

Sharing visual multi-secrets using circle shares

Hsien-Chu Wu^{a,*}, Chin-Chen Chang^b

^a*Department of Information Management, National Taichung Institute of Technology, 129 Sec. 3, San-min Road, Taichung, Taiwan 404, ROC*

^b*Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan 621, ROC*

Received 28 June 2004; received in revised form 7 December 2004; accepted 14 December 2004

Available online 13 January 2005

Abstract

Traditional visual cryptography technique has provided sufficient security to fulfill the purpose of protecting confidential messages. In current technology, the same set of shares can be embedded with many sets of secret messages after one of the shares is rotated at different degrees. However, the used share is rectangle so that only four kinds of angle variation exist when stacking shares. Thus, when intending to embed many sets of confidential messages by using these shares, the angle variation of rotating the shares is limited. This paper proposes an improved (2, 2)-visual secret sharing scheme that adapts circular shares to deal with the limitation of rotating angles in traditional visual cryptography. The primary property of the proposed technique is that two sets of confidential messages can be embedded in the same shares. After rotating one of the shares to a certain degree and stacking it with another share, the content of the second confidential message can be obtained. The share used in this technique is circular, where confidential data can be embedded in various different angle conditions. Compared with traditional visual cryptography, this technique has more flexibility, extensibility and security.

© 2004 Elsevier B.V. All rights reserved.

Keywords: Visual cryptography; Visual secret sharing

1. Introduction

Recently, due to the thriving of the Internet, traditional ways of transmitting and receiving data have been changed. Many enterprises are gradually using the Internet to exchange important documents or

data because of its great convenience and economic profit. However, since the Internet is an open and insecure hyperspace, hackers or illegal users can intercept the data when people transmit data via the Internet. Consequently, many security problems happen; for example, interception or tampering of important data, etc. How to protect the security of data is currently one of the issues to which people should pay much attention.

In order to protect the security of data, in 1994, Noar and Shamir proposed a new field of cryptography called visual cryptography (VC) [4]. The most

* Corresponding author. Tel.: +886 4 22196604; fax: +886 4 22453902.

E-mail addresses: wuhc@ntit.edu.tw (H.-C. Wu), ccc@cs.ccu.edu.tw (C.-C. Chang).

significant characteristic of the new field is that human visual systems can identify confidential messages directly without any computation when restoring encrypted messages. Thus, it improves the drawback of complex calculation that is necessary during the decryption process in traditional cryptography. The theory of visual cryptography can be applied to group secret systems to obtain the goal of sharing secrets. As for (t, n) -threshold visual secret sharing scheme, a dealer or secret owner can make n shares from the confidential message by using visual cryptography, and every participant in the group receives one share. When restoring the confidential images, printing each share to a transparency and only stacking the transparencies of these t members is needed to extract the confidential message, without any computation. If the number of stacked transparencies is less than t , the confidential image could never be restored. Because confidential messages are embedded in shares that refer to nothing in visual cryptography, hackers or illegal users cannot obtain any related messages about the embedded data from any share. Therefore, visual cryptography [1–6] can ensure the security of data communication and even protect the confidential message more thoroughly.

In order to solve the shortcoming that only one set of a confidential message can be embedded in traditional visual cryptography, many researchers have proposed various improved methods [2,7]. For example, by rotating a certain share, two sets of confidential messages can be embedded. That is, the content of two different kinds of confidential messages can be revealed in two different degrees of share stacking due to angle manipulation. Because the shares that these researchers used were all rectangles, which have four kinds of angle rotating variation: 0° , 90° , 180° and 270° , the choices of rotating angles are limited.

This paper proposes a $(2, 2)$ -visual secret sharing scheme, which can be used to embed two sets of confidential messages in two shares and prevent the drawback mentioned above. In this proposed scheme, circular shares are used and, by rotating a certain share to a fixed angle, two sets of confidential messages can be embedded in differently stacked and angled shares. In the proposed method, every two degrees is regarded as one unit. In the beginning, the first share is created randomly, and then the second share is

created according to the first share and the two embedded sets of confidential messages. Once the embedded confidential messages are retrieved, only stacking the two shares is needed to extract the content of the first confidential message. Then, by rotating the first share to a certain angle and stacking it with another share, the content of the second set of confidential messages can be extracted.

The remaining part of this paper is organized as follows. In Section 2, a brief description about current existing techniques in traditional visual cryptography is given. Section 3 introduces the proposed technique in detail. Next, the experimental results of the proposed technique are discussed in Section 4. Finally, Section 5 states the conclusions of this paper.

2. Related works

2.1. Noar and Shamir's visual secret sharing scheme

In 1994, Noar and Shamir proposed a new technique called visual cryptography. The primary property of visual cryptography is using a method called “stacking shares” to recover secret messages. “Stacking” refers to layering the shares on top of one another. The secret owner or a dealer creates two or more shares for the secret message. Each cannot be used to reveal the secret alone. Receiving all of the shares, printing each share onto a transparency, stacking the transparencies and using human visual system, the secret message can be visible without any computation needed. In this way, visual cryptography has proven to provide perfect security. Furthermore, the technique can be applied to group secret system, which is using (k, n) -threshold visual secret sharing scheme in order to perform secret sharing, where $k \leq n$. With (k, n) -threshold visual secret sharing scheme, the dealer or the secret owner can base a group of n participants to produce n shares for the secret message. Each participant in the group can have his own share. When recovering the secret message, only k or more transparency stacks are required without any computation. The secret message cannot be restored if less than k transparencies are used. Fig. 1 shows an example to illustrate the feature of $(2, 2)$ -visual secret sharing scheme. In Fig. 1, the secret is a logo, as shown in Fig. 1(a). Fig. 1(b) shows the two

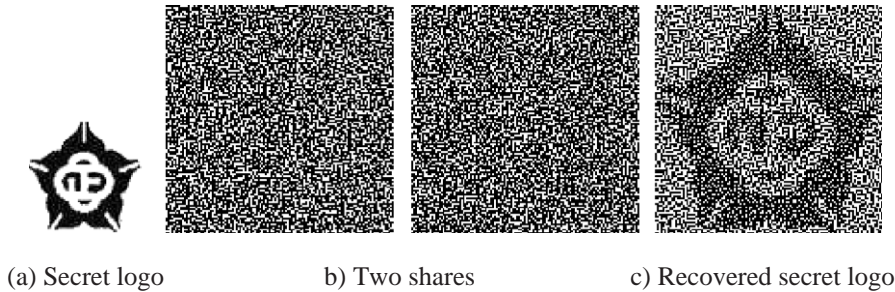




Fig. 1. An example of (2, 2)-visual secret sharing scheme.

corresponding shares of the secret message. The secret can then become visible to human eyes after these two shares are stacked. In Fig. 1(c), the stacked results are presented.

Next, we use the following example to briefly explain the basic concept of (2, 2)-visual secret sharing scheme. First, the confidential message is transformed to become a black–white confidential image with the size $N \times N$ pixels and then two corresponding shares are created after the encoding process. In the encoding process, each pixel $O(i, j)$ in the original black–white confidential image is corresponding to a block $P_A(i, j)$ in the first share and another $P_B(i, j)$ in the second share such that $P_A(i, j)$ and $P_B(i, j)$ are extended to contain $n \times n$ pixels. Therefore, the size of the two created corresponding shares is $nN \times nN$ and the size of the recovery confidential message stacked from them is $nN \times nN$. In this example, n is set to be 2. In Fig. 2, six patterns of the extended blocks with size 2×2 are denoted, so that every 2×2 extended block contains 2 white pixels and 2 black pixels. We randomly select a pattern from Fig. 2 to generate a 2×2 extended block $P_A(i, j)$ in the first share. Thus, the first share, which is called share A , is then created.

Each 2×2 extended block $P_B(i, j)$ of the second share, which is called share B , must be determined based on the corresponding $P_A(i, j)$ in share A and the pixel $O(i, j)$ in confidential image. Thus, each 2×2 extended block in the third line of Table 1 is defined based on the pixel color of the first line in the

confidential image and a 2×2 extended block to which the second line in the share A corresponds. For example, when $P_A(10, 3)$ in the share A is  (as shown in column 2 line 5 in Table 1) and the pixel of the corresponding position in confidential image is white, the 2×2 extended block $P_B(10, 3)$ in share B is  (as shown in column 3 line 5 in Table 1). According to the above mapping rule, share B that visually represents nothing can be created.

When restoring the confidential images, two corresponding transparencies of shares A and B are printed and stacked together. If the 2×2 extended block has 2 white pixels and 2 black pixels, it means the visual appearance of the 2×2 extended block would be white. If the 4 pixels are all black, it means the visual appearance of the 2×2 extended block would be black.

The disadvantage of the above conventional visual secret sharing scheme is that only one set of confidential messages can be embedded, so the method is not recommended for large amounts of confidential messages.

2.2. Chen and Wu's new visual secret sharing scheme

Chen and Wu [2] proposed a new visual cryptography technique in 1998. It uses share rotating to embed two sets of confidential messages into two shares. First, two sets of confidential messages are converted to become two binary confidential images of the size $N \times N$. If each pixel of two original black–white confidential images is corresponding to a 2×2 extended block in each share, two shares of the size $2N \times 2N$ would be created through the encoding process. Note that $P_A(i, j)$, $P_A(j, N-i-1)$, $P_A(N-j-1, i)$ and $P_A(N-i-1, N-j-1)$ must be defined to be the

Fig. 2. Six patterns of the 2×2 extended block.

Table 1
An implementation of (2, 2)-visual secret sharing scheme

Pixel of the confidential image	White						Black					
2×2 extended block of share A												
2×2 extended block of share B												
Stacked 2×2 extended block												

same 2×2 extended blocks. Thus, the first share *A* can be completely segmented to become four equal regions, as shown in Fig. 3. Then, each 2×2 extended block of the first region I in the first share *A* is randomly selected from one of the 2×2 patterns in Fig. 4. Each 2×2 extended block in the other three regions (II, III, IV) can be defined according to a corresponding 2×2 extended block in the first region I. For example, suppose the size of a confidential image is 8×8, if the 2×2 extended block at the position (1, 1) of the first region I is , the extended blocks at (1, 6) of the region II, (6, 1) of the third region and (6, 6) of the forth region must all be defined as . According to this mapping rule, share *A* can be generated.

The 2×2 extended block of the second share *B* must be defined according to the distribution of the 2×2 extended block of share *A* at the relative position and the pixel values at the relative position that corresponds to the two sets of confidential images as well as by one of the lines from column 4 lines 2 to 17 in Table 2. For example, when a 2×2 extended block at certain position in share *A* is (as shown in column 3 line 5 in Table 2), the pixel at the corresponding position of the first confidential image is black, and the pixel at the corresponding position of the second confidential image is white, the extended block at the relative position of the share *B* is (as in column 4 line 5 in Table 2). When two shares are

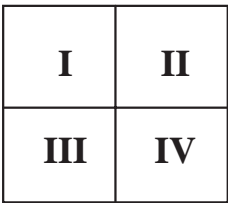


Fig. 3. Four divided regions of the share.

stacked together and the stacked 2×2 extended block has one white pixel and three black pixels, it means the stacked block would show in white color; if the four pixels in the stacked block are all black, it means the 2×2 stacked block would show in black color. Therefore, in the above case, after the two shares *A* and *B* are stacked together, the four pixels in the 2×2 extended block of the relative position are all black, then the color that this 2×2 extended block presents is black. That is, the pixel value of the corresponding position in the first confidential image is black. Next, rotate the share *A* counterclockwise 90°, then the 2×2 extended block at the original position would change from to . Then, stack it with the share *B*. Thus, the 2×2 extended block at the position would have one white pixel and three black pixels. It means this 2×2 stacked extended block appears in white color; that is, the pixel value of the corresponding position in the second confidential image is white. According to the above description, share *B* without any meaning can be created.

Although the above method solves the problem that only one set of confidential messages can be embedded in traditional visual cryptography, it still has limitation. That is, during the confidential image embedding process, the creation of shares is limited since the rotating angle can only be 0°, 90°, 180° and 270°.

3. The proposed (2, 2)-visual secret sharing scheme

In traditional visual cryptography, only one set of confidential messages would be embedded. By using



Fig. 4. Four patterns of the 2×2 extended block.

Table 2
An implementation of Chen and Wu's (2, 2)-visual secret sharing scheme

Pixel of the first confidential image	W	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B
Pixel of the second confidential image	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B	W
2×2 block of share A																
2×2 block of share B																
Stacked block																

the technique of stacking rotation angles, more than one set of confidential messages can be embedded. Since the shape of a share is square, only four kinds of angle degrees are used in the rotation: 0° , 90° , 180° and 270° . As a result, in conventional methods, rotation angles as well as the amount of confidential message would be limited.

This paper adapts circular shares to embed two sets of confidential messages into different angle degrees of the shares. The proposed method includes two processes—share *A* generation process and share *B* generation process, respectively. As shown in Fig. 5, two confidential messages M_1 and M_2 are transformed to become corresponding $n \times m$ confidential images O_1 and O_2 . Then, O_1 and O_2 are encoded to generate two shares, which are share *A* and share *B*, as shown in Fig. 5(a). When decoding the confidential message, the first confidential image can be obtained by completely stacking shares *A* and *B*, as in Fig. 5(b). Next, after rotating share *A* in x degrees (the share is called share *A'* after the rotation) and stacking it with the share *B* completely, the second confidential image can be obtained, as in Fig. 5(c).

Through share generation processes, each pixel in the confidential image corresponds to a 2×2 extended block in share *A* and share *B*. The 2×2 extended block in the share *A* consists of two white pixels and two black pixels, while the 2×2 extended block in the share *B* consists of one white pixel and three black pixels. When two shares are stacked together, if a white pixel and three black pixels exist in the 2×2 extended block of the stacked image, this 2×2 extended block represents a white pixel in the confidential image; if four black pixels exist, this

2×2 extended block would represent a black pixel in the confidential image.

3.1. Share *A* generation process

In the initial step, suppose r_1 is the radius of the circular share *A* and s is the radius difference of every two neighboring circles in the circular share. Besides, let P_1 be the area that is created from the space between the outer circle with radius r_1 and the second outer circle with radius $(r_1 - s)$ in the share; that is, P_1 is created from the sector space between the outer two circles in the share *A*. Similarly, let P_2 be the area that is created from the space between the second outer circle with radius $(r_1 - s)$ and the third outer circle with radius $(r_1 - 2s)$ in the share. Let $P = P_1 \cup P_2$.

In the first step, one degree is used as the unit for segmenting P . Thus, P would contain 360 sector areas. These sector areas are divided to become blocks by every two degrees. That is, 2×2 sector pixels are defined as one block and this block stands for a pixel at the corresponding position in the original image. We use the direction of three o'clock to represent degree 0 (0°) of the circular share. The clockwise direction represents increase in angle degree. In P , the area in 0° and 1° stands for the first 2×2 sector block, and the area of 2° and 3° stands for the second 2×2 sector block, etc. In the proposed method, when rotating share *A* in x degrees and stacking it with the share *B* to create the confidential image O_2 , the rotation degree x must be a multiple of 2 because each two degrees is used as one unit for a sector block. That is, each 2×2 sector block is occupied by two degrees. Moreover, x must be the common factor of

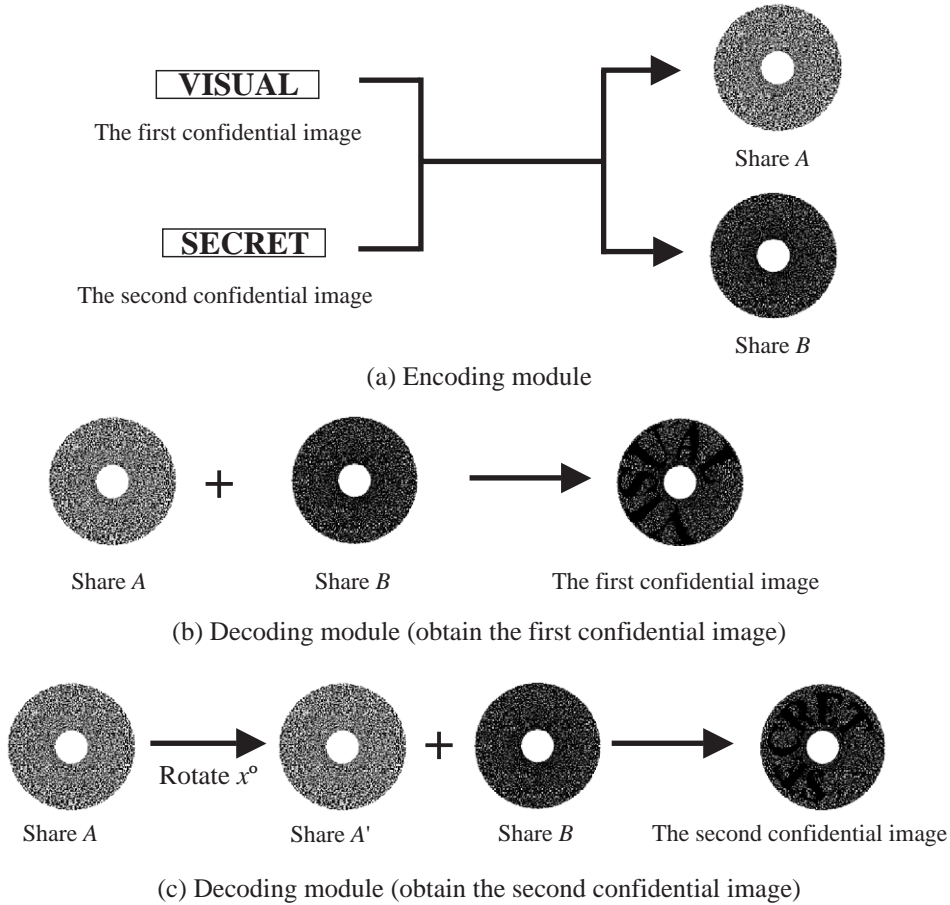


Fig. 5. The processing of the proposed method.







360. Thus, the share can be completely segmented into integer amount of areas.

As for the rotation degrees is x , the proposed method divides P to become $360/x$ non-overlapping areas so as to make each area cover x° . In the first area (0° to $(360/x)^\circ$), each 2×2 sector block is randomly selected from a pattern from Fig. 6. Each 2×2 sector block in the second area ($((360/x)^\circ$ to $2 \times (360/x)^\circ$) is defined by the rotating type counterclockwise in 90° of the corresponding 2×2 sector block in the previous area (the first area); other areas are defined as above. In other words, we only need to randomly determine

Fig. 6. Four patterns of the 2×2 sector block.

the type of each 2×2 sector block of the first area, and the 2×2 sector blocks in other areas can be determined based on the type of rotation in the corresponding 2×2 sector blocks of the previous area which are rotated counterclockwise 90° . Afterwards, a total of $360 \times 2 \times 2$ sector blocks can be created in P .

We call share A after rotation as share A' . After stacking the share A' and the share B , the second confidential image can be obtained. The i th pixel value in the second confidential image can be obtained by stacking the i th 2×2 sector block in share A' and the i th 2×2 sector block in share B . The i th 2×2 sector block in the share A' is obtained from the $(i-x)$ th 2×2 sector block in share A . However, when rotating the circular share, only the 2×2 sector block is actually rotated. The black-white pixels in the 2×2 sector block are not rotated in reality.

Therefore, the i th 2×2 sector block in share A has to be defined by type from rotating the $(i-x)$ th 2×2 sector block within share A counterclockwise 90° ; the $(i-x)$ th 2×2 sector block in the share A must be defined by the type from rotating the $(i-2x)$ th 2×2 sector block in the share A , and so on. Thus, it can follow the definition shown in Table 3 to embed each pixel in the first and the second confidential images into share A and share B . For example, suppose the j th pixel in the first confidential image is white, the j th pixel in the second confidential image is black and the rotation angle is x degrees. If the $(j-x)$ th 2×2 sector block in share A is , the j th 2×2 sector block in share A must be  and the j th 2×2 sector block in the share B must be . Therefore, after two shares are stacked together, the j th stacked 2×2 sector block would be , which reveals the j th pixel in the first confidential image to be white. Next, rotate share A clockwise x degrees, the new share is called share A' and its j th 2×2 sector block is . After stacking the shares A' and B , the resulting j th 2×2 sector block is , which reveals the j th pixel in the second confidential image to be black.

In the second step, each P_k , $k \geq 2$ is created from the space between the circle that radius is $(r_1 - (k-1) \times s)$ and the circle that radius is $(r_1 - k \times s)$ in A . Let $P = P_k \cup P_{k+1}$. After repeating the first step to create 360 2×2 sector blocks in P , the first share A can be created.

Because the sector block that is closer to the center of the circle would become smaller, the distribution of

































































the sector block would also become intense; that is, the difference between black and white blocks would become less obvious. As a result, when stacking two shares, the confidential image that is closer to the center of a circle would become unclear. A restriction is set up when the radius is between a small range and P_k would no longer be created. Therefore, the circular share that is produced by using the proposed method would be a sector circle.

3.2. Share B generation process

In the beginning, like share A generation process, r_1 is defined as the radius of the circular share, s is defined as the radius difference of every two neighboring circles in circular share. Suppose C_1 is from the space between the outer circle with radius r_1 in share B and the second outer circle with radius $(r_1 - s)$; that is, C_1 is created from the sector space between the outer two circles in the share B . Similarly, let C_2 be the area that is created from the space between the second outer circle with radius $(r_1 - s)$ and the third outer circle with radius $(r_1 - 2s)$ in the share. Let $C = C_1 \cup C_2$.

In the first step, each degree is used as a unit for segmenting C . Thus, C contains 360 sector blocks. Every neighboring sector region of two degrees is denoted as one block, so 2×2 sector block represents a pixel at corresponding positions in the original image. The direction of three o'clock represents the degree 0 of the circular share and

Table 3
An implementation of the proposed (2, 2)-visual secret sharing scheme

Pixel of the first confidential image	W	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B
Pixel of the second confidential image	W	B	W	B	W	B	W	B	W	B	W	B	W	B	W	B
2×2 sector block of Share A																
2×2 sector block of Share B																
Stacked block by Shares A and B																
Stacked block by Shares A' and B																

clockwise direction would increase in angle degree. The area of degree 0 and degree 1 in C_1 stands for the first 2×2 sector blocks, while the area of degree 2 and degree 3 stands for the second 2×2 sector blocks, and so on. In the proposed method, the distribution of 2×2 sector blocks in C is determined according to share A , the first confidential image O_1 and the second confidential image O_2 . Table 3 shows the mapping rule to produce the 360 sector blocks for C . For example, when a 2×2 sector block in share A is $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ (as shown in column 3, line 10 of Table 3), the pixel at the corresponding

position of the first confidential image is white, and the pixel at the corresponding position of the second confidential image is black, then the defined 2×2 sector blocks in C would be $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ (as in column 4 line 10 of Table 3).

In the second step, C_k is made up from the space between the circle that radius is $(r_1 - (k-1) \times s)$ and the circle that radius is $(r_1 - k \times s)$ in the share B . Let $C = C_k \cup C_{k+1}$. Repeat executing the first step and create 360 2×2 sector blocks for C until all 2×2 sector blocks in C are defined. Finally, the second share B can be created.

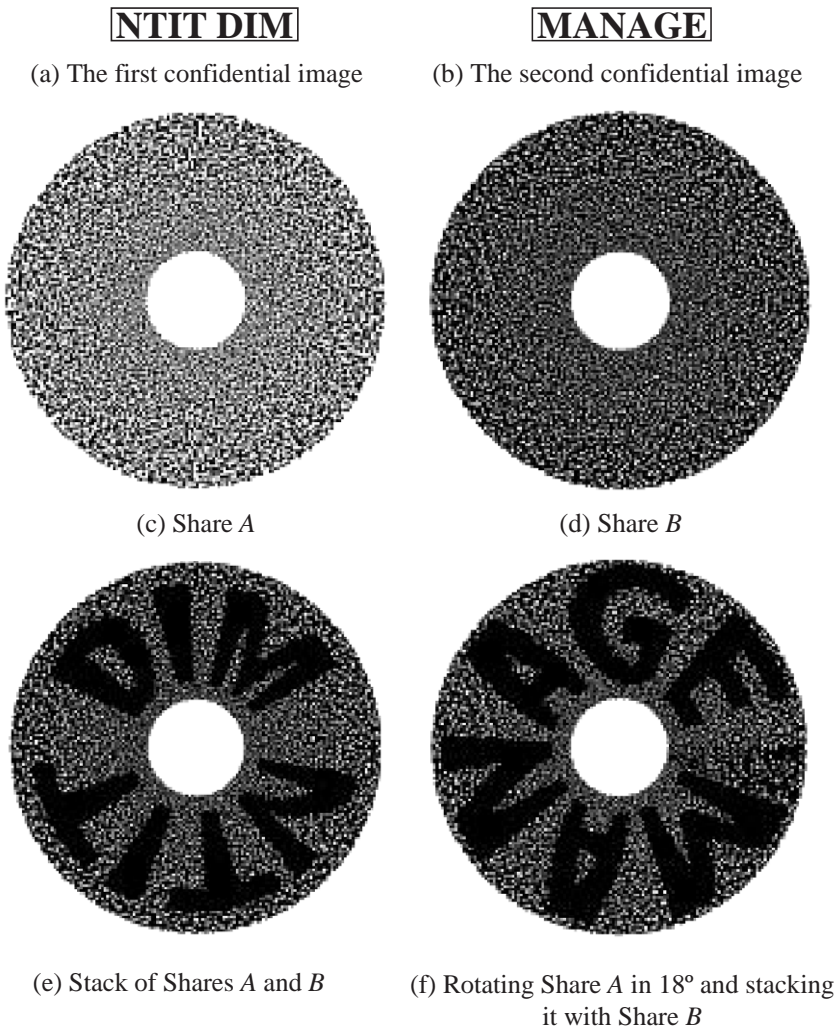


Fig. 7. Experiment result of rotating the share in 18° .

4. Experimental result and analysis

This paper proposes a (2, 2)-visual secret sharing scheme, which uses the technique of circular shares to embed two sets of confidential messages into two shares. By using the method of rotating a certain share in a certain fixed degree, two sets of confidential messages can be embedded into different stacking angle degrees. In this section, the effectiveness of the method is stated based on the following experiment. The platform for this experiment is Pentium-450 MHz, Windows 2000 Professional OS, Java 1.3.1 for programming tool, Adobe Photoshop 6.0 and Ulead Photo-impact 6.0 for image processing.

There are three experiments with stacking angles 18° , 40° and 72° , respectively. First, two confidential images with 180×32 pixels are respectively embedded into two shares. The embedding angle degree for the first confidential image is 0° , while the embedding angle degree for the second one is 18° . By using the proposed share generation processes, two shares as shown in Fig. 7(c)–(d) would be created. If the two shares are stacked together completely, the content of the first confidential image can appear, as shown in Fig. 7(e). If the first share is rotated clockwise 18° , and then two shares are stacked together completely, the content of the second confidential image can appear, as shown in Fig. 7(f).

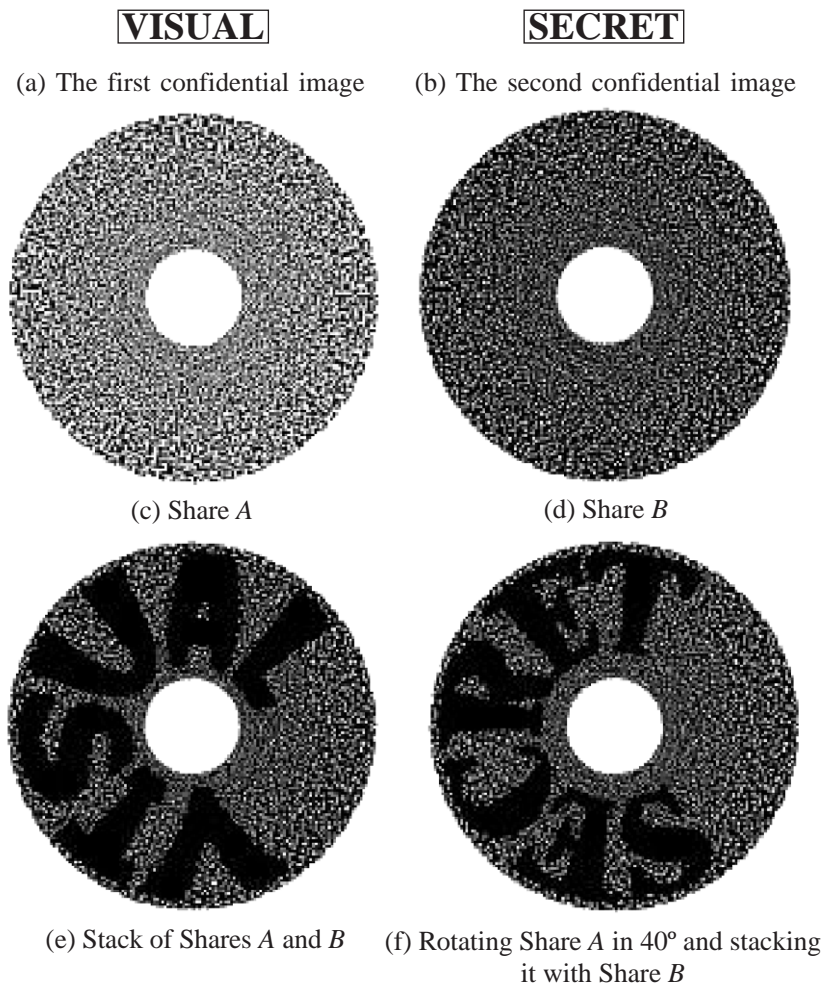


Fig. 8. Experiment result of rotating share A in 40° .

Fig. 8 shows the second experiment with 40° for the second stacking angle and Fig. 9 shows our third experiment with 72° .

In the proposed method, when the rotation angle degree is x , the shares are divided into $(360/x)$ areas. Let $y=(360/x)$. As mentioned in Section 3, x must be an even number and also be a common factor of 360. The reason for being an even number is that each block of the shares takes 2° in place and the blocks should be stacked completely, and the reason for being a common factor of 360 is that the confidential image can be separated into non-overlapping areas. Note that, if y cannot be divided by 4, the first region between 0 to x° cannot be embedded into any

confidential data. Otherwise, when presenting the second confidential data, the information from that region would be incorrect. On the contrary, if y can be divided by 4, then confidential data can be embedded into all shares. The reason is that in share A , the distribution of all possible 2×2 sector blocks has only four conditions, as shown in Fig. 6. Besides, only the 2×2 sector blocks in the first region (0° to $(x-1)^\circ$) are randomly selected from any pattern in Fig. 6, and the type of 2×2 sector blocks in other regions are determined based on its previous region. Therefore, in Share A , the 2×2 sector blocks in the i th region and the $(4i+1)$ th region have the same definition, where $i=0, 1, \dots, (y-1)$. The 2×2 sector blocks in the last

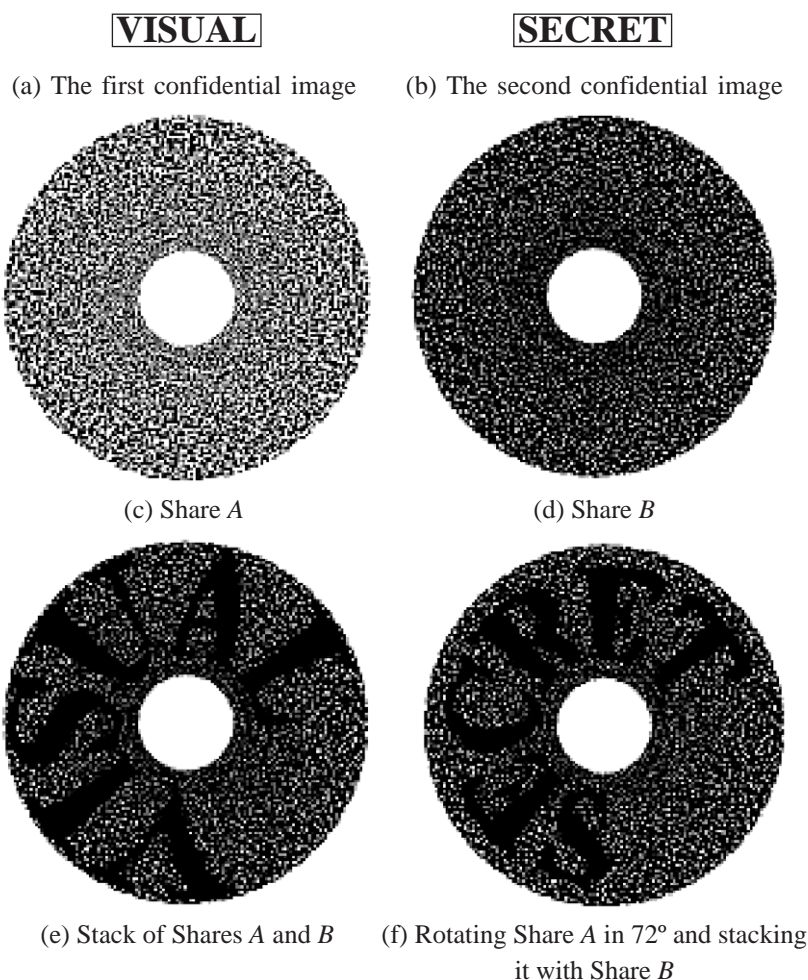








Fig. 9. Experiment result of rotating share in 72° .

region must be defined according to the type of rotation from the 2×2 sector blocks in the first region of 90° . For example, suppose the rotation angle is 30° , then the share would be divided into $12(360/60=12)$ regions, each region is a curve area of 30° . Let the first 2×2 sector block in the first region (0 to 29°) be , the first 2×2 sector block in the second region (30° to 59°) be , the first 2×2 sector block in the third region (60° to 89°) be , the first 2×2 sector block in the fourth region (90° to 119°) be , the first 2×2 sector block in the fifth

region (120° to 149°) be  and so on. The first 2×2 sector block in the final region (330° to 359°) is . Therefore, after the first share is rotated 30° , the 2×2 sector blocks between 0° and 29° regions would conform to the definition in Table 3. Thus, when presenting the second confidential data, the information revealed from the region between 0° and 29° is correct.

If y cannot be divided by 4, the 2×2 cambered blocks in the final region would not become the type by rotating clockwise 90° of the 2×2 sector blocks of

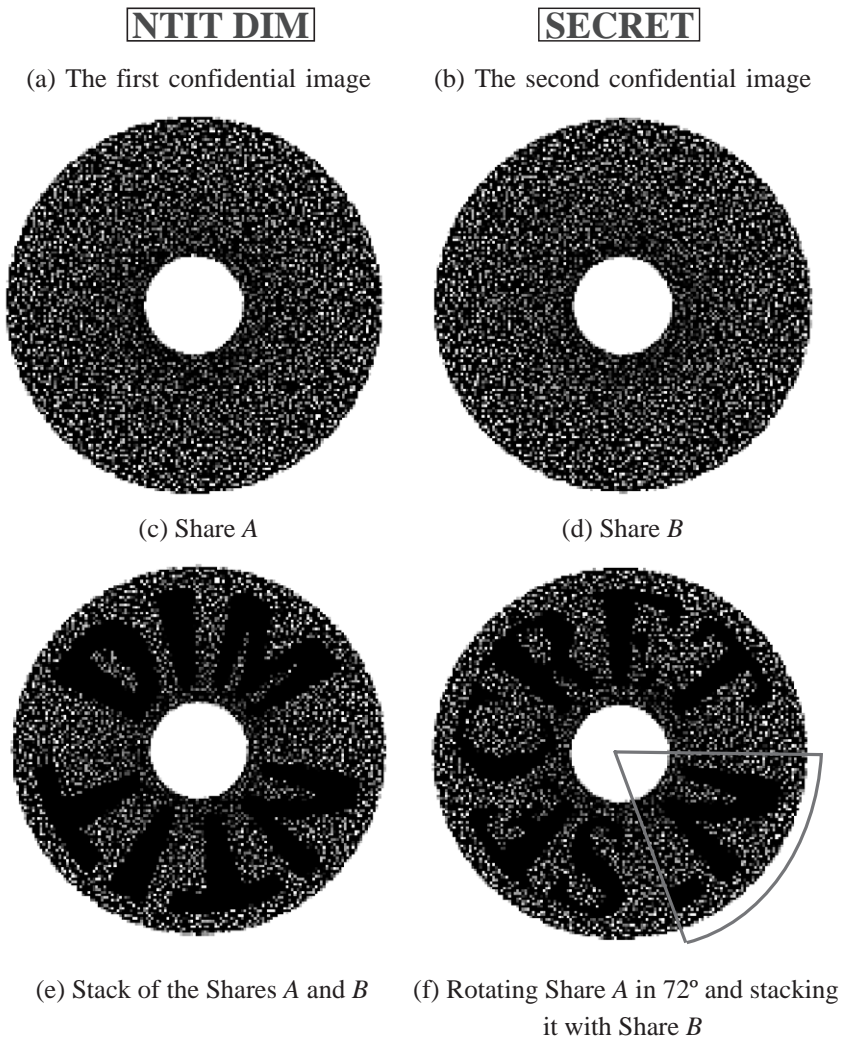


Fig. 10. Experiment result of the case that rotation angle degree cannot be divided by 4.

the first region. After the first share is rotated, the 2×2 sector blocks between 0° and the rotation angle degree would not conform to the definition in Table 3. Therefore, when presenting the second confidential data, the information revealed from the region between 0° and the rotation angle is incorrect.

At last, two sets of confidential images with 180×32 pixels are respectively embedded into shares, as in Fig. 10(a)–(b). The embedding angle of the first confidential image is 0° , while the embedding angle of the second confidential image is 72° . Thus, two shares are created, as shown in Fig. 10(c)–(d). If two shares are stacked completely together, the content of the first confidential image can be revealed, as shown in Fig. 10(e). However, in this case, $x=72$, $y=5$ and y cannot be divided by 4. If the first share is rotated clockwise 72° , the information from the first region of the second confidential image is incorrect after the two shares are stacked together, as in Fig. 10(f).

The performance of a visual secret sharing scheme depends on several features such as the access structure (or the decrypt model), contrast and expanding size. The proposed scheme emphasizes that two different secrets are embedded into two shares while the other two performance indices are also preserved. The contrast is the difference between the revealed white and revealed black. For example, the contrast of the proposed scheme is $1/4$ since it reveals a black secret pixel by four black sub-pixels and reveals a white secret pixel by one white and three black sub-pixels. The expanding size of the proposed scheme is four since every secret pixel is turned into a 2×2 block. Recalling the related schemes in Section 2, Chen and Wu's scheme has the same features as the proposed method, but our scheme frees from the limitation of the stacking angles.

5. Conclusions

In recent visual cryptography techniques, the adapted shares are generally rectangle. Therefore, only four kinds of rotation angle degree change exist when presenting confidential data, and they are respectively 0° , 90° , 180° and 270° . It limits the variation of rotation angle in share generation. In this

paper, we propose an improved method, which uses a circular shape of share. By using the feature that a circle has 360° in angle degree, confidential messages can be embedded into circular shares in any selected angle degree.

In ordinary traditional visual cryptography, only one set of confidential messages can be embedded. Our proposed technique can be used to embed two sets of confidential messages. By using the feature of rotation angle, two sets of confidential messages can be embedded into different angles. When extracting the message, these two sets of confidential messages can still be available. Therefore, the proposed method can be used to embed two times the amount of confidential message in traditional visual cryptography. Moreover, when extracting the confidential message, the proposed method can provide equal clarity quality in comparison with that of traditional visual cryptography. Therefore, our proposed method not only overcomes the disadvantages in traditional visual cryptography, but also preserves its advantages. More than two secrets decrypted from two shares or general models are the next interesting directions.

References

- [1] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, "Visual Cryptography for General Access Structures," Electronic Colloquium on Computational Complexity, TR96-012, 1996, available at <http://www.eccc.uni-trier.de/eccc>.
- [2] L.H. Chen, C.C. Wu, "A Study on Visual Cryptography," Master thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.
- [3] S. Drostle, New results on visual cryptography, Advances in Cryptology: Eurocrypt'96, Lecture Notes in Computer Science, vol. 1109, Springer-Verlag, 1996, pp. 401–415.
- [4] M. Noar, A. Shamir, Visual cryptography, Advances in Cryptology: Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1995, pp. 1–12.
- [5] M. Noar, B. Pinks, "Visual Authentication and Identification," CRYPTO97, pp. 322–336, available at <http://theory.lcs.mit.edu/~cryptol>.
- [6] V. Rijmen and B. Preneel, "Efficient Colour Visual Encryption for Shared Colors of Benetton," presented at Eurocrypt'96, Rump Session, available at <http://www.iacr.org/conferences/ec96/rump/preneel.ps>.
- [7] C.S. Tsai, C.C. Chang, T.S. Chen, Sharing multiple secrets in digital images, Journal of Systems and Software 64 (2002) 163–170.



HSIEN-CHU WU was born in Tainan, Taiwan, Republic of China, on October 26, 1962. She received the B.S. and M.S. degrees in Applied Mathematics in 1985 and 1987, respectively, from the National Chung Hsing University, Taichung, Taiwan. She received the Ph.D. degree in Computer Science and Information Engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. Since

August 2002, she has been an associate professor of the Department of Information Management at National Taichung Institute of Technology, Taichung, Taiwan. Her research interests include information security, image authentication, digital watermarking and image processing.



CHIN-CHEN CHANG was born in Taichung, Taiwan, the Republic of China, on November 12, 1954. He received his B.S. degree in Applied Mathematics in 1977 and his M.S. degree in Computer and Decision Sciences in 1979 from National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.d. in Computer Engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. From 1983 to

1989, he was among the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. Since August 1989, he has worked as a professor of the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Dr. Chang is a Fellow of IEEE and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include computer cryptography, data engineering, and image compression.