Sharing Secret Images Using Keyed Information Hiding Technique

Chiang-Lung Liu[1*], Kai-Ping Wang[2], and Der-Chyuan Lou[3]

[1] *Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology, National Defense University*
[2] *School of Defense Science, Chung Cheng Institute of Technology, National Defense University*
[3] *Department of Computer Science and Information Engineering, Chang Gung University*

ABSTRACT

Sharing secret through the Internet is very popular nowadays. Traditional meaningless sharing images may attract attackers' attentions. If an attacker can collect enough shares, he/she can overlap the intercepted images and reveal the secret. In this paper, we propose a new secret image sharing method to improve this situation. The secret image is first transformed into two meaningful sharing images depending on a cover image and a predefined secret codebook. The secret image can be reconstructed by using the secret codebook. Experimental results show that two meaningful sharing images can be effectively created using the proposed sharing images creation process and the original secret image can be reconstructed according to the proposed secret image reconstruction process.

Keywords: secret sharing, information hiding, codebook

使用鍵控資訊隱藏技術的秘密影像分享技術

劉江龍[1*]　王開平[2]　婁德權[3]

[1]國防大學理工學院電機電子工程學系
[2]國防大學理工學院國防科學研究所
[3]長庚大學資訊工程學系

摘　要

透過網際網路進行秘密分享目前已非常普遍。傳統無意義內容的秘密影像分享策略容易引起攻擊者的注意。 如果攻擊者能收集足夠的分享影像，其可以透過重疊被攔截的圖像而破解秘密。在本文中，我們提出一個新的秘密影像分享技術以改進這個情況。本技術所使用的分享影像均為內容有意義的影像，其分別依據掩護影像及事先定義的密碼簿所產生；而後續憑藉這兩個分享影像及密碼簿則可重建原始秘密影像。實驗結果顯示，依據本文提出的分享影像產生程序，可有效建立內容有意義的分享影像；而原始的秘密影像也可透過本文提出的秘密影像重建程序進行復原。

關鍵詞：密秘分享，資訊隱藏，密碼簿

文稿收件日期 100.11.25;文稿修正後接受日期 101.5.23; *通訊作者
Manuscript received November 25, 2011; revised May 23, 2012; *Corresponding author

Ⅰ. INTRODUCTION

Due to the rapid development of information technology, computer and communication network have become the living need. Besides enjoying the convenience of spreading information quickly, anyone can download a great deal of digital information through the network, such as image, audio, and video, etc. Organizations can also create a great deal of business opportunities to benefit themselves. However, the convenience of network also causes a severe problem, that is, the hacker may intrude your network and computer system to steal the important information and sold them to third party to gain higher benefit. Such illegal behaviors have caused great damages to organizations or personal benefits. Hence how to protect the security of information has become a very important issue.

To protect the security of information, many different technologies have been developed, such as cryptography, information hiding (or data hiding), and visual cryptography technologies. By using complicated mathematics calculation, cryptography techniques can transform the secret information into nonsense. Anyone cannot understand the message except the legal owner that owns the decryption key. Information hiding techniques [1, 2] use the characteristic of media (such as image, audio, and video) to embed useful information. To ensure the security, the information embedded media should not cause any noticeable distortion and anyone cannot obtain any information from the media except the legal person. The visual cryptography technique is a kind of secret sharing technique which was first proposed by Shamir [3]. By dividing the secret information into several shares, the security of information can be assured. When these shares are stacked, the secret information can be recovered. In 1994, Noar and Shamir [4] further used the similar concept to propose a visual secret sharing technique. First, they use the secret image and codebook to generate *n* sharing images. Then the *n* sharing images are protected by *n* protectors. However, no one can understand the meaning of the secret image unless enough sharing images can be collected and stacked. It should be noted that the recovered secret image can be recognized directly by human eyes.

The recent studies of the secret sharing technique can be divided into two categories. One is traditional sharing method, the other is polynomial method. The traditional sharing method does not need complicated calculation to decode the secret information and the recovered information can be recognized directly by human eyes. In 2006, Fang and Lin [5] utilized the concept of Noar and Shamir's method to propose a progressive secret sharing method. In their method, each pixel of a halftone secret image is first expended to a 2×2 block. Then *n* sharing images are created according to the following way. If a pixel is black, all four pixels of the 2×2 block are set to black. If the pixel is white, two random pixels of the 2×2 block are set to black and the others are set to white. By this way, nobody can obtain any information about the secret image from one of the sharing images. On the other hand, the secret image can be obtained by staking some of the sharing images. The more the sharing images stacked, the clearer the secret image appeared. Although the above method can quickly view the secret image, the security is a consideration [6].

To enhance the security of secret information, Chen et al. [7] proposed a novel subliminal channel method combining the concept of visual cryptography with image hiding. In their method, a secret image is first encrypted and transformed from base 10 into base 6. Two sharing images are then constructed by using the transformed information, a halftone image, and a codebook. The method can not only keep the security of the secret information, but also increase the embedding capacity.

To protect the safety of secret information and reduce the space of information storage, Thien and Lin [8] extended the concept of Blakley and Shamir and proposed a polynomial image sharing technique. First the pixel values more than 250 of a grayscale image are set to 250. The sharing images are then computed by using a polynomial. If collecting all of the sharing images, the secret image can be reconstructed by using Lagrange's interpolation. The advantage of the method is that the size of the sharing images is 1/2 of the secret image and, therefore, can reduce the space of image storage.

However, cutting the pixel values more than 250 will cause a lossy image. More recently, secret color image sharing becomes a new research trend of visual secret sharing [6, 9, 10].

The non-color secret image sharing methods mentioned above have a common disadvantage that the sharing images are meaningless and, therefore, may draw the attackers' attentions. That is, an attacker may try his/her best to collect enough shares to reveal the secret. To improve this disadvantage, we propose a novel secret image sharing method based on the concept of Naor and Shamir's method. The proposed method also integrated with the concept of information hiding to produce meaningful sharing images. Besides, a secret codebook is used in the proposed method as the secret key to provide another security. If an attacker is capable of collecting all the sharing images, he/she still cannot retrieve the embedding information without the secret codebook.

To completely describe the proposed method, the remainder of this paper is organized as follows. Section II reviews the concept of the Naor and Shamir's secret image sharing method. The proposed method is described in Section III. Section IV shows the experimental results. The conclusions are given in Section V.

II. REVIEW OF NAOR AND SHAMIR'S SECRET IMAGE SHARING METHOD

The concept of secret sharing is firstly proposed by Shamir in 1979 [3]. The basic scenario of the secret sharing goes as follows. Someone uses a key to lock the secret information in a safe. The key is further divided into several pieces and shared among users. If enough pieces are obtained, the secret information can be released. In 1995, Naor and Shamir used the concept of codebook to propose an image sharing technique [4]. A secret image is first divided into several sharing images by using a codebook. Because the shared images are meaningless, anyone cannot obtain any information from each shared image. However, the secret image can be reconstructed by overlapping all the shared images. Their method is very simple and easy to be implemented. Besides, the reconstructed image can directly be recognized by human eyes.

In general, human eyes are more sensitive to bright objects. Therefore, when a black and a white show at the same time, they will be recognized as a white rather than a black. Table 1 is a sample of codebook constructed according to this characteristic. If the pixel is white, we can randomly select a block to be the sharing block 1 from upper left 6 blocks, e.g., the block (1010). Besides, the corresponding block will be selected to be the sharing block 2, namely block (1010). On the other hand, if the pixel is black, we can randomly select a block to be the sharing block 1 from lower left 6 blocks, e.g., the block (0101), and the corresponding block (1010) will be selected to be the sharing block 2. If the overlapping result is two whites and two blacks, that stands for white. If the overlapping result is four blacks, that stands for black. By overlapping the sharing blocks, the reconstructed information can directly be recognized by human eyes. The sample secret image sharing method mentioned above is especially called (2, 2) sharing method.

The concept of the (k, n) secret sharing is similar to the (2, 2) sharing method. The main difference is that the (k, n) secret sharing method divides an image into n sharing images and only needs any k sharing images to reveal the secret image. It implies that we cannot obtain any information if less than k sharing images been collected.

III. THE PROPOSED METHOD

In this section, we use the concept of Naor and Shamir's method to propose a novel secret image sharing method. To avoid drawing attackers' attentions, the concept of information hiding is adopted by the proposed method to create meaningful sharing images. The proposed secret image sharing method can be divided into two stages: sharing images creation and secret image reconstruction. The details of the proposed sharing images creation and secret image reconstruction are described in the following subsections.

Table 1. The codebook used in the sample (2, 2) image sharing method.

Pixel	Sharing block 1		Sharing block 2		Overlapping result	
□ White	(1010)	(0101)	(1010)	(0101)	(1010)	(0101)
	(0011)	(1100)	(0011)	(1100)	(0011)	(1100)
	(0110)	(1001)	(0110)	(1001)	(0110)	(1001)
■ Black	(0101)	(1010)	(1010)	(0101)	(0000)	(0000)
	(0011)	(1100)	(1100)	(0011)	(0000)	(0000)
	(0110)	(1001)	(1001)	(0110)	(0000)	(0000)

3.1 Sharing Images Creation

Fig. 1 shows the flowchart of the proposed sharing images creation process. The cover image is then divided into non-overlapping 2×2 blocks and the average value for each block is calculated. Two meaningful sharing images are then constructed according to the above results and a predefined secret codebook. The detailed steps of the proposed sharing images creation process are as follows.

Input: An $M \times N$ cover image, an $M/2 \times N/2$ halftone image, and a predefined secret codebook.

Output: Sharing image 1 and sharing image 2.

Step1: Divide the cover image into non-overlapping 2×2 blocks and calculate the average values for each block.

Step2: Match the pixels of the halftone image with the predefined codebook. A sample secret codebook is shown in Table 2.

Step3: Output two sharing images each with size $M \times N$.

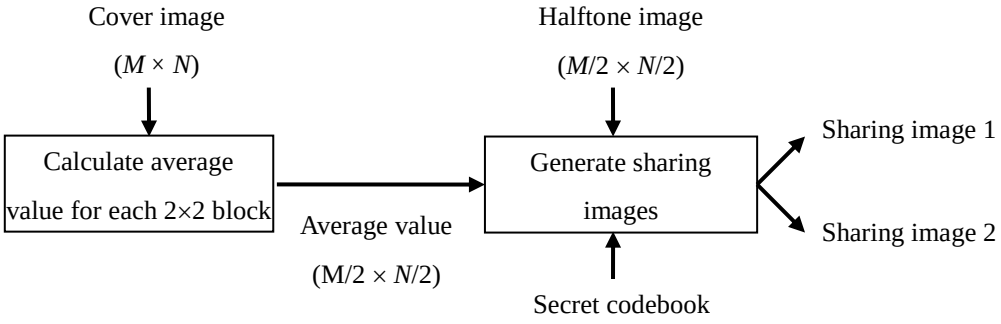


Fig. 1. The flowchart of the proposed sharing images creation process.

Table 2. The sample secret codebook used in our experiments

Image pixel	Pixel value	Sharing image1	Sharing image2	Overlapping image	Image pixel	Pixel value	Sharing image1	Sharing image2	Overlapping image
White	>224	(1111)	(1111)	(1111)	Black	<32	(0000)	(0000)	(0000)
	>192	(0111)	(1111)	(0111)		<64	(0010)	(0010)	(0010)
	>160	(1111)	(0111)	(0111)		<96	(1000)	(1000)	(1000)
	>128	(1101)	(1101)	(1101)		<128	(1110)	(0110)	(0110)
	>96	(0111)	(0110)	(0110)		<160	(1011)	(1011)	(1011)
	>64	(0011)	(0011)	(0011)		<192	(1100)	(1100)	(1100)
	>32	(0110)	(0110)	(0110)		<244	(1001)	(1001)	(1001)
	≤32	(0101)	(0101)	(0101)		≥244	(1010)	(1010)	(1010)

To further explain the proposed sharing images creation process, we take a 4 × 4 cover image (shown in Fig. 2(a)) and a 2 × 2 halftone image (shown in Fig. 2(c)) as an example. The cover image was first divided into non-overlapping 2 × 2 blocks. The average values of these 2 × 2 blocks were then calculated and the results were 50, 170, 40, and 118 as shown in Fig. 2(b). The first value 50 and the corresponding value (i.e. black) in the halftone image were then matched with Table 2 to obtain two sharing blocks (0010) and (0010). The other three pixel values were then sequentially processed in the same way to obtain their corresponding sharing blocks. Finally, two sharing images were obtained and shown in Figs. 2(d) and 2(e), respectively.

3.2 Secret image reconstruction

Input: Sharing image 1, sharing image 2, and a predefined secret codebook.
Output: An $M/2 \times N/2$ halftone image.
Step1: Divide each sharing image into non-overlapping 2×2 blocks.

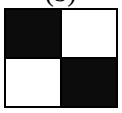
Step2: Sequentially match the 2×2 blocks with the secret codebook to obtain the halftone image.

50	25	15	195
75	50	195	275
10	25	35	195
15	30	40	200

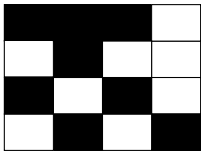
(a)

50	170
40	118

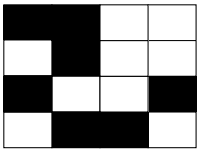
(b)



(c)



(d)



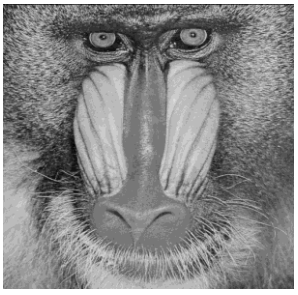
(e)

Fig. 2. An example of the proposed sharing image creation: (a) the 4×4 secret image, (b) the corresponding average values, (c) the 2×2 secret image, (d) the sharing image 1 and (e) the sharing image 2.

IV. EXPERIMENTAL RESULTS

Several experiments have been performed to prove the feasibility of the proposed method. Figs. 3(a) and 3(b) show the cover image with size 512×512 and the halftone secret image with size 256×256, respectively. Two meaningful sharing images were then created according to the proposed sharing images creation process and shown in Figs. 4(a) and 4(b), respectively. It is clear that both the sharing images reveal no information about the secret image. It should be noted that Table 2 was used in our experiments as the secret codebook to generate the sharing images. To encode the white and black pixels in the secret halftone image, the codebook shown in Table 2 is composed of two sections. One is for encoding the white pixel of the secret image is composed of 16 4-bit blocks. The other is for encoding the black pixel of the secret image and is also composed of 16 4-bit blocks. Therefore, the size of the codebook is $2 \times 16 \times 4 = 128$ bits. Moreover, there is only one codebook used through our experiments. In practical applications, the secret codebook can be carefully designed to provide the security of uncertainty.

The two sharing images were then used to reconstruct the halftone secret image according to the proposed secret image reconstruction process. Fig. 4(c) shows the reconstructed halftone secret image which can be clearly recognized by human eyes. Two more sets of cover images and secret halftone images have been tested according to the same test processes described above. The experimental results are shown in Table 3. It is clear that, in Table 3, the meaningful sharing images can be effectively created and the secret halftone images can be correctly reconstructed. The feasibility of the proposed method is therefore proven.



(a)

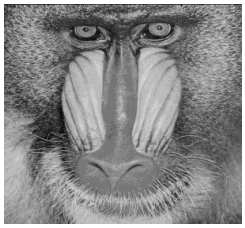
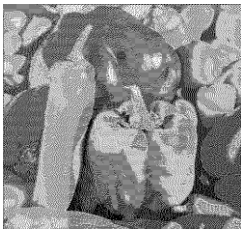
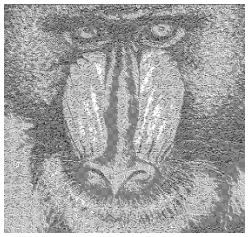
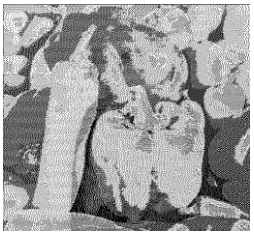
(b)

Fig. 3. (a) The cover image and (b) the halftone secret image.

(a) (b) (c)

Fig. 4. (a) The sharing image 1(PNSR = 12.04 dB), (b) the sharing image 2 (PNSR = 15.41 dB), and (c) the reconstructed secret image.

Table 3. Experimental results of two more sets of test images.

	Example1	Example2
Cover image		
Secret halftone image		
Sharing image 1	 PSNR = 11.65 dB	 PSNR = 12.35 dB
Sharing image 2	 PSNR = 15.53 dB	 PSNR = 14.80 dB

In the proposed secret image sharing method, we adopted the concept of information hiding to elegantly convert the secret half-tone image into two meaningful sharing images to avoid the attention of eavesdroppers. Besides, a secret codebook is used in the proposed method so that the attackers cannot reconstruct the secret half-tone image by simply overlapping the two sharing images. In other words, the security is the major concern for the proposed secret image sharing method, not the capacity.

To show the superior of the proposed method in security, we make some comparisons with two recently published methods and the results are shown in Table 4. From Table 4, we can see that the sharing images constructed by Chen et al.'s method [7] are meaningless and may attract attackers' attentions. Although the sharing images constructed by Fang and Lin's method [5] are meaningful, they preserved no information. Besides, once parts of the sharing images are collected by attackers, they will obtain the important information of the secret image easily [5]. The disadvantages described above have been avoided for the proposed method.

V. CONCLUSIIONS

Due to the rapid increase of information damage, information security has become a very important issue in modern society, especially in military. Secret sharing techniques divide secret information into different shares to ensure the security of the information. Only if collecting enough shares, secret information can be recovered.

In this paper, we propose a secure secret sharing technique to protect the security of secret images. The advantage of the proposed method is that the shared images are meaningful and, therefore, can avoid attracting attackers' attentions. Anyone cannot obtain any information of the secret image except the authorized owner. Compared with the recently published works, the proposed method are more secure. It should be noted that suitable design of the codebook is the key to obtain the sharing images with better visual quality. Combining the human visual contrast may be a good manner to achieve this purpose. The sample codebook shown in Table 2 is designed according to this philosophy. However, clearly, it can be improved by combining more effective human visual models to obtain two sharing images with better visual quality.

Future works of our study include improving the quality of sharing images and developing a secret sharing technique for color image protection.

Table 4.The comparison results with the published methods

	Meaningful	Preserving information	Overlapping
Chen et al.' method	No	Yes	Yes
Fang and Lin's method	Yes	No	Yes
Our method	Yes	Yes	No

REFERENCES

[1] Lee, Y. K. and Chen, L. H., "An adaptive image steganographic model based on minimum-error LSB replacement," Proceedings of the 9th National Conference on Information Security, Taichung, Taiwan, pp. 5-15, 1999.

[2] Petitcolas, F. A., Anderson, R. J., and Kuhn, M. G., "Attacks on copyright marking system," Proceedings of the 2nd Workshop on Information Hiding, Portland, Oregon, pp. 1-21, 1998.

[3] Shamir, A., "How to share a secret," Communication of the ACM, Vol. 22, No. 11, pp. 612-613, 1979.

[4] Naor, M. and Shamir, A., "Visual Cryptography," Lecture Notes in Computer Science, Vol. 950, pp. 1-12, 1995.

[5] Fang, W. P. and Lin, J. C., "Progressive viewing and sharing of sensitive images," Pattern Recognition and Image Analysis, Vol. 16, No. 4, pp. 632-636, 2006.

[6] Leung, B. W., Ng, F. Y., and Wong, D. S., "On the security of a visual cryptography scheme for color image," Pattern Recognition, Vol. 42, No. 5, pp. 929-940, 2009.
[7] Chen, T. H. , Wu, C. S. , and Lee, W. B. , "A novel subliminal channel found in visual cryptography and its application to image hiding," Proceedings of the 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kaohsiung, Taiwan, pp. 421-424, 2007.
[8] Thien, C. C. and Lin, J. C., "Secret image sharing," Computer & Graph, Vol. 26, pp. 765-770, 2002.
[9] Yang, C. N. and Chen, T. S., "Colored visual cryptography scheme based on additive color mixing," Pattern Recognition, Vol. 41, pp. 3114-3129, 2008.
[10] Lou, D. C., Chen, H. H., Wu, H. C., and Tsai, C. S., "A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares," Displays, Vol. 32, pp. 118-134, 2011.