

# LEARNING WITH FUN

## *An Application of Visual Cryptography*

Young-Chang Hou and Zen-Yu Quan

*Department of Information Management, Tamkang University  
151 Ying-Chuan Road, Tamshui, Taipei County, Taiwan 251, R.O.C., Taiwan*

Keywords: Visual Cryptography, Information Sharing, Computer-Aided Instruction.

Abstract: Visual Cryptography, an emerging cryptography technology, exploits the characteristics of human visual system to decrypt the overlapping images without mass and complicated computations. Almost all the related studies of visual cryptography were concentrated on the topics of the information security. In this paper, we propose to use the technique of visual cryptography to teach young kids counting. It can stimulate the curiosity of the kids and increase the fun of learning.

## 1 INTRODUCTION

It is not uncommon to transfer multimedia data via the Internet recently. With the coming age of Electronic Commerce, it is urgent to solve the problem of how to ensure the information safety in the open network environment. The encrypting technologies of the traditional cryptography are usually used to protect the information content. The data become disordered after encrypting and then are recovered by the correct key. After encrypting, the content can hardly be recognized even though unauthorized persons steal the data. Hence it can achieve the goal of protecting information safety.

Naor and Shamir proposed a new cryptography area, Visual Cryptography, in 1995 (Naor and Shamir, 1995). The most notable feature is that it can recover the secret image without any computing. It exploits the human visual system to read the secret message from the overlapping shares and thus overcome the disadvantage of huge and complex computation in the traditional cryptography. The  $(k, n)$ -threshold scheme (Naor and Shamir, 1995, 1996) makes the application of visual cryptography more flexible. The manager can first produce  $n$  copies of transparency drawn from one secret image for his members. Each one holds only one transparency. If any  $t$  of them stacks their transparencies together, the content of the secret image will show up. If the number of transparencies is less than  $t$ , the content of the secret image still keeps hidden.

There have been many published studies (Ateniese et al, 1996, 2001, Blundo et al, 1996, Naor and Shamir, 1995, 1996) of visual cryptography. All of them, however, concentrated on discussing the topics about information security. In this paper, we use the technology of visual cryptography to generate shares with numbers on them. When playing with kids, we can show them two shares, and ask for the answer. The correct answer will show automatically when you superimpose one share over another. This can stimulate the curiosity of the kids and increase the fun of learning.

## 2 VISUAL CRYPTOGRAPHY

### 2.1 Basic Theorem of Visual Cryptography

The output media of visual cryptography is transparency, so the white pixels are treated as transparent. The most common way of black-and-white visual cryptography is to decompose every pixel in the secret image into a  $2 \times 2$  block on the two transparencies according to the rules in the Table 1. When the pixel is white (black), randomly choose one of the first (last) two rows of the Table 1 to form the corresponding content of the block on the two transparencies.

As to the security of the shares, there are six possible patterns of every block on the transparency,

Table 1: Sharing and stacking scheme of black and white pixels.

Secret image	Share1	Share2	Stacked image
□			
■			

and they are chosen randomly, so the secret image cannot be identified from a single transparency. Because every block on the transparencies consist of two white pixels and two black pixels, no matter it comes from white pixel or black pixel of the secret image, there is no clue of revealing the secret image on the shares.

When stacking two transparencies, the block corresponding to the black pixels in the secret image will be full black, and that corresponding to the white pixels will be half-black-and-half-white, which can be seen as gray pixel (50% black). This gives enough contrast to recognize the secret information on the stacked shares by human eyes. Take Figure 1 for example, a secret image with the words of “淡江資管” are decomposed into two shares. When we stack them together, we can get the reconstructed image. Though the contrast of the stacked image is degraded to 50%, human eyes can still identify the content of the secret image easily.

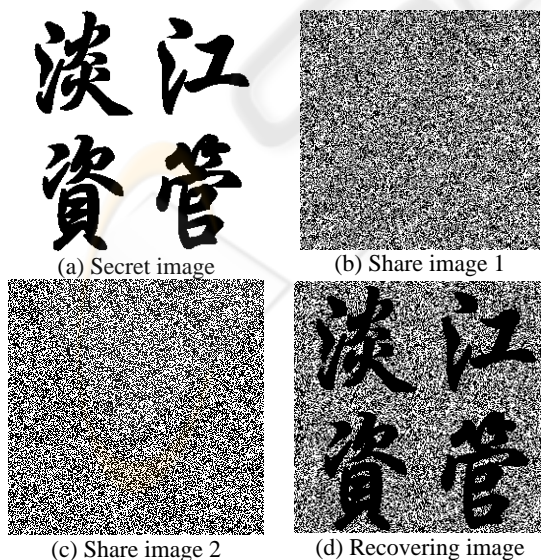


Figure 1: Visual cryptography for “淡江資管”.

## 2.2 Visual Cryptography for Grey-level and Colour Images

Every kind of the media has different ways to represent the colour level of an image according to its physical characteristic. The general printer, such as dot matrix printers, laser printers, or jet printers etc., can only control a single pixel to be printed (black pixel) or not to be printed (white pixel). Hence one way to represent the gray level of an image is to control the density of the printed dots; for example, the printed dots of the bright part are sparse, but those of the dark part are dense. Such method that uses the density of the net dots to simulate the gray level is called “Halftone”. Hou might be the first researcher to use the concepts of colour decomposition and halftoning technology to produce shares needed by visual cryptography for both grey-level and colour images (Hou, 2003). By means of halftone, we can transform an image with gray level into a binary image (Figure 2). Because human eyes cannot identify too tiny printed dots and will mix with the nearby dots, though the transformed image has only two colours - black and white, we can simulate different gray levels through the density of printed dots.

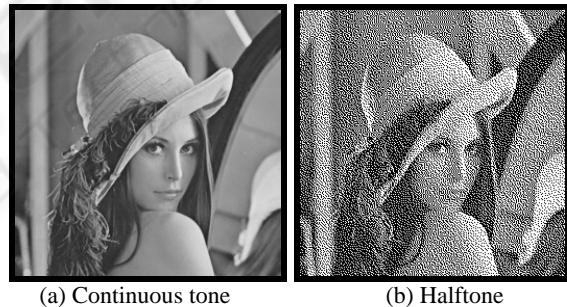


Figure 2: Grey-level image and black-and-white image.





















The transformed halftone image (Figure 2b) is a black-and-white image, such image format is very suitable to apply the traditional visual cryptography method to generate the shares (Figure 3). Secret image Figure 3c is hidden into Figure 3a and 3b.

As for colour image, most colour printers use cyan, magenta and yellow inks to display colour. These three components of a colour image can be decomposed to form three monochromatic images. This monochromatic image is like a single gray-level image which can be handled by the above mentioned method. Each participant will get a colour share which is composed of cyan, magenta and yellow monochromatic shares. After stacking these shares, colour secret image can be revealed.

### 2.3 Extended Scheme of Visual Cryptography

The shares generated by visual cryptography (Naor and Shamir, 1995) are noise-like and meaningless. There is no clue of the secret image on the share. It meets the requirement of security. But the meaningless shares will cause adversary's attention and invite the illicit attempts. Ateniese (Ateniese et al, 2001) proposed an extended visual cryptography scheme (Table 2) to hide a secret image into two meaningful sharing transparencies. When stacking the transparencies generated from Table 2 together, we will get the secret message with no trace of the original cover image on the shares.

Table 2: Sharing and stacking scheme of black and white pixels.

Secret image	Share1	Share2	Stacked image
white (W) 	(W) 	(W) 	
	(W) 	(B) 	
	(B) 	(W) 	
	(B) 	(B) 	
Black (B) 	(W) 	(W) 	
	(W) 	(B) 	
	(B) 	(W) 	
	(B) 	(B) 	

According to Table 2, blocks with 2 white pixels and 2 black pixels on the share image represent a white pixel of the cover image. Blocks with 1 white pixel and 3 black pixels on the share image represent a black pixel of the cover image. There is 25% contrast between black and white pixels on the sharing transparencies. Hence, we can disclose the content of the cover image.

When the pixel of the secret image is white (black), choose one of the first (last) four rows of the Table 2, depending on the corresponding colours on the cover images, to form the content of the block on the two transparencies. As to the security, there are six possible white patterns and four possible black patterns to be chosen as the content of every block in the transparency, and they are determined randomly. Therefore, to have share1 or share2 alone, there is no

clue of revealing the secret image on the sharing transparencies.

When stacking two transparencies, the block corresponding to the black pixel in the secret image will be full black, and those that corresponding to the white pixel in the secret image will be 3-black-and-1-white, which can be seen as gray pixel (75% black). There is also 25% contrast between black and white pixels on the stacked transparencies. Hence, the content of the secret image can be disclosed easily by our visual system.

Take three colour-level images for example, Figures 3d and 3e are two meaningful sharing transparencies produced by using the sharing scheme of the Table 2. Figure 3f is the reconstructed secret image produced by superimposing Figure 3d and 3e. In other words, secret image Figure 3f is hidden into Figure 3d and 3e or Figure 3d and 3e cover secret image Figure 3f. Though the contrast of the sharing images and stacked secret image are degraded to 50% and 75% respectively, human eyes can still identify the content of the cover images and the secret image easily

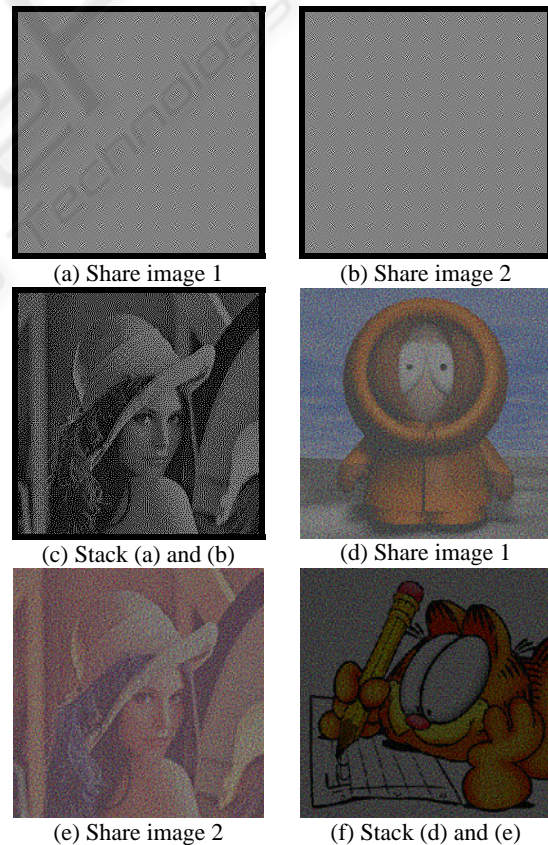


Figure 3: Visual cryptography with meaningless and meaningful shares.

### 3 POSSIBLE SCENARIOS IN EDUCATION

Teaching of counting has created significant difficulties to both teachers and young kids. Class size is one of the major barriers to effective instruction. As the lowering cost of the computer hardware and widely spread of the Internet, pupils might have their own laptop personal computers for homework and instruction, especially in some highly computerized cities or countries. A well-designed pedagogy, such as Computer-Assisted Instruction (CAI), can make the instruction most effective.

In the information security field, visual cryptography is used as one of the technologies to implement the topics about watermarking, information hiding and information sharing. It can generate shares, stack them together, the secret information will automatically show up and recognize by human eyes. Therefore, it is a good tool to be used to practice counting for kids.

For example, the sum of two numbers can be treated as a secret number, the generated share 1 and share 2 can be treated as the summand and the addend. When kids are doing their counting exercises, they can select one number share, dragging it to another share, stacking them together, magically, the number on these two meaningful shares disappears, the correct answer shows up on the stacked shares. When you shift these two shares a little bit, pixels are not stacked properly, the answer will fade away. It can stimulate the curiosity of the kids and increase the fun of learning.

Figure 4 and Figure 5 are examples of the sum and the product of two numbers, respectively.

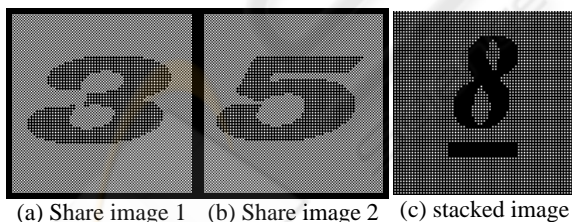


Figure 4: Sum of 3 and 5.

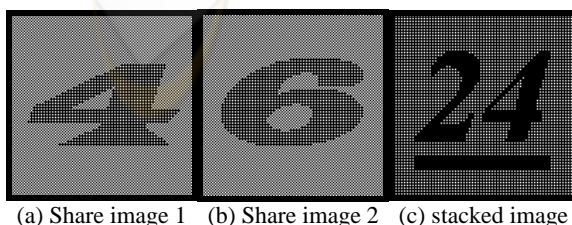


Figure 5: Product of 4 and 6.

A set of programming exercises have been designed with help of computer assisted instruction. The demo system can pose questions to students, return feedbacks, and select additional questions based on the kids' responses. By using this system, kids can practice counting and learn the basic principle of the visual cryptography.

### 4 CONCLUSIONS

Visual Cryptography exploits the characteristics of human visual system to decrypt the overlapping images without mass and complicated computations. Traditionally, visual cryptography is used as one of the technologies to implement the topics about watermarking, information hiding and information sharing. In this paper, we propose a teaching system which uses the technique of visual cryptography to teach young kids counting. The technology of visual cryptography can be used to generate numbers, stack them together, the result will automatically show up and recognize by human eyes. It can stimulate the curiosity of the kids and increase the fun of learning.

### ACKNOWLEDGEMENTS

This work was supported in part by a grant from National Science Council of the Republic of China under the project NSC96-2221-E-032-027.

### REFERENCES

- Ateniase, G., C. Blundo, A. De Santis, and D. R. Stinson, 1996, "Visual Cryptography for General Access Structures", *Information and Computation*, 129, pp.86-106.
- Ateniase, G., C. Blundo, A. De Santis, and D. R. Stinson, 2001, "Extended Capabilities for Visual Cryptography," *Theoretical Computer Science*, Vol. 250, pp. 134-161.
- Blundo, C. A. De Santis and D. R. Stinson, "On the Contrast in Visual Cryptography schemes", <ftp://theory.lcs.mit.edu/pub/typto1/96-13.ps>.
- Y.C. Hou, 2003, "Visual Cryptography for Color Images," *Pattern Recognition*, Vol. 36, No. 7, pp. 1619-1629
- Naor, M. and A. Shamir, 1995, "Visual Cryptography", *Advances in Cryptology: Eurpocrypt'94*, Springer-Verlag, Berlin, pp. 1-12.
- Naor, M. and A. Shamir, 1996, "Visual Cryptography II: Improving the Contrast Via the Cover Base". *Theory of Cryptography Library Report 96-07*, <ftp://theory.lcs.mit.edu.tw/pub/cryptol/96-07.ps>.