The 13th IPPR Conference on
Computer Vision, Graphics and Image Processing

Visual Cryptography for Gray-level Images

Chang-Chou Lin and Wen-Hsiang Tsai

Department of Computer and Information Science
National Chiao Tung University, Hsinchu, Taiwan 300, Republic of China
Fax: 886-3-5727382
E-mail: whtsai@cis.nctu.edu.tw

Abstract A (k,n)-threshold visual cryptography scheme is proposed to encode a secret image into n shadow images, where any k or more of them can visually recover the secret image, but any k-1 of them gain no information about it. The decoding of visual cryptography schemes, which differs from the traditional secret sharing, is without any knowledge of cryptography and without performing any cryptographic computations. Otherwise, it can be decoded directly by the human visual system. Previous efforts in this topic are almost restricted in binary images, which seems to be insufficient in many kinds of applications. In this paper, a new visual cryptography scheme for gray-level images is proposed. At the same time, some comparisons with the previously proposed method are also made. Then we show some experimental results to prove our proposed method is feasible. Finally, we do some extensions to show its practicability.

Keywords: visual cryptography; shadow images; secret sharing; dithering

1. Introduction

Since Naor and Shamir proposed the idea of visual cryptography [1], this topic has attracted wide attention and various extensions has been proposed. A (k,n)-threshold visual cryptography scheme is a method to encode a secret image into n shadow images called shares, where any k or more of them can be combined visually to recover the secret image, but any k-1 or fewer of them gain no information about it. The visual recovery process consists of xeroxing the shares onto transparencies, and then stacking them. This basic model has been applied to many applications, which include information hiding [1], general access structures [2, 3], visual authentication and identification[4], and so on. Unfortunately, these applications are all restricted to the use of binary images as input due to the nature of the model. This drastically decreases the applicability of visual cryptography because binary images are usually restricted to represent text-like messages. The characteristics of images for showing object shapes, positions, and brightness thus can not be utilized. And at the age of Internet, data of image form gradually replace data of text form. It is not sufficient that visual cryptography schemes can only deal with binary images. Verheul and van Tilborg [5] first tried to extend visual cryptography into gray-level images. The details of their scheme will be described in Section 2. They used gray levels existing in the original images to form shares instead of using black and white values only. But in ordinary situations, their method has the disadvantage of resolution reduction in the recovered image. So in this paper, we propose a new way of cryptography for gray-level images. Our method utilizes the techniques of digital image halftoning to transform a gray-level image into an approximate binary image. Then the visual cryptography schemes used for binary images are applied. Some advantages of the proposed approach are that it can inherit any developed technique for binary images and that it has less reduction of resolution. We also give an example to prove its practicability.

The remainder of this paper is organized as follows. In Section 2, we briefly review the (k,n)-threshold visual cryptography scheme for binary images, which is the basis of our approach. In Section 3, we introduce the method proposed in [5] and analyze it. In Section 4, the details of our approach based on the image halftoning technique are described. Some experimental results are shown in Section 5. A possible application is proposed in Section 6. Finally, some conclusions are given in Section 7.

2. Review of (k,n)-Threshold Visual Cryptography

We review the (k,n)-threshold visual cryptography scheme for binary images proposed in [1] first. Before an image is encrypted, each pixel in the encoded image is expanded into b subpixels and then all subpixels are assigned proper values (0 for white and 1 for black) for the corresponding shares. To do this systematically, two $n \times b$ basis matrices C_0 and C_1 are defined, each of whose rows represents the subpixel values of each share. To clarify this usage, we demonstrate the case of (2,2)-threshold visual cryptography. First, define $C_0 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ and $C_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. To encrypt a white pixel in the original image, we give *share*1 the first row of C_0 to assign its subpixel values and *share*2 the second row of C_0. Their visual patterns are depicted in Figure 1 (a) and (b). The result of stacking is shown in Figure 1 (c). Correspondingly, we use C_1 to encrypt a black pixel and the two shares and stacking result is shown in Figure 2. We define the term "contrast" to represent the difference between a black and a white pixel in the decoded image. The larger the measure is, the better the performance is. In the meantime, to avoid the adversary to find out the regularity of the patterns (e.g., the

pattern 0101 implies black in the original image), we must equalize the probability of appearance of each pattern. Consequently, we permute the columns of each basis matrix to randomize the patterns pixel by pixel before we assign the values of subpixels according to the basis matrices. We demonstrate an example of basis matrices for (2,2)-threshold visual cryptography in Figure 3. Figure 3(a) shows all the permutations of C_0 and Figure 3(b) the corresponding permutations of C_1. No matter how they permute, the result of stacking is consistent in contrast. In this example, the decoded white pixel is composed with two white subpixels and two black subpixels while the decoded black pixel is composed with four black subpixels. Figure 4 represents an example of (2,2)-threshold visual cryptography. The general construction of basis matrices for (k,n)-threshold visual cryptography has been deduced in [1] and refined in [2, 3, 5].

(a) (b) (c)

Fig. 1: (a) The visual pattern of *share*1. (b) The visual pattern of *share*2.(c) Decoding of a white pixel.

(a) (b) (c)

Fig. 2: (a) The visual pattern of *share*1. (b) The visual pattern of *share*2.(c) Decoding of a black pixel.

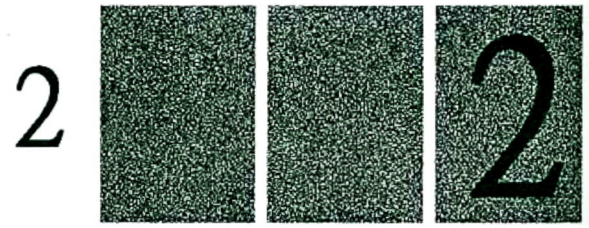
$$\begin{pmatrix}1&0&1&0\\1&0&1&0\end{pmatrix}\begin{pmatrix}1&0&0&1\\1&0&0&1\end{pmatrix}\begin{pmatrix}1&1&0&0\\1&1&0&0\end{pmatrix}$$
$$\begin{pmatrix}0&1&1&0\\0&1&1&0\end{pmatrix}\begin{pmatrix}0&1&0&1\\0&1&0&1\end{pmatrix}\begin{pmatrix}0&0&1&1\\0&0&1&1\end{pmatrix}$$

(a)

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

(b)

Fig. 3: (a) All the permutation of C_0. (b) All the permutation of C_1.



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

Fig. 4: an example of $(2,2)$-threshold visual cryptography (a) The original image. (b) The *share*1. (c) The *share*2. (d) The decoded image.

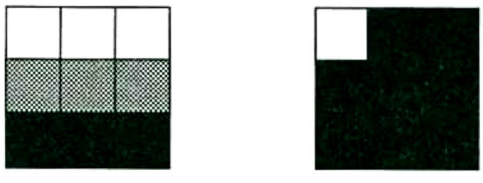
3. Related works

Topics about visual cryptography for gray-level images are seldom discussed. Verheul and van Tilborg [5] described a method to encrypt gray-level images. We review their method briefly here. For an image with c gray-levels, expand first a pixel into b subpixels. Each subpixel may take one of gray-levels 0, 1, ..., c-1. After all shares are stacked, gray-level i is revealed if corresponding subpixels of all shares are of gray-level i; otherwise, the level of black is revealed. The general construction of (k,n)-threshold visual cryptography is proposed. As an illustration, we describe the case of a (3,3)-threshold scheme. If there are three gray-levels, we construct three basis matrices belonging to gray-levels 0, 1, 2, respectively, in the following.

$$C_0=\begin{pmatrix}0&0&0&1&1&1&2&2&2\\0&1&2&0&1&2&0&1&2\\0&1&2&1&2&0&2&0&1\end{pmatrix},C_1=\begin{pmatrix}0&0&0&1&1&1&2&2&2\\0&1&2&0&1&2&0&1&2\\2&0&1&0&1&2&1&2&0\end{pmatrix},$$
$$C_2=\begin{pmatrix}0&0&0&1&1&1&2&2&2\\0&1&2&0&1&2&0&1&2\\1&2&0&2&0&1&0&1&2\end{pmatrix}.$$

To encrypt a pixel of gray-level 0, we give *share*1 the first row of C_0 to assign its subpixel values, *share*2 the second row of C_0, and *share*3 the third row. Their visual patterns and stacking result are depicted in Figure 5. We can see that the subpixel of all these three shares in the top-left corner is of gray-level 0, which is the gray-level value of the encoded pixel, and this does not hold for all other subpixels. The stacking result is gray-level 0 in the top-left corner and gray-level black in the other positions.

The most serious disadvantage of this proposed scheme is the reduction of resolution and the increase of image size at the same time. If we want to encrypt an image with c gray-levels using a (k,n)-threshold visual cryptography scheme, we have a resolution reduction and size increase deduced in [5]. When $c > n$, we have a resolution decrease with a factor c^{k-1} at least.



(a) (b)

Fig. 5: (a) The visual pattern of *share*1. (b) The visual pattern of *share*2.(c) The visual pattern of *share*3. (d) Decoding of a pixel with gray-level 0.

4. Proposed scheme

With the (k,n)-threshold visual cryptography scheme for binary images proposed in [1], the reduction of resolution is with a factor $n^k \times 2^{k-1}$, which is comparatively smaller than Verheul and van Tilborg's scheme [5] in ordinary situations. Here ordinary situations mean those with $\frac{1}{\frac{1}{n^{k-1}}} \times \frac{c}{2} \geq n$. Therefore, if we convert a gray-level image into an approximate binary image with the same size first and then apply the scheme proposed in [1], we can get less reduction of resolution than Verheul and van Tilborg's scheme. Ordered dithering is such a technique to fast and parallelizably transform a gray-level image into a binary image. Space-filling curve ordered dithering (SFCOD) [6] is an algorithm that can significantly improve ordered dithering, in the aspect of keeping image quality by determining dither thresholds along a space-filling curve. Let I be an $n \times n$ gray image, H the corresponding halftoned binary image, $C(n,n)$ the map of a traversal order numbers of the pixels of the image I along a space-filling curve over I (an example is shown in Figure 6, where the numbers in the grid are traversal order numbers), and $A(k)$ a space-filling curve dither array (i.e., a permutation of 0, 1, 2, ..., k-1), where k is the length of the dither array. Then the method SFCOD can be formulated as the following algorithm:

```
PROCEDURE SFCOD(C, A, k, I, H)
BEGIN
FOR i = 0 TO n-1 DO
  FOR j = 0 TO n-1 DO
    IF I(i,j) ≧ (A(C(i MOD k, j MOD k)) + 0.5)/k
    THEN H(i,j) = 1 ELSE H(i,j) = 0;
END
```

This algorithm can be regarded as using an $a \times a$ mask like Figure 6 to stack on the image with no overlapping and assign each pixel a value equivalent to the corresponding value on the mask. Then we input the assigned value of each pixel into the dither array $A(k)$ and get a mapped value. Finally, we use the mapped values as the thresholding values to binarize the original gray images.

After we transform the original gray image into an approximate binary image, we apply the visual cryptography schemes proposed in [1]. Then we get a result of (k,n)-threshold visual cryptography for gray-level images.

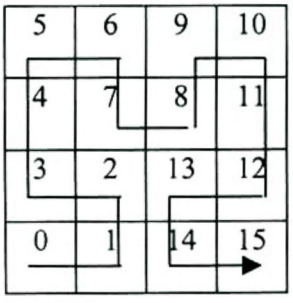


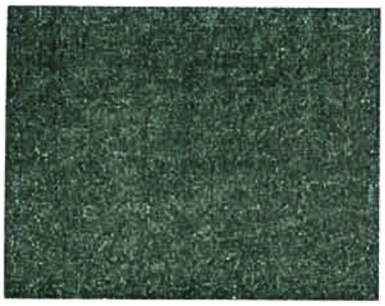
Fig. 6. Traversal order determined by a space-filling curve

5. Experimental results

In this section, three gray images are used to evaluate the performance of our proposed scheme. The reason of choosing these images is that they contain sufficient image details and gray-levels. Such images are good for evaluating the effect of halftoning and visual cryptography. Figure 7 shows an original gray image with 16 gray-levels. The result of applying the SFCOD with the parameters suggested in [6], where $A(i) = i$, $i = 0, 1, 2, \ldots, k\text{-}1$, $k = 16$, and $C(i,j)$ as shown in Figure 6, is shown in Figure 8. Then we perform the (2,2)-threshold visual cryptography scheme. The corresponding two shares are shown in Figure 9. The result of decoding the two shares is shown in Figure 10. We observe that most details can be revealed in the image of Figure 10 and the size of the image is just 1/4 of the image used by Verheul and van Tilborg's scheme. Figure 11 and Figure 15 are two other gray images with 8 and 16 gray-levels. The results of using the SFCOD with the same parameters as the first experiment are shown in Figure 12 and Figure 16, respectively. Their corresponding two shares are shown in Figure 13 and Figure 17, respectively. The results of decoding the two shares are shown in Figure 14 and Figure 18, respectively. We observe that the two results, like the result of the first experiment, are also acceptable and with smaller size than the results proposed by Verheul and van Tilborg's scheme.

Fig. 7. The original image.

Fig. 8. The image after using SFCOD.



(a)

(b)

Fig. 9: (a) The *share*1. (b) The *share*2.

Fig. 10. The decoded image.

Fig. 11. The original image.

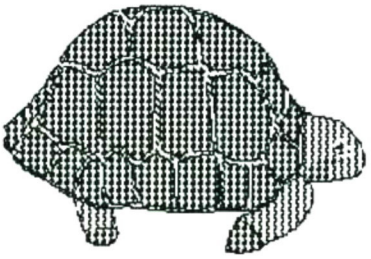
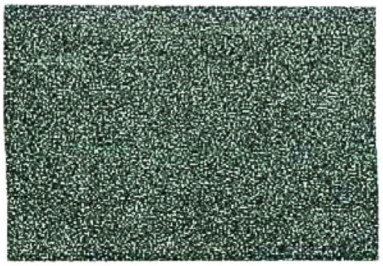
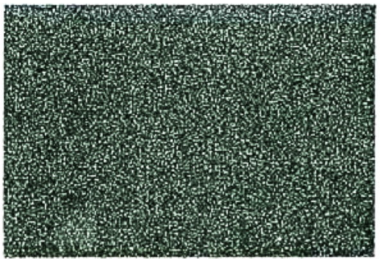


Fig. 12. The image after using SFCOD.



(a)



(b)

Fig. 13: (a) The *share*1. (b) The *share*2.

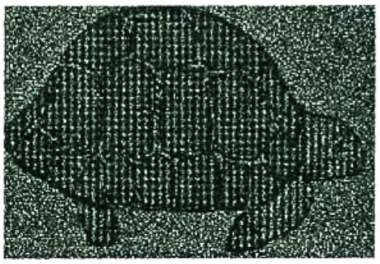
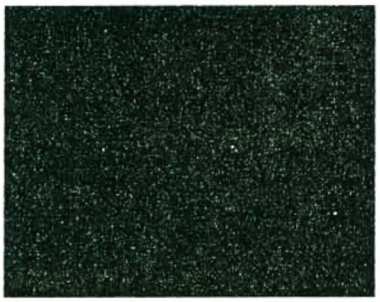


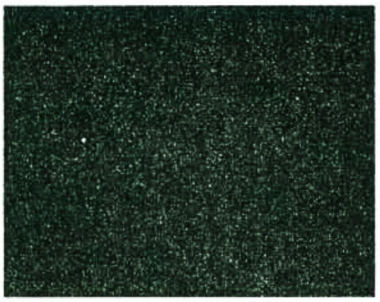
Fig. 14. The decoded image.

Fig. 15. The original image.

Fig. 16. The image after using SFCOD.



(a)



(b)

Fig. 17: (a) The *share*1. (b) The *share*2.

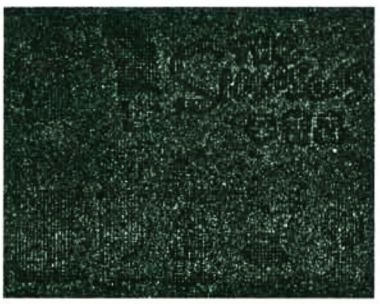


Fig. 18. The decoded image.

6. An application

Imagine an authentication system. Instead of using existing credit cards, each user of the system has a card with an image which looks meaningless. When he goes shopping and pays a bill, he gives the clerk his card. Then the clerk puts the card into a small machine and checks the similarity between an image revealed by the system and the appearance of the customer to authenticate the customer. Visual cryptography for gray-level images can be applied to implement this system. First, we encrypt the portrait of the customer using the (2,2)-threshold scheme. We make one of the two shares, which is an image and assumes the role of a public key in cryptography, to be the same for each customer. The other share, also an image, is attached in the customer's card to act as the corresponding secret key. Each shop owns the public key and when customers pay a bill, the clerk stacks the two shares to obtain the encoded image, which must be similar with the appearance of the customer, to accomplish the anthentication work. This scheme possesses several advantages, compared with other authentication schemes. Compared with passwords, it is more confidential. A 512× 512 binary image has 2^{262144} decoding combinations, so the probability to obtain a correct guess of a person's secret key is very low. Compared with recognition of fingerprints and signatures, this scheme does not need complicated computation and has higher recognition rates. Finally, the system may be implemented as a small device and this makes this scheme even more feasible.

Authentication is just one of the possible applications of visual cryptography schemes. With our proposed scheme, it is convenient to extend various applications of visual cryptography developed for binary images to gray-level images. This characteristic enlarges the applicability of our scheme.

7. Conclusions

In this study, we have developed a scheme with the capability of visual cryptography for gray-level images. Extension of visual cryptography from binary images to gray-level ones is useful for wider applications. The proposed approach for gray images is to convert the original gray images into an approximate binary image first with the dithering technique, and then apply the visual cryptography method for binary images to the resulting image. This scheme possesses the advantage of inheriting any developed techniques for binary images and having less reduction of resolution in ordinary situations. Some experiments are used to evaluate the effect of our proposed method. The results can reveal most details of the original images and have less image resolution reduction. These results prove that our approach is feasible. A possible application is also proposed in this study. An authentication system based on our proposed method is superior to some existing systems in many aspects, which include confidence, low complexity, and higher recognition rates. For further research, efficient visual cryptography for color images is the next goal to develop.

References

[1] M. Naor and A. Shamir, "Visual Cryptography," *Advances in Cryptology --- EUROCRYPT'94*, vol. 950 of Lecture Notes in Computer Science, pp. 1-12, 1995.

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual Cryptography for General Access Structures," *Information and Computation*, vol. 129,

pp. 86-106, 1996.

[3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Constructions and bounds for Visual Cryptography," *23rd International Colloquium on Automata, Languages and Programming*, vol. 1099 of Lecture Notes in Computer Science, pp. 416-428, 1996.

[4] M. Naor and B. Pinkas, "Visual Authentication and Identification," *Advances in Cryptology --- CRYPTO'97*, vol. 1294 of Lecture Notes in Computer Science, pp. 322-336, 1997.

[5] E.R. Verheul and H.C.A. van Tilborg, "Construction and Properties of k out of n visual secret sharing schemes," *Designs, Codes, and Cryptography*, vol. 11, pp. 179-196, 1997.

[6] Y. Zhang, "Space-filling Curve Ordered Dither," *Computer & Graphics*, vol. 22, no. 4, pp. 559-563, 1998.