VISUAL CRYPTOGRAPHY SCHEMES WITH PERFECT RECONSTRUCTION OF WHITE PIXELS

THOMAS MONOTH, BABU ANTO P

Abstract: The existing pixel patterns for the visual cryptography scheme are based on the perfect reconstruction of black pixels (PRBP). Mathematically in PRBP the white pixels are represented by 0 and the black pixel by 1. In the usual binary image, the number of white pixels is much larger than the number of black pixels. Therefore, the perfect reconstructions of black pixels in visual cryptography schemes can decrease the contrast. Here, a visual cryptography scheme which is focused on the perfect reconstruction of white pixels (PRWP) and hence can provide better clarity is presented. As in the case of all existing binary image file formats, PRWP represents white pixel by 1 and black pixel by 0.

Keywords: Perfect reconstruction of white pixels, Secret sharing, Visual cryptography, Visual secret sharing.

Introduction: In 1995, Naor and Shamir introduced a very interesting and simple cryptographic method called visual cryptography to protect secrets [1]. Basically, visual cryptography has two important features. The first feature is its perfect secrecy and the second is its decryption method which requires neither complex decryption algorithms nor the aid of computers. It uses only human visual system to identify the secret from the stacked image of some authorized set of shares. Therefore, visual cryptography is a very convenient way to protect secrets when computers or other decryption devices are not available. The simple decryption method is the reason that attracts many researchers to make further detailed enquiries in this research area. Nowadays, many related methods concerning the theory and the applications of visual cryptography are proposed.

An extended visual cryptography scheme (EVCS) was proposed by Ateniese et al. [2]. Extended visual cryptography schemes permits the construction of visual secret sharing schemes within which the shares are meaningful as opposed to having random noise on the shares. After the sets of shares are superimposed, this meaningful information disappears and the secret is recovered. This is the basis for the extended form of visual cryptography [3-4].

The image size invariant visual cryptography was proposed by Ito et al.[5]. The traditional visual cryptography schemes employ pixel expansion. In pixel expansion, each share is m times the size of the secret image. Thus, it can lead to the difficulty in carrying these shares and consumption of more storage space. Ito's scheme removes the need for this pixel expansion. That is, the reconstructed image is identical to the original image. There are also some other studies which focus on the methods without pixel expansion [6-12].

In 1996, Naor and Shamir proposed an alternative VCS model for improving the contrast in [13]. In 1999, Blundo et al. [14-16] analyzed the contrast of the reconstructed image in k-out-of-n VCS schemes . Blundo et al. gave a complete characterization of 2-out-of-n VCS schemes having optimal contrast and minimum pixel expansion in terms of certain balanced incomplete block designs. Blundo et al.'s research results are valuable for the researchers who are interested in the area of visual cryptography. The other research works done by different authors are found in [17-21].

The Existing Model: The existing model for black-and-white visual cryptography schemes has been developed by Naor and Shamir [1]. In this model, both the original secret image and the share images contain only black and white pixels. Each pixel in the original image is subdivided into a set of m black and white subpixels in each of the n share images. The set of subpixels can be represented by an n x m Boolean matrix S = [sij], where

sij = 1 $\Leftrightarrow$ the jth subpixel in the ith share is black.

sij = 0 $\Leftrightarrow$ the jth subpixel in the ith share is white.

To distinguish between black and white pixels in the recovered image, we define a fixed threshold parameter d, where $1 \leq d \leq m$. If $\omega H(V) \geq d$, then the subpixels are interpreted as black, and if $\omega H(V) \leq d - \alpha .m$, then the subpixels are interpreted as white, where $\omega H(V)$ is the Hamming weight (the number of ones) of the 'or' ed m-vector V. The threshold parameter (d) is a numeric value for the point at which black areas are distinct from white. The m denotes the pixel expansion. This represents the loss of resolution from the original image to the share image, which is to be as small as possible. The parameter $\alpha > 0$ is called the relative contrast difference of the scheme. It is desirable to have a relative contrast difference as large as possible to minimize the loss of contrast in the recovered image. The value $\alpha.m$ is the contrast, which is greater than or equal to 1 and hence ensures that the black and white areas will be distinguishable. The formal definition for black-and-white visual cryptography schemes by Naor and Shamir [1] is:

Definition 1: A solution to the k-out-of-n visual cryptography scheme consists of two collections of n x m Boolean matrices C0 and C1. To share a white pixel, the dealer randomly chooses one of the matrices in C0 and to share a black pixel, the dealer randomly chooses one of the matrices in C1. The chosen matrix defines the colour of the m subpixels in each one of the n transparencies. The solution is considered valid if the following three conditions are fulfilled:

1.For any $S \in C_0$, the OR m-vector V of any k of the n rows in S satisfies $\omega H(V) \leq d - \alpha .m$.

2.For any $S \in C_1$, the OR m-vector V of any k of the n

rows in S satisfies $\omega H(V) \geq d$.

3.For any subset {r1, r2, . . . , rt} {1,2,. . .,n} with t<k, the two collections of t x m matrices obtained by restricting each n x m matrices in C_0 and C_1 to rows r1, r2,…, rt, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

For a visual cryptography scheme to be valid, these three conditions must be satisfied. The first two conditions ensure that some contrast in the scheme is maintained, and the third condition ensures that security in the scheme is maintained. The third condition states that no information can be obtained if less than k shares are stacked together. In other words, a matrix in $C_0 \cup C_1$, to less than k rows, will not be able to tell whether the matrix is from C_0 or C_1.

To encrypt a white pixel of the original image, a matrix is randomly chosen from C_0 and is used to create the shares. A black pixel is encrypted by randomly choosing a matrix from C_1. At least two matrices in each collection are needed so that the dealer can randomly choose one of them. If the matrix is chosen randomly, a cryptanalyst, examining less than k shares, will not be able to predict the color of the pixel in the original secret image based on the pixel positions, since each matrix in the collection is equally likely to have been chosen.

Visual Cryptography Scheme with PRWP: Let P = {1, . . . , n} be a set of elements called participants, and let 2P denote all the subsets of P. Let ΓQual ⊆ 2P and ΓForb⊆ 2P, where ΓQual ∩ ΓForb = Ø. Here the members of ΓQual are referred to as qualified sets and the members of ΓForb are called forbidden sets. The pair (ΓQual, ΓForb) is called the access structure of the scheme.

Define Γ0 to consist of all the minimal qualified sets:

Γ0 = {A ∈ ΓQual : B ΓQual for all B⊆ A, B ≠ A }

The secret image consists of a collection of black and white pixels. Each pixel appears in n versions called shares. Each share is a collection of m black and white subpixels. The resulting structure can be described by an n × m Boolean matrix S = [sij] where

(sij) = 0 the jth subpixel in the ith share is black. (sij) = 1 the jth subpixel in the ith share is white.

Therefore the gray level of the combined share, obtained by stacking the transparencies i1, . . . , is, is proportional to the hamming weight ωH (V) of the m-vector V = OR(ri1, . . . , ris), where ri1 , . . . , ris are the rows of S associated with the transparencies stacked. This gray level is interpreted by the visual system of the users as black or white in according with some rule of contrast.

Definition 2*:* Let (ΓQual , ΓForb) be an access structure on a set of n participants. Two collections of n × m Boolean matrices C_0 and C_1 constitute a visual cryptography scheme (ΓQual, ΓForb) VCS with PRWP if there exists values β(m) and threshold $1 \leq tX \leq m$ satisfying:

1.Any qualified set X = {i1, i2, . . . , ip} ∈ ΓQual can recover the shared image by stacking their transparencies.

Formally, for any M ∈ C0, the "or" V of rows i1, i2, . . . , ip satisfies $\omega H(V) \geq tX - \beta(m)$; whereas, for any M ∈ C1, it results that $\omega H(V) \leq tX$.

2.Any nonqualified set X = {i1, i2, . . . , ip} ∈ ΓForb has no information on the shared image.

Formally, the two collections of p×m matrices Dt, with t ∈ {0, 1}, obtained by restricting each n × m matrix in Ct to rows i1, i2, . . . , ip are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first condition is related to the contrast of the image. The number β(m) is referred to as the contrast of the image. The second condition is security, which implies that by inspecting the shares of a nonqualified subset of participants one cannot gain any advantage in deciding whether the shared pixel was white or black.

The Construction of Basis Matrices: Let (ΓQual, ΓForb) be an access structure on a set of n participants. A (ΓQual , ΓForb) VCS with PRWP with relative difference α(m), contrast β(m) and threshold $1 \leq tX \leq m$ is realized using the n × m basis matrices MS0 and MS1 if the following two conditions hold:

1. If X = {i1, i2, . . . , ip} ∈ ΓQual is a qualified set, then the "or" V of rows {i1, i2, . . . , ip} of MS0 satisfies $\omega H(V) \geq tX - \beta(m)$; whereas, for MS1 it results that $\omega H(V) \leq tX$.

2.If X = {i1, i2, . . . , ip} ∈ ΓForb is not a qualified set then the two p×m matrices obtained by restricting MS^0 and MS^1 to rows {i1, i2, . . . , ip} are equal up to a column permutation.

The collections C_0 and C_1 are obtained by permuting the columns of the corresponding matrix (MS^0 for C_0 and MS^1 for C_1) in all possible ways.

Formula 1 (Relative Difference):

Let $\omega H(MS^0)$ and $\omega H(MS^1)$ be the hamming weight corresponding to the basis matrices MS^0 and MS^1. Then relative difference α(m) is defined as:

$\alpha(m) = (\omega H(MS^0) - \omega H(MS^1))/ m$

Formula 2(Contrast):

Let α(m) be the relative difference and m be the pixel expansion. The formula to compute contrast in different VCS with PRWP is:

$\beta(m) = \alpha(m).m , \quad \beta(m) \geq 1$

The Construction of 2-out-of-2 VCS with PRWP: The basic idea of visual cryptography scheme with PRWP can be explained by 2-out-of-2 VCS. The pixel layouts for the scheme are as shown in table 1.

Table 1 The pixel layout for 2-out-of-2 VCS with PRWP

Original Pixel	Pixel Value	Share1	Share2	Share1+ Share2
□	1	■□	□■	□
□	1	□■	■□	□
■	0	■□	■□	■□
■	0	□■	□■	□■

The basis matrices, MS^0 and MS^1 are:

$$MS^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad MS^1 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

The relative difference $\alpha(m)$ and contrast $\beta(m)$ can be computed as:

$\alpha(m) = ½$, $\beta(m) = 1$

The matrices C_0 and C_1 are :

$$C_0 = \{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \} \text{ and}$$

$$C_1 = \{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \}$$

While observing the basis matrices MS^0 and MS^1, S^0 of VCS becomes MS^1 of PRWP scheme and S^1 becomes MS^0. Therefore, in VCS with PRWP scheme, to share a white pixel, the dealer randomly selects one of the matrices in C_1, and to share a black pixel, the dealer randomly selects one of the matrices in C_0 of Noar & Shamir scheme. From the results, both the relative difference and contrast of VCS with PRWP are equal to that of Noar & Shamir scheme.

The Experimental Results of VCS with PRWP : For assessing the feasibility, some experiments were conducted using 2-out-of-2 VCS with PRWP) is shown below :

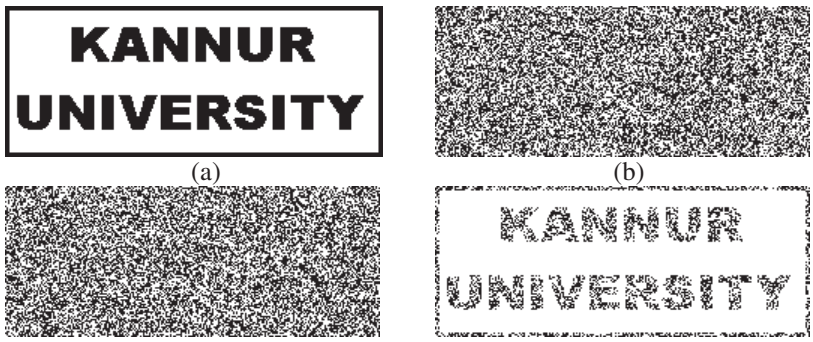

Figure 1 The 2-out-of-2 VCS with PRWP: (a) SI, (b) S1, (c) S2 and (d) S1+S2

Analysis of Experimental Results in VCS with PRWP: This section focuses on comparing the number of pixels in the reconstructed images of VCS with PRWP and Noar & Shamir scheme with the help of graphs.

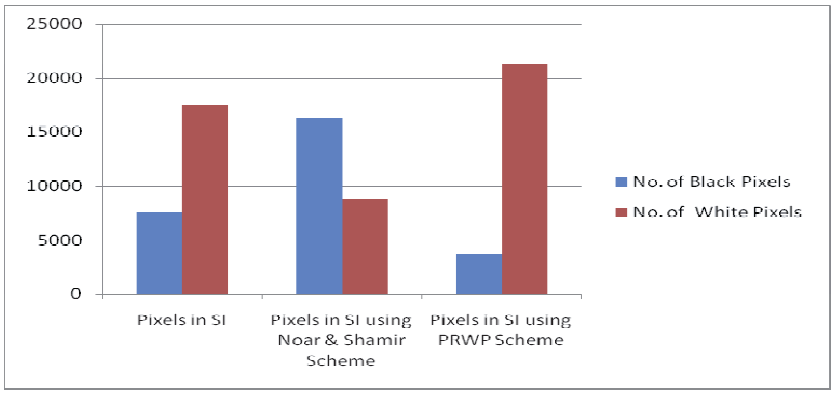

Figure 2 The graphical representation of 2-out-of-2 VCS with PRWP.

The graphs (Figure 2) show that the number of white pixels in the secret image is greater than the number of

black pixels in both the secret image. In the reconstructed secret images by using Noar & Shamir scheme, the number of black pixels is larger than the number of white pixels, which in turn reduces the contrast. In order to retain the contrast, the change of number of white (black) pixels in the original image to the reconstructed secret image should be as small as possible. In VCS with PRWP method, the rate of this change can reduced to a considerable extent. From this one can reach the conclusion that the VCS with PRWP method gives a clearer image than Noar & Shamir scheme.

Conclusions: This paper presents new methods for contrast-enhanced visual cryptography schemes with PRWP. This method is explained and implemented with examples. The contrast of the presented visual cryptography schemes and traditional VCS are compared here. Using this method, some experiments were also conducted based on different VCS. These results are analysed by using tables and graphs and are also compared with the features of existing visual cryptography schemes.

References:

1. M. Naor and A. Shamir, Visual Cryptography, Advances in Cryptology-Eurocrypt'94, LNCS 950,pp. 1-12, 1995.
2. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended schemes for visual cryptography. Theoretical Computer Science 250,pp. 1–16,1996.
3. G. Ateniese, C. Blundo, A. D. Santis, and D. Stinson, Constructions and bounds for visual cryptography, Proceeding of the 23rd International Colloquium on Automata, Languages and Programming (ICALP '96), pp.416–428, 1996.
4. G. Ateniese, C. Blundo, A. D. Santis, and D. Stinson. Visual cryptography for general access structures, Information and Computation, 129(2):86–106, 1996.
5. Ito, R., Kuwakado, H., Tanaka, H, Image size invariant visual cryptography. IEICE Transactions E82-A(10),pp. 2172–2177 1999.
6. Yang, C.N., New visual secret sharing schemes using probabilistic method. Pattern Recognition Letters 25(4), pp.481–494, 2004.
7. Yang, C.N., Chen, T.S., Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. Pattern Recognition Letters 26(2), pp. 193–206, 2005.
8. Yang, C.N., Chen, T.S., Size-adjustable visual secret sharing schemes. IEICETransactions 88-A(9),pp. 2471–2474,2005.
9. Yang, C.N., Chen, T.S., New size-reduced visual secret sharing schemes with half reduction of shadow size. IEICE Transactions 89-A(2),pp. 620–625, 2006.
10. Yang, C.N., Chen, T.S., Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation. Pattern Recognition 39(7), pp.1300–1314, 2006.
11. Liguo Fang and BinYu, Research on Pixel Expansion of (2,n) Visual Threshold Scheme, Proc. of the IEEE International Symposium on Pervasive Computing and Applications, pp.856-860, 2006.
12. Ching-Sheng Hsu, Shu-Fen Tu, and Young-Chang Hou, An Optimization Model for Visual Cryptography Schemes with Unexpanded Shares, ISMIS 2006, LNAI 4203, pp.58 – 67, 2006.
13. M. Naor and A. Shamir., Visual Cryptography II : Improving the Contrast Via the Cover Base, Security in Communication Networks, pp. 197-202, 1996.
14. C. Blundo, Alfredo De Santis and Douglas R. Stinson, On the contrast in visual cryptography schemes, Journal of Cryptology, 12, pp. 261-289,1999.
15. C. Blundo, A. D. Bonis, and A. De Santis. Improved schemes for visual cryptography, Designs, Codes and Cryptography, 24(3), pp.255–278, 2001.
16. C. Blundo, P. D'arco, A. De Santis, and D. R. Stinson, Contrast optimal threshold visual cryptography, SIAM Journal of Discrete Math. 16(2), pp. 224–261, 2003.
17. T. Hofmeister, M. Krause, and H. U. Simmon, Contrast-optimal k out of n secret sharing schemes in visual cryptology, Theoretical Computer Science, pp. 471–485, 2000.
18. Matthias Krause and Hans Ulrich Simon, Determining the Optimal Contrast for Secret Sharing Schemes in Visual Cryptography, LATIN 2000, LNCS 1776, pp. 280-291, 2000.
19. R.Youmaran, A. Adler and A. Miri, An Improved Visual Cryptography Scheme for Secret Hiding, Proc. of the IEEE 23rd Biennial Symposium on Communications, pp. 340- 343, 2006.
20. Ching-Nung Yang and Tse-Shih Chen, Visual Secret Sharing Scheme: Improving the Contrast of a Recovered Image Via Different Pixel Expansions, ICIAR 2006, LNCS 4141, pp. 468 – 479, 2006.
21. Lin Kezheng, Fan Bo and Zhao Hong, Visual Cryptographic Scheme with High Image Quality, Proc. of the IEEE International Conference on Computational Intelligence and Security, pp.366-370, 2008.

* * *

Thomas Monoth/Assistant Professor/Department of Computer Science/Mary Matha Arts & Science College/ Vemom P.O., Mananthavady-670645/ Kerala/ India/tmonoth@yahoo.com/
Babu Anto P/ Associate Professor/Department of Information Technology/Kannur University/Kannur/ Kerala/ India.