Text-Based Visual Secret Sharing

Wen-Pinn Fang **Jia-Hao Hsu** **Wei-chi Cheng**

Department of Computer Science and Information Engineering, Yuanpei University, Hsinchu, Taiwan,R.O.C.

Summary
This paper proposed a text form visual sharing scheme. Different from traditional visual sharing scheme which handle with image, the proposed method shares text file. Secret information revealed after users stack two or more transparencies which print texts. The advantages of proposed method include not only the advantages of traditional visual sharing method, but also have the characteristic of friendly visual sharing method.

Keywords:
Visual secret sharing, text format, friendly sharing.

1. Introduction

With the advance of computer science and technology, the circulations and exchanges of information have created challenges to data security while the common methods applied are digital water marking and cryptography. In recent years scientists have begun to investigate the techniques of visual secret sharing and its feature is messages can be decoded without computer application and the difficulty of being decoded while messages are shared. However, with visual secret sharing, the quality of images after being decoded is lower than the one via visual sharing so that it causes difficulties for managements and this paper will present discussions about the related issues.
To offer solutions to the problems listed above, this paper suggests word visual secret sharing whose advantages are easier managements of shared data and not easy to be hacked. More importantly, this method has most of the features the visual secret sharing owns. This paper also contains an introduction to Visual Cryptography in the second part, the proposed methods in the third part, the experimental results are in the fourth part and a discussion and a conclusion are in the fifth part.

2. Visual cryptography

Visual cryptography was first proposed by M. Naor and A. Shamir [1] when the easiest version of producing two noise-like transparencies with each pixel is black or white 50% each. With a single transparency, the content cannot be recognized to show the original image, while the two transparencies Fig.1 (b) and (c) overlaid the original image can be shown as in Fig.1 (d). The theory is based on human eyes' relative cognition toward dark and light colors. The dark spots in one area are seen black by human eyes, if the original image is black, then the locations of dark spots in the area will be reversed and vice versa is white. First it is to create two basis matrices, as shown in Table 1, two corresponding points will be expanded into blocks, if the original image is black, the locations of the black points are reversed, on the contrary, the same. The overlaying produces expansion, however it is close to the result of the overlaid original image.

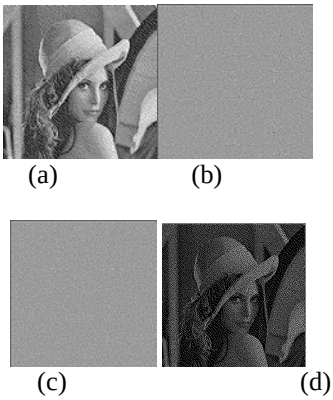


Figure 1. Examples of traditional visual cryptography (a) Original image , (b) (c) for the stars kept , (d) the superposed (b) and (c) the result.

Table 1, visual cryptography Method Description

Original image	corresponding block		Stacked Share
	Share 1	Share 2	
□	■□□■	□■■□	■■■■
	□■■□	■□□■	■■■■
■	■□□■	□■■□	■■■■
	□■■□	■□□■	■■■■

Manuscript received May 5, 2013
Manuscript revised May 20, 2013

3. Proposed methods

This paper proposes word visual secret sharing as the flow chart in Fig.2. First it takes a word file as a base and reads the shared secret image (this paper uses a passage of Chinese characters). After that, it needs a calculation of the locations of the characters and the secret image. The second transparency is created when the words are randomly located from the first transparency while the word production of the second transparency is accordant with random secret visual movement to compete the coding.

Encoding Algorithm

Input: Sharing text file F (length N), confidential information coordinates H, Sharing text length and width W × H , word size a × b

Output: Sharing S_1 、S_2 (length N)

j=0

For i=1 to N

x= (i MOD W) ×a

y=$\left\lceil \frac{i}{W} \right\rceil$ ×b

Δx =Random selection -1、0、1

Δy =Random selection -1、0、1

If i=H(j) then

Draw F(i) in S_1(x+Δx, y+Δy)

Draw F(i) in S_2(x-Δx, y-Δy)

Else

Draw F(i) in S_1(x+Δx,y+Δy)

Draw F(i) in S_2(x+Δx,y+Δy)

End if

End For

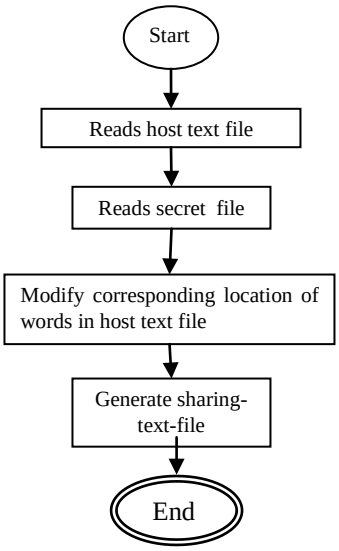


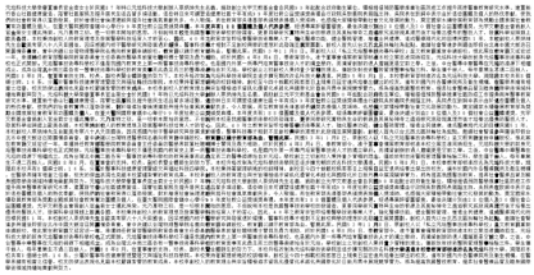
Figure 2. Sharing flow chart

4. Experimental results

This paper proposed a sharing scheme for text files. An experimental result is shown as below. Fig.3 (a) and (b) are the sharing text files. Fig.3 (d) is the stacked result. The letters “YPU” can be seen after the shares are stacked.

(a)

(b)



(c)

Figure 3. Experimental result (a) and (b) are share text file (c) is the stack result

5. Discussion and conclusion

This paper proposes a visual secret sharing of word files used in media. Sharing is for word files so that it is to be managed. Besides, locating of each word varies a little so that it is very difficult to identify the differences between original file and encoding file to reading quality. The advantage is to have only one word file without getting to read the hidden data. It reveals the hidden content after overlaying which is different from the traditional result via Visual cryptography. The features are shown in the sharing format without expanding sharing sizes. It is possible to

design n, r sharing in the future and different sharing systems.

References

[1] M. Naor and A. Shamir, “Visual Cryptography,” Advances in Cryptogoly --- Eurocrypt ’94, Lecture Notes in Computer Science, vol. 950, 1-12,Springer-Verlag, Berlin,1995

[2] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, “Visual Cryptography for General Access Structure”, Information and Computing, Vol. 129, 86-106, 1996

[3] H.C. Wu and C.C. Chang, “Sharing Visual Multi-secrets Using Circle Shares,” Computer Standards & Interfaces, Vol. 28, 123-135, 2005

[4] W.P. Fang, “Visual Cryptography in Reversible Style, ”IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing(IIHMSP2007), Kaohsiung, Taiwan, R.O.C, 2007, 11, 26～2007, 11, 28.

[5] Wen-Pinn Fang, “A Survey for Visual Sharing Scheme with Geometry Property, ”Journal of Image Processing and Communication, Vol. 2, No. 1, 2010, 12, pp. 35-39.

[6] W.P. Fang, “Non-expansion Visual Secret Sharing in Reversible Style, ”International Journal of Computer and Network Security, Vol. 9, No. 2, 2009, 2, 204-208

[7] W.P. Fang, “Maximizing the Secret Hiding Ratio in Visual Secret Sharing with Reversible Property, ”International Journal of Computer and Network Security.

[8] Kafri and E. Keren, “Encryption of Pictures and Shapes by Random Grids,” Optics Letters, Vol. 12, No. 6, 377 - 379, 1987.

[9] S. J. Shyu, “Image Encryption by Random Grids,” Pattern Recognition, Vol. 40, Issue 3, 1014 - 1031, 2007.

[10] T. H. Chen and K.H. Tsao, “Visual Secret Sharing by Random Grids Revisited”, Pattern Recognition, 2008, online(http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6V14-4V1TXMJ-1-1&_cdi=5664&_user=2414342&_orig=mlkt&_coverDate=11%2F30%2F2008&_sk=999999999&view=c&wchp=dGLzVtz-zSkzV&md5=0f9b092b81e841ed86e4a8c6eadd4a22&ie=/sdarticle.pdf)

[11] C. N. Yang, ”New Visual Secret Sharing Schemes Using Probabilistic Method,” Pattern Recognition Letter, Vol. 25 2004, 481–494

[12] W.P. Fang, J.C. Lin, 2006, 4, “Visual Cryptography with Extra Ability of Hiding Confidential Data” Journal of Electronic Imaging, 15, 023020

[13] R.Lukac and K.N. Plataniotis , “Bi-level Based Secret Sharing for Image Encryption”, Pattern Recognition Vol. 38, 2005, 767–772.

[14] W.P. Fang and J. C. Lin, “Multi-channel Secret Image Transmission with Fast Decoding: by using Bit-level Sharing and Economic-size Shares” International Journal of Computer and Network Security, 6, 2006, 6, 228-234.

Wen-pinn Fang received his BS degree in Mechanical Engineering in 1994 from National Sun Yat-sen University and his MS degree in Mechanical Engineering in 1998 from National Chiao Tung University, where he also got his PhD degree in Computer Science in 2006. His recent research interests include image sharing, pattern recognition, image processing and e-learning.

Wei-chi Cheng has been an English professional since 1999 when she gained her MA degree in English Languages and Literature in Providence University. Her recent research interests include EFL applications, learners’ personality types and motivation and mobile learning.

Jia-Hao Hsu received his BS degree in Department of Computer Science and Information Engineering in 2012 from Yanpei University. His is studying in master's degree. His recent research interests include Wireless, mobile devices, image sharing and e-learning.