demonstrate the results of Chou's visual secret sharing scheme. Although this is a non-expansion scheme, compared to the original images, the quality of the recovered images is poor due to the low contrast between black and white pixels causing a darkening effect. This means that the pixels which appeared black on the shares are outnumber the white ones. The last experiment is applied using novel visual secret sharing scheme without size expansion as seen in Figure 1(i) and (j). Note the significant improvement in the image quality compared to the other 2 non-expansion schemes. Details incuding eyes, hat, edges, background and fingerprint minutia of the images are recovered more clearly and are visually similar to the original images in our construction. Measured values from Table V provide strong evidence to support the correctness of our visual experiment.

V. Conclusion

The traditional visual secret sharing scheme is a perfectly secure method that encodes a secret image into random shares and recovers the image by superimposing the shares. However, this scheme leads to the degradation in the quality of the recovered images and in image size expansion. In this paper, we have extended traditional visual secret sharing by

TABLE IV
AN EXAMPLE OF OUR ENCODING PROCESS

Secret Block	Probability	Share1	Share2	After Stacking
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			

TABLE V
COMPARISION OF RECOVERED IMAGE CHARACTERISTICS

Halftone Lena	Total pixels	Fraction of black	Pixel error
Secret image	262144	0.5212	-
Traditional VSS	1048576	0.7518	N/A
MLVSS scheme	262144	0.4044	19.94%
Chou's scheme	262144	0.8730	41.45%
Proposed scheme	262144	0.5065	13.86%

introducing a novel (2, 2)VSS scheme without size expansion.

The principle of this scheme is to encode a secret block with four pixels into two share blocks according to the number and distribution of black and white pixels, thereby allowing the secret image to be clearly restored by using XOR operation. Our novel scheme can be applied on both binary and halftone images and does not increase the number of pixels required to represent the shares or the recovered image. Although the scheme introduces some noise into the recovered image, the recovered image is substantially clearer than in other proposed non-expansion schemes.

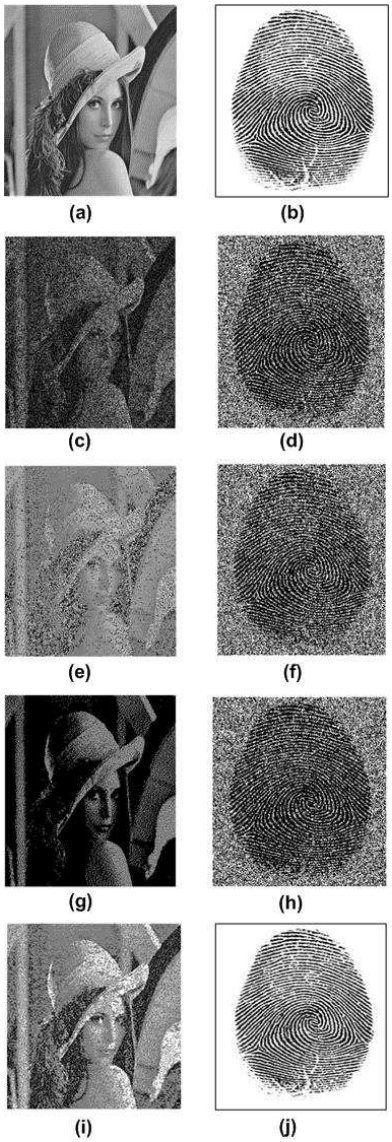

Fig. 1. Comparision of Experimental Results of proposed scheme with other schermes: (a) halftone Lena [13]; (b) binary fingerprint [14]; (c),(d) recovered images of Naor and Shamir's scheme; (e),(f) recovered images of Chen's scheme; (g),(h) recovered images of Chou's scheme; (i),(j) recovered images of our proposed scheme.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography", *in Eurocrypt'94 Proceeding*, LNCS, vol. 950, Spring-Verlag, pp. 1-12, 1995.

[2] M. Naor and A. Shamir, "Visual cryptography:Improving the contrast via the cover base" *IACR Eprint archive*, 1996.

[3] N. Askari and C. Moloney and H.M. Heys, "Application of visual cryptography to biometric authentication", *Newfoundland Electrical and Computer Engineering Conference*, 2011.

[4] C. Blundo and A. De Santis and M. Naor, "Visual cryptography for grey level image", *Information Processing Letters*, vol. 75, pp. 255-259, 2000.

[5] Y.C. Hou, "Visual cryptography for color images", *Pattern Recognition*, vol. 36, pp. 1619-1622, 2003.

[6] R. Ito and H. Kuwakado and H. Tanaka, "Image size invariant visual cryptography", *IEICE Trans.Fundamentals*, vol. E82-A, no. 10, pp. 2172-2177, 1999.

[7] C.N. Yang, "New visual secret sharing schemes using probabilistic method", *Pattern Recognition*, pp. 481-494, 2004.

[8] C.L. Wang and C.T. Wang and M.L. Chiang, "The image multiple sharing schemes without pixel expansion", *International Conference on Machine Learning and Cybernetics*, Guilin, 2011.

[9] C.L. Chou,"A watermarking technique based on non-expansible visual cryptography", Thesis, Department of Information Management, National Univercity, Taiwan, 2002

[10] Y.F. Chen et al, "A multiple-level visual secret-sharing scheme without image size expansion", *Information Sciences*, vol. 177, no. 21, pp. 4696-4710, 2007.

[11] C. Blundo and A. De Santis and D.R. Stinson, "On the contrast in visual cryptography schemes", *Journal of cryptography*, vol. 12, pp. 261-289, 1996.

[12] Z. Zhouand and G. R. Arce and G. Di Crescenzo, "Halftone visual cryptography" *IEEE Trans. Image Process*, vol. 15, no. 8, pp. 2441-2453, 2006.

[13] http://en.pudn.com/downloads89/sourcecode/others/detail340374

[14] http://caro.officialpsds.com/Fingerprint-PSD16620.html