Binary Image Visual Cryptography

Yaseen Hikmat Ismaiel, PhD
Lecture
Department computer science
Collage of computer and mathematic science
Mosul University

Muna Mahmood Khether
Diploma student
Department computer science
Collage of computer and mathematic science
Mosul University

ABSTRACT

Modern computer networks make it possible to distribute documents quickly and economically. This is because of the decreasing cost of the equipment needed to copy, print, process the information. The widespread adoption of electronic distribution of material is accompanied with more emphasis on data security. One of the modern data security methods is Visual Cryptography. Visual Cryptography(VC) is the technique that is used for securing data specially image-based secrets such as credit card information, personal health information, military maps and personally identifiable information and commercial identification data.

Visual Cryptography allow us to share secret effectively and efficiently, the secret image can be distributed in to two or more shares, when shares are superimposed exactly together the original image would be discovered with human visual system(HVS) without out aid of computer or without performing complicated computations.

Keywords

Visual Cryptography (VC), Binary image.

1. INTRODUCTION

VC is introduced by first in 1994 Naor and Shamir [1]. The idea is allowing data in the case of images, to be digitally transmit or stored with no concern that the data could be intercepted and accidentally revealed to unauthorized parties. The main description associated with VC is the message being encoded into two or more shares. When looking at each one separately the shares reveal no information about message contained in and reassemble random noise will show the secret [1,2].

In 1996, G.Ateniese, and et. al [3] describes general access structure which it gives a set of n share separated into two subsets named as qualified and forbidden according to the importance of shares. The secret information can be retrieve only by stacking any of the k shares from qualified subset of shares that is called as subset n and that secret information can’t be retrieved by k or more shares of forbidden set.

In 1997, E.Verheul and H.V tilborg [4] using black and white images and it develops first gray colored VC scheme for sharing single sequence colored secret images. Each pixel is divided into b subpixels of color 0, 1,…… c-1. These subpixels interrelate which each other in the following way: When subpixels are put on top of each other and held to the light, one sees a "generalized" or, i.e. if all subpixels are of color i then one sees light of color i, otherwise one sees no light at all (i.e. black).

In 2005 hiding binary image into two meaningful shares Chin-Chen Chang et al [5] suggested spatial-domain image hiding schemes. The two secret shares will be embedded into two gray level cover images. To decode the hidden messages, embedding images can be superimposed.

Liguo Fang [6] recommend a (2, n) scheme based on combination. Threshold visual secret sharing schemes mixing XOR and OR operation with reversing and based on binary linear error correcting code was recommended by Xiao-qing and Tan [7].

The disadvantage of the above schemes is that only one set of confidential messages can be embedded, to share large amount of confidential messages a number of shares must generated.

For coding multiple secret, Wu and Chen [8] were first researchers to present the VC schemes to share two secret images in two shares. They hide two secret binary images into two random shares, with the names A and B, the first secret can be retrieved by stacking the two shares, denoted by A⊗ B, and the second secret can be obtained by first rotating A ϴ anti-clockwise. The design with the rotation angle ϴ to be 90◦. However, it is simple to obtain that ϴ can be 180 or 270.

To overcome the angle limitation of Wu and Chen’s scheme [8], Hsu et al. [9] proposed a scheme to hide two secret images in two rectangular shares with arbitrary rotating angles.

S J Shyu et al [10] advise multiple secrets sharing scheme encodes a set of $n\geq 2$ secrets into two circular shares. The n secrets can be retrieved one by one by stacking the first share and the rotated second share with n different rotation angles.

To provide more randomness for generating the shares Mustafa Ulutas et al [11] give an advice of the secret sharing scheme based on the rotation of the shares. In this scheme shares are rectangular in shape and are created in full randomly manner, Stacking the two shares reveal the first secret. Rotating the first share by 90° counterclockwise , stacking it with the second share reconstructs the second secret image.

Tzung-Her Chen et al [12] presented multiple secret images encryption schemes by rotating random grids, with no any pixel expansion and codebook redesign.

In order to encode four secrets into two shares and recovering the reconstructed images with no distortions Zhengxin Fu et al [13] intended a rotation VC scheme. Rotation VC scheme construction based on correlative matrices set and random permutation, which might be used to encode four secret images into two shares.

Jonathan Weir et al [14] suggested sharing multiple secrets with visual cryptography. A master key is generated for all of the secrets; correspondingly, secrets are shared using the master key and multiple shares obtained.

2. BINARY IMAGES IN VC

The process behind VC is allowing the messages to be contained in seemingly random shares. The generation of these shares demonstrates the concept of VC along with its strengths and limitations. Assuming that the message being encrypted is a binary image with p pixels, each of these pixels are separately encoded with a subpixel grouping with s pixels. This will allow n shares to be generated by using these subpixel groupings.

"Each share is a collection of m black and white subpixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions"[8].

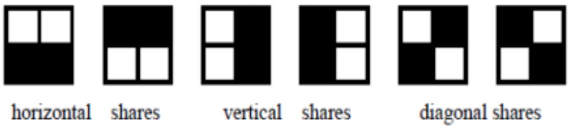


Fig.1: Shares most commonly used for VC **algorithms.**

The most frequently used subpixel groupings in VC algorithms that is shown in Fig.1. The image is encoded in n shares and the message would be revealed by stacking k of these n shares. still, if k -1 shares are stacked together, the encoded message cannot be revealed, the generation of these shares is based on the value of the pixel and the probability of a subpixel group occurring. Share generation scheme for k = 2 and n = 2 is shown in Fig.2[10].

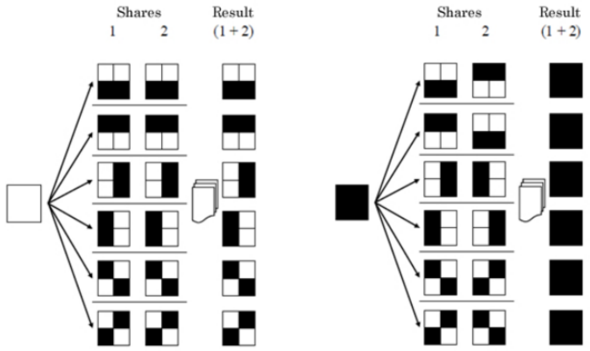


Fig.2: A share generation scheme corresponding to k=2 and n=2 ,with the probability of 50% [2]

Next fig.3 is an example for (3,3) k out of n that could be used to distribute an image into four shares, stacking all of them are needed to reveal the secret image. The shares have the following properties:-

- Any single share have 5 black subpixels.
- Any stacked pairs contains exactly 7 black subpixels.
- Any stacked triple contains 8 black subpixels.
- When all four in each row of fig.3 are combined the top row (black pixel) contains 9 subpixel (black).
- When all four in each row of fig.3 are combined the bottom row will contain only 8 (allow light to pass for necessary contrast to read the image [1].

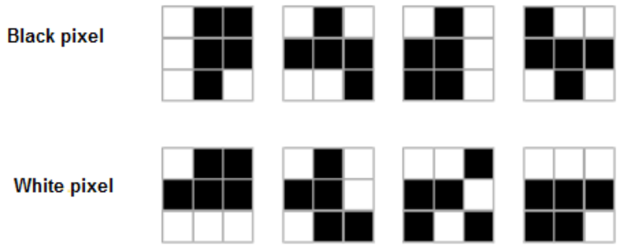


Fig.3 VC scheme for (3,3) k out of n secret sharing problem.

3. PROPOSED METHOD

3.1 It is noted in previous studies that all methods used in the VC of binary images lead to an increase in the size of the original image and the size and number of the shares and this considered a weak point where it requires a large storage space and increasing the time it takes to send shares to the receiver.

Also some methods may result in a slight distortion in the recovered image, in addition, some proposed methods may facilitate the detection of the original image by rotating the shares at a certain angle as in [8]. In this paper, a proposed method of binary image VC so that we can overcome most of the weaknesses in the previous methods. The proposed method introduced a new method of VC, including obtaining the shares by dividing the original image and thus obtaining small shares in the total number of shares that the combination of them equals the size of the original image. The recovered image is 100% similar to the original image.

Adding a level of security during the process of construction and retrieval of shares by using a key which the length of key representing the number of shares entered randomly and relying on it is configured shares and retrieval. The generated shares are random and the intruder cannot retrieve the original image or predict its content.

3.2 The Proposed Method Algorithm

The steps of the proposed algorithm can explained with the following steps:

1. Read the binary image ,read the key.

2. The length of the key must equal the number of shares.

3. Depending on the length of the key the rows of the original image will be distributed vertically on the shares depending on the key value for example, the key is 213 the number of the shares will be 3 which equal the length of the key. The first three rows will be taken from the image and placed in share 2 vertically, the second 3 rows will go to share 1, the third 3 rows will be in share number 3 then take the next three rows and so on. In some cases the key may be in non-standard format and must be converted to the standard format before using it in the share configuration as shown in table (1). Flowchart fig.4 to show the coding process:-

Table (1): key convention to the standard states.

Original key	Standard key
5928	2413
0559	1234
Help	2134
Soon	4231
4z8y	1324

4. The process of retrieving the original image takes place in the receiving side, where the secret key is entered with the shares. As in the encryption, the length of the key must be equal to the number of shares the key is first converted to the standard format. Depending on the key sequence, the original image is created by dragging the columns from the shares on to the image rows.

For example, if the key is 213, the first three columns of the share two will be withdrawn at the reconstructed image rows horizontally followed by the first three columns of the share one will be reconstructed as second three rows and withdrawn the three columns of share 3 as third three rows and thus continue in the same sequence to get the original image. Flowchart Fig.5 illustrate the process of original image retrieval process.

All the simulation work has been implemented in MATLAB environment 2013 using general MATLAB toolbox and Image processing toolbox. We have taken an arbitrary input binary image as test image for proposed method and applied the above algorithms. Fig.6 show the secret images with the shares created, size details and time needed for the process.

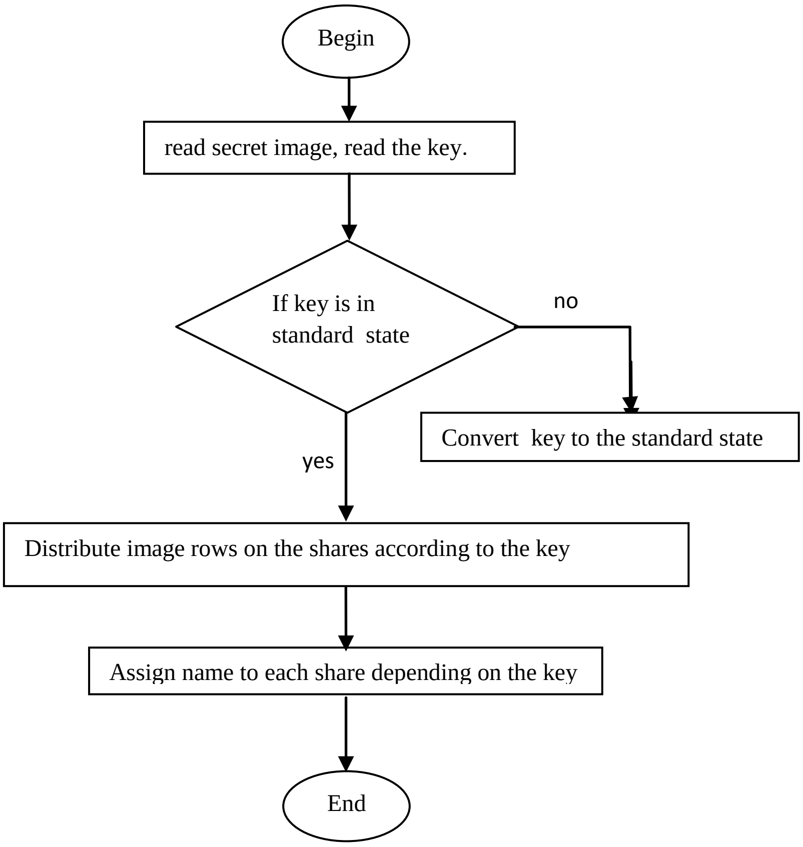

Begin
read secret image, read the key.
If key is in standard state
no
Convert key to the standard state
yes
Distribute image rows on the shares according to the key
Assign name to each share depending on the key
End

Fig.4: VC proposed method flowchart for creating shares.

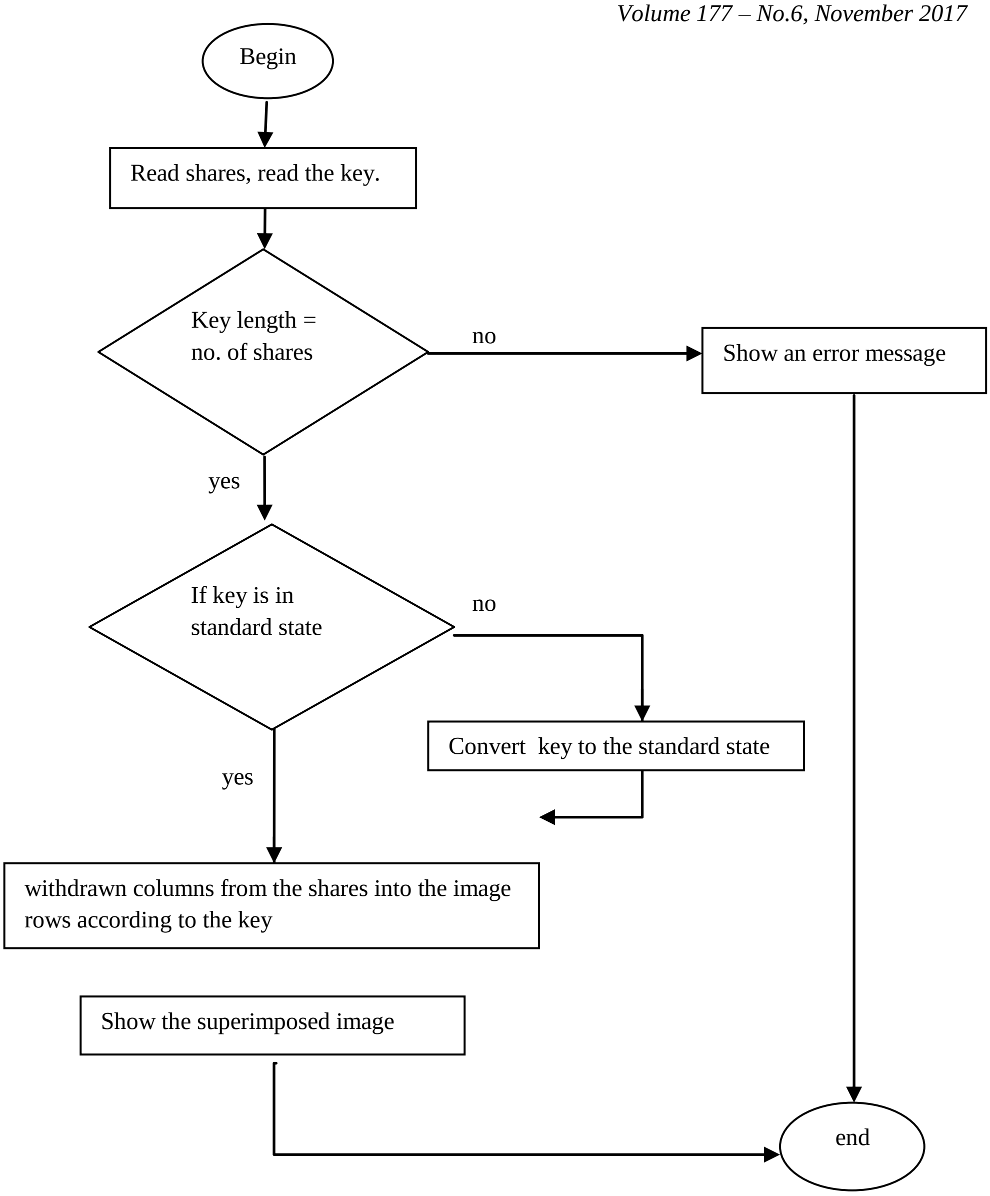
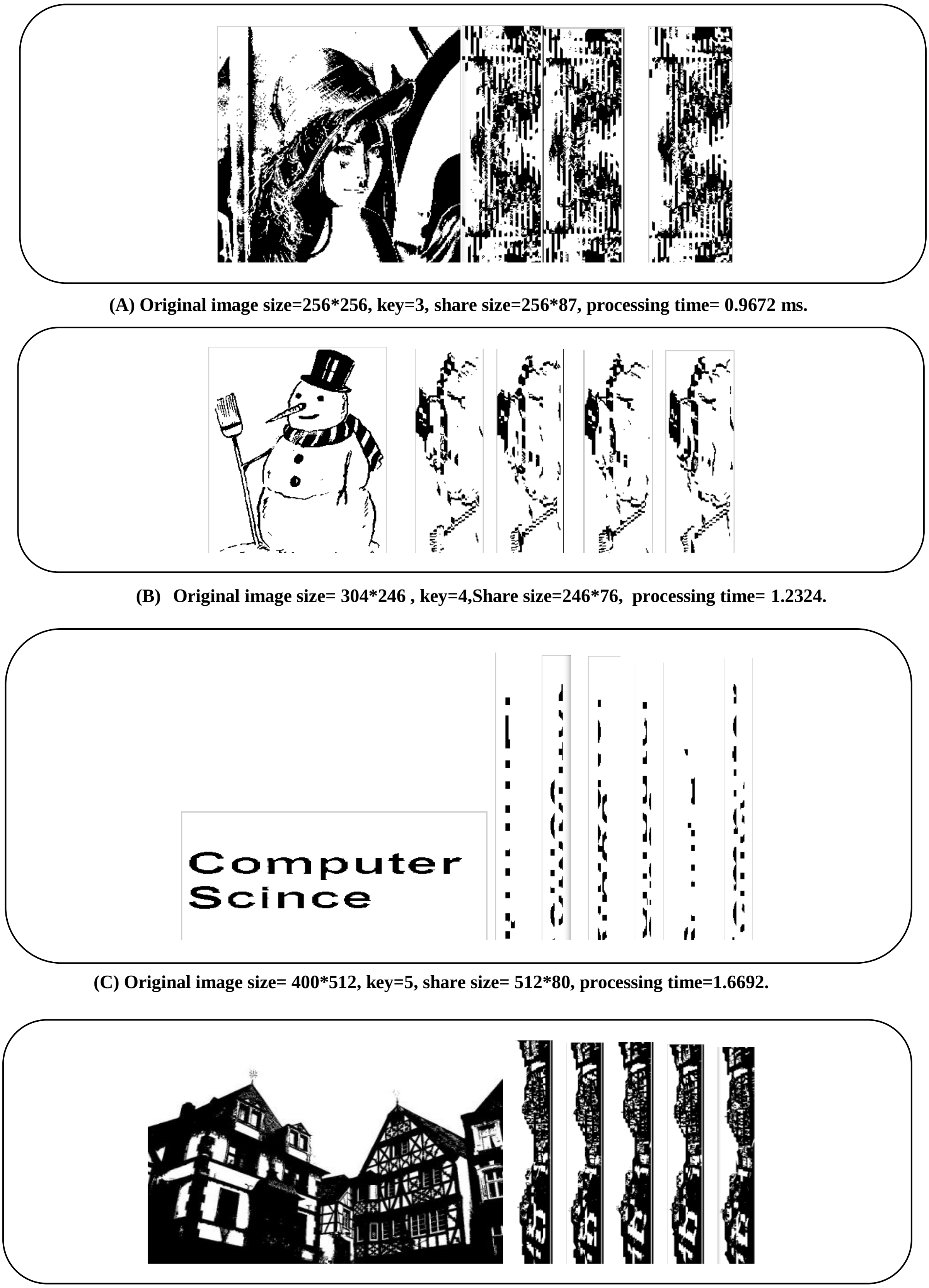

Begin
Read shares, read the key.
Key length = no. of shares
no
Show an error message
yes
If key is in standard state
no
Convert key to the standard state
yes
withdrawn columns from the shares into the image rows according to the key
Show the superimposed image
end

Fig.5: VC proposed method flowchart for the process of superimposing original image.



(A) Original image size=256*256, key=3, share size=256*87, processing time= 0.9672 ms.

(B) Original image size= 304*246 , key=4,Share size=246*76, processing time= 1.2324.

(C) Original image size= 400*512, key=5, share size= 512*80, processing time=1.6692.

(D) Original image size=252*50, key=6, share size=500*42, processing time= 1.7004.

Fig.6:The secret images and the shares created for each.

4. CONCLUSION AND FURTHER WORK

In this paper a new robust Visual Cryptography scheme has been proposed. The proposed method divided the original image into number of shares (depending on the key values) , the size of share is smaller than the original image size (image size/key) , so there is no increasing in the size . converting original image rows into columns and distributed into shares depending on the key adding secure level for protection and the resulted shares image differs from the original image with more confusion . As explained in Fig.6 the computation time is small and when stacking shares in the recipient side the resulted image is 100% similar the original image with no distortion .

As VC schemes operate at the pixel levels, each pixel on one share must be matched correctly to its right position in the original image in the reconstruction method depending on the key value .

The future study involves more number of shares and to implement on gray and color images with more security options to increase the image protection without performing complicated computations, also the proposed method can be used in many interested area like image steganography and watermarking.

5. REFERENCES

[1] M. Noar and A. Shamir, 1995. "Visual cryptography," Advances in Cryptology – EUROCRYPT'94, pp. 1-12.

[2] Naor, Moni, and Adi Shamir, 1996. "Visual cryptography II: Improving the contrast via the cover base". International Workshop on Security Protocols. Springer Berlin Heidelberg.

[3] Giuseppe Ateniese ,Carlo Blundo and Alfredo De Santis, 1996. "Visual Cryptography for General Access Structures, information and computation" article no. 0076,129, 86106 .

[4] E. Verheul and H. V. Tilborg, 1997. ”Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes". Designs, Codes and Cryptography, 11(2) , pp.179–196,

[5] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, 2005. “Sharing A Secret Two-Tone Image In Two Gray-Level Images”, Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05).

[6] Liguo Fang, BinYu, , On Sep 5, 2006. “Research On Pixel Expansion Of (2,n) Visual Threshold Scheme”, 1st International Symposium on Pervasive Computing and Applications ,pp. 856-860, IEEE.

[7] Xiao-qing Tan, , 2009 .“Two Kinds Of Ideal Contrast Visual Cryptography Schemes”, International Conference on Signal Processing Systems, pp. 450-453.

[8] C.C. Wu, L.H. Chen, 1998. “A Study On Visual Cryptography”, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C.

[9] H.-C. Hsu, T.-S. Chen, Y.-H. Lin, March 2004. “The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing”, in Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001.

[10] S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, and K. Chen, , 2007. “Sharing multiple secrets in visual cryptography”, Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651.

[11] Mustafa Ulutas, Rıfat Yazıcı, Vasif V. Nabiyev, Güzin Ulutas, (2,2) , 2008. “Secret Sharing Scheme With Improved Share Randomness”, 978-1-4244-2881-6/08, IEEE.

[12] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, 2008. “Multiple-Image Encryption By Rotating Random Grids”, Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256.

[13] Zhengxin Fu, Bin Yu, 2009. “Research On Rotation Visual Cryptography Scheme”, International Symposium on Information Engineering and Electronic Commerce, pp533-536.

[14] Weir, WeiQi Yan, 2009. “Sharing Multiple Secrets Using Visual Cryptography”, 978-1-4244-3828-0/09, IEEE, pp 509-512.