Volume 5, No. 2, March 2014 (Special Issue)

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Dissolution of Secret Sharing as meaningful shares & Review on Extended Visual Cryptography Scheme

T.Ram Kumar
Vignan Institute of Technology and Aeronautical Engg.
Deshmukhi, Nalgonda(dt). India

Abstract: Visual cryptography (VC) schemes hide the secret image into two or more images which allows the encoding of a secret image into shares distributed to participants. The secret image can be recovered simply by stacking the shares together without any complex computation involved. An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS. In this paper, a color visual cryptography scheme producing meaningful shares is proposed. These meaningful shares will not arouse the attention of hackers. The proposed scheme utilizes the halftone technique, cover coding table and secret coding table to generate two meaningful shares show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCSs in the . Comparative analyses have demonstrated that the new scheme is perfectly applicable and achieves a high security level.

Keywords – Secret Sharing Extended Embedded system, visual cryptography, Halftone Coloring.

I. INTRODUCTION

The idea of traditional secret sharing scheme that was invented by Shamir [1] and Blakley [2] independently, here is an example to illustrate the idea. Assume that a bank has a vault that must be opened by a secret key. The bank employs three senior tellers, but the bank does not want to trust any of them individually. Hence, they would like to design a system such that any two of the three senior tellers can open the vault together. This problem can be viewed as a (2,3) secret sharing scheme.

In general, a (k, n) secret sharing scheme is a method to share a secret K among n participants such that the following conditions hold:

Any k participants together can compute K. Any t participants, t < k, gain no information

about K.

Here is an example of a (2, 2) secret sharing scheme. Assume that the secret K is a binary sequence of length, i.e. $K = (k_1, k_2, \ldots., K_m)$. The two shares, S_1 and S_2 can be constructed as follow. The first share is chosen to be a random binary sequence of length m, say $S_1 = (S_{11}, S_{12}, \ldots., S_{1m})$. Then, we can compute the second share by doing "exclusive-or" on K and S_1.

$$_{2i} \quad {}^{k}{}_{i} \quad {}^{s}{}_{1i} \quad , i \;\; 1, \;\; , m \qquad (1)$$

For example, assume that m=2, k = (0,1). Then the two shares can be constructed as follow:

s_1 (0,0) , then s_2 s_1 K (0,1) .

s_1 (0,1) , then s_2 s_1 K (0,0) .

s_1 (1,0) , then s_2 s_1 K (1,1) .

s_1 (1,1) , then s_2 s_1 K (1,0) .

However, looking only at one share, say s_1 , any four values of K are possible. In other words, it gains no information about K if another share s_2 is unknown.

Associated secret sharing problem and its physical properties such as contrast pixel expansion and color were extensively studied by researchers worldwide. For example, Naor *etal.* [3] and Blundo*et al.* showed constructions of threshold VCS with perfect reconstruction of the black pixels. Ateniese*etal.* [4] gave constructions of VCS for the general access structure. Krishna *et al.*, Luo*et al.*, Hou*et al.*, and Liu *et al.* considered color VCSs. Shyu*et al.* proposed a scheme which can share multiple secret images [5]. Furthermore, Eisen*et al.* proposed a construction of threshold VCS for specified whiteness levels of the recovered pixels [6].The term of extended visual cryptography scheme (EVCS)was first introduced by Naor *et al.* in [3], where a simple example of (2,2)-EVCS was presented. In this paper, when werefer to a corresponding VCS of an EVCS, we mean a traditional VCS that have the same access structure with the EVCS. Generally, an EVCS takes a secret image and original share images as inputs, and outputs shares that satisfy the following three conditions: 1) any qualified subset of shares can recover the secret image; 2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image; 3) all the shares are meaningful images. EVCS can also be treated as a technique of steganography. One scenario of the applications of EVCS is to avoid the custom inspections, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected.

II. SECTION II

A. *Related Work On Visual Secret:*

Naor and Shamir [3] proposed a visual secret sharing scheme (VSSS) that uses human visual system to decrypt the secret image without performing any cryptographic computation. The difference between a VSSS and a traditional secret sharing scheme is in how the secret is decrypted. Usually, the traditional secret sharing scheme requires computation over a finite field. In a VSSS, however, the computation is simply performed by the human visual system of the users.

It is important to realize that the construction of a secure VSSS is difficult. Suppose that a particular pixel P on a share S_1 is black. Whenever a set of shares (including s_i) is stacked together, the result must be black. It means that in the secret image, the pixel P must be black. In other words, we gain "some" information about the secret image be examining one of the shares, and the security condition does not allow this. Naor and Shamir [3] proposed a VSSS that solved this problem by splitting each original pixel into *m* sub-pixels. In this section, we will introduce this idea and explain how to decrypt "visually".

In general, a VSSS assumes that the secret is a collection of black and white pixels, or a binary image, and each pixel is encrypted separately. Each original pixel encrypts into *n* shares, and each share is a collection of *m* black and white sub-pixels, which are printed near to each other such that human visual system averages their individual black/white contribution. The VSSS can be described by an n m Boolean matrix M where $M[i, j]$ 1iff the *j*-thsub-pixel in the *i*-th shares is black, and $M[i, j]$ 0 iff the *j*-thsub-pixel in the *i*-th shares is white.

To decrypt the secret image, we simply xerox*t* shares onto transparencies, and then stacking them together with perfect alignment. We can see a stacked version share *V* whose black subpixels are represented by the Boolean "or" of row $s_1, s_2, \ , s_t$ in M .

$$V \ s_1 \ \ s_2 \ \ \ s_t \qquad (2)$$

The gray level of this stacked share *V* is proportional to the Hamming weight $H(V)$ of V . This gray level is interpreted by the visual system of the users as black if $H(V)$ d and as white if $H(V)$ d m for some fixed threshold 1 d m and relative difference 0 .

Here is a (2,2) example to illustrate the idea. A (2,2) VSSS can be described by the following 2 2 Boolean matrices.

$$M_0 \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, M_1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

In this example, a particular pixel *P* in the secret image is split into two subpixels, i.e. m 2 , in each of the two shares. If the given pixel *P* is white, we use M_0 to encrypt the pixel by setting the first row to s_1 and setting the second row to s_2 , s_1 (1,0) , s_2 (1,0) . The Hamming weight of the Stacked version share *V* is $H(V)$ 1, where$V$ s_1 s_2 (1,0) . If the given pixel *P* is black, we use M_1 to encrypt the pixel, and the Hamming weight is $H(V)$ 2 , where. In this example, the fixed threshold d 1 , and the relative difference 0.5 , by stacking s_1 and s_2 together, a pixel *P* is interpreted by the visual system of the users as white if the Hamming weight $H(V)$ 1 and as black if $H(V)$ 2 .

By permuting the columns of collections of 2 2 Boolean matrices.

$$C_0 \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\}, C_1 \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\},$$

To share a white pixel, we randomly choose one of the matrices in C_0 , and to share a

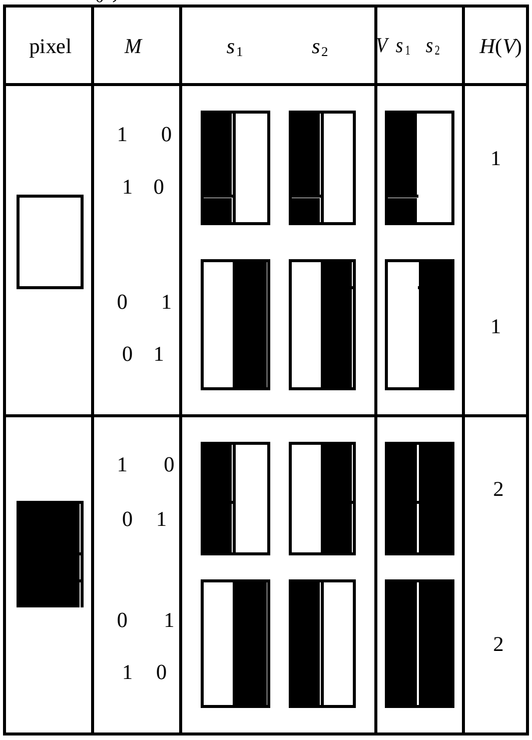
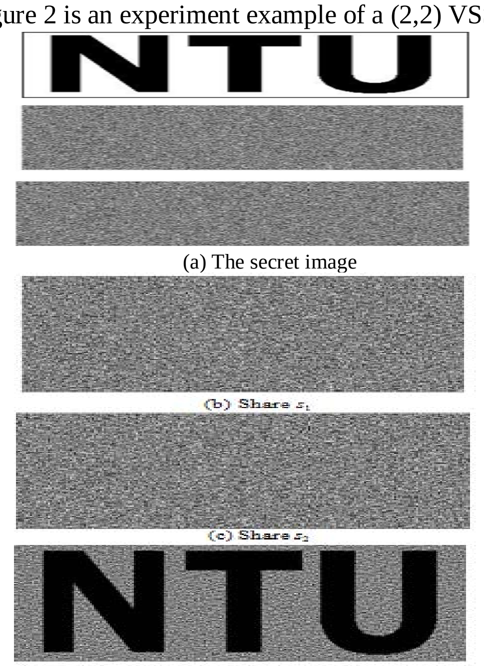


Figure: 2 Encrypting algorithm of a (2,2) VSSS

Black pixel, we randomly choose one of the matrices in C_1. Figure 1 illustrates the scheme byspecifying the algorithm for encrypting one pixel.

Note that permuting the column of M_0 and M_1 does not change the Hamming weight of the matrix. However, this procedure is required in order to satisfy the security condition.

In the discussion above, we introduce the algorithm for encrypting one pixel. This algorithm is to be applied for every pixel in the secret image to construct the two shares. Figure 2 is an experiment example of a (2,2) VSSS.



(a) The secret image

(b) Share s_1

(c) Share s_2

(d) Decrypted image V s_1 s_2

Figure 2 Experiment example of a (2,2) VSSS We can xtend this algorithm to a (k, n) VSSS as below:

a. Design M_0 and M_1 .

b. Construct C_0 and C_1 .

c. To share a white pixel, we randomly choose one of the matrices in C_0 , and to share a black pixel, we randomly choose one of the matrices in C_1 .

The scheme is valid if the following three conditions are satisfied:

d. For any M in C_0 , the "or" stacked version share V of any k of the n rows satisfies $H(V)\ d\ m$.

e. For any M in C_1 , the "or" stacked version share V of any k of the n rows satisfies $H(V)\ d$.

f. For t k, the "or" stacked version share V of any t of the n rows is a function of t , i.e. $H(V)\ f(t)$, regardless of whether the matrix were taken from C_0 or C_1 . In other words, it gains no information about the secret image by examining less than k shares.

In this stage, we already introduce the VSSS idea of Naor and Shamir. The problem is, however, how to design M_0 and M_1 .In the next section, we introduce the design method of a general (k, k) VSSS, i.e. the design method of M_0 and M_1 .A more general (k, n) VSSS can be extend from a

(k, k) solution.

III. SECTION

A. Visual Cryptography on other applications:

a. Halftone Gray scale & Color Visual Cryptography:

Digital half toning has been extensively used in printing applications where it has been proved to be very effective, for visual cryptography use of digital half toning is for the purpose of converting the gray scale image into a monochrome image. Once we have a binary image then the original visual cryptography techniques can be applied. For color images, there are two alternatives for applying digital half toning. One is to split the color image into channels of cyan, magenta and yellow. Then each channel is treated as a gray scale image to which half toning and visual cryptography are applied independently. After the monochrome sharesare generated for each channel, channels are combined separately to create the color shares. The alternative approach would be to directly apply color half toning, then perform the separation into color channels followed by the application of visual cryptography to each channel independently. Actually, these two approaches lead to the same results finally. There are many mature half toning techniques available for selection. We have experimented with the dispersed-dot dithering, clustered-dot dithering and error diffusion techniques. For the second approach, generalized error diffusion described in [13] was used. In practice, we have found that error diffusion usually produces superior quality results compared to the results produced using dithering arrays though both of the alternatives have an acceptable performance.

Half toning cryptographic is further divided into following

a) ***Color Half toning***: standard algorithms can be used for this, one could do the color channel splitting first and then do the gray scale half toning for each channel

$$I \xrightarrow{split\ \ CMY} [I^C, I^M, I^Y] \xrightarrow{halftoning} [I^C_{hft}, I^M_{hft}, I^Y_{hft}]$$

Or

$$I \xrightarrow{color\ \ halftoning} I_{hft} \xrightarrow{split\ \ CMY} [I^C_{hft}, I^M_{hft}, I^Y_{hft}]$$

Creation of shares the technique presented in this can be used for this step. Considering the case of (2,2) –VCS the steps are

$$I^C_{hft} \xrightarrow{(2,2)-VCS} [S^C_0, S^C_1]$$

$$I^M_{hft} \xrightarrow{(2,2)-VCS} [S^M_0, S^M_1]$$

$$I^Y_{hft} \xrightarrow{(2,2)-VCS} [S^Y_0, S^Y_1]$$

Sub sampling for reconstruction, these operations need to be performed where every block of four pixels is sub-sampled into one pixel of the final image.

b. Visual Cryptography with Perfect Restoration:

Digital half toning techniques results in some downgrading of the original image quality due to its inherently lossy nature and it is not possible to recover the original image from its halftone version. A new encoding method which allows us to transform gray scale and color images into monochrome ones without loss of any information. Furthermore, we seamlessly incorporate this new encoding scheme into our visual cryptography techniques, that it can allow perfect recovery of the secret gray scale or color image. In short, we will refer to this proposed scheme as PVCS (Perfect Visual Cryptographic Scheme).The novelty of our approach is that it not only allows the secret image to be just seen but allows the secret image to be reconstructed with perfect quality.

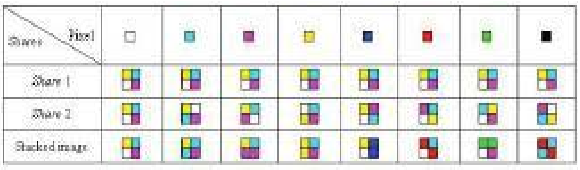
c. Color Visual Secret Scheme:

Visual color methods used same technique to decompose the color secret image into three images such as cyan magenta yellow then halftone technique used to translate the three color images into halftone images a color halftone image can be generated.

Figure 3 Color decomposition

CONFERENCE PAPER
Two day National Conference on Advanced Trends and Challenges in Computer Science and Applications
Organized by: Shree Vishnu Engineering College for Women, Bhimavaram A.P.
Schedule: 18-19 March 2014

Table 1 Secret Coding table



The color halftone image generation process is shown in figure 2; halftone image takes eight different colors to display cyan magenta yellow black red green blue and white. This method describe the details for each pixel of the color halftone image following the process must be done 2*2 blocks are builds according to share 1 and foupixels C,M,Y and W are randomly permuted then the number of blocks is calculated for share according to the color ratio of the four pixels with the coding table. For example if one pixel of the color halftone image is green then the pixel color ratio would be 100% 0% and 100% for C,M, and Y [7] respectively. Block in share 1 is the permutation of pixels cyan magenta yellow white then the above information is a produce block of share 2 where the permutation of the pixels is yellow magenta cyan and white. When all pixels are done processed two shares are produced. Each block of the two [8] shares will be composed of C,M, Y and W then the secret image can be readily recognized visually when the two shares are stacked together.

IV. SECTION

A. *Problem definition:*

Encoding scheme which allows a secret image shares into n participants this kind of process is visual cryptography. Set of participants is able to recover the secret image without any cryptographic knowledge. To share this kind of construction our analysis realized by embedding random shares into meaningful covering shares and we call it embedded color visual cryptography.

a. *Comparative study:*

Visual cryptography is the art of science of encrypting the image in such a way that no one apart from the sender and recipient even realizes the original image a form of security through obscurity, by contrast cryptography obscures the original image but it does not conceal the fact that it is not the actual image. Previous work of visual cryptography does not provide a friendly environment encrypt or decrypt the data or images. Compare to previous analysis visual cryptography provides a friendly environment to deal with images generally cryptography tools supports only one kind of images formats, this application supports graphical image format and portable network graphics formatted images and our application has been developed using swing applet technologies provides a friendly environment to users. Proposed extended visual cryptography is flexible in the sense that there exist two tradeoff between the share pixel expansion and the visual quality of the shares between the secret image pixel expansion and the visual quality of the shares. Flexibility allows the dealer to choose the proper parameters for different applications. Visual quality shares embedded visual color scheme is competitive with that of many well-known surveys.

b. *Analysis Results:*

The secret image used was a 25*256 color image and the cover images were also 256*256 color images. Share 1 and share 2 were 512*512 pixels each. By stacking share 1 and share 2 together the secret image peppers shows can be retrieved. The first cover image “Lena” and second cover image “Goldhill” are shown in Fig. 4 (a) and Fig. 4 (b), respectively. *Share* 1 and *Share* 2 are shown in Fig. 5

(a) and Fig. 4 (b), respectively. The reconstructed secret image is shown in Fig.6. As the analysis have revealed, scheme can successfully conceal the secret image inside the meaningful shares, and later the secret image can be recovered simply by stacking *Share* 1 and *Share* 2 together. However, checking out the analysis in detail, we found that certain areas of the recovered secret image were darker in color than their counterparts in the original secret image. The cause can be either region II or region I, depending on which one was black when *Share* 1 and *Share* 2 were stacked. As part of the analysis, we have also verified the security of the shares. Before producing block 3 and block 4, the proposed scheme must first learn the colors of the extracted pixels from the secret image. Then the obtained colors must meet their matches in the coding table so that a suitable block can be produced.

Figure 4 shows cover image over image and secret image

Figure 5 share 1 and share 2

Figure 6 stacking of share 1 and share 2

V. CONCLUSION

Construction of EVCS which was realized by embedding the random shares into the meaningful covering

CONFERENCE PAPER
Two day National Conference on Advanced Trends and Challenges in Computer Science and Applications
Organized by: Shree Vishnu Engineering College for Women, Bhimavaram A.P.
Schedule: 18-19 March 2014

shares, few color VC schemes produce meaningful shares, but we consider this a pretty meaningful field of research to explore. The shares of the proposed scheme are meaningful images, and the stacking of a qualified subset of shares will recover the secret image visually. We show two methods to generate the covering shares, and proved the optimality on the black ratio of the threshold covering subsets. We also proposed a method to improve the visual quality of the share images, we extend a single pixel into a 2×4 block. However, the size of the share remains the same as what happens in the 2×2 pixel expansion case. This way, a considerable part of the storage space can be saved, and more importantly, the shares do not look like random noise. Comparisons on the Analysis show that the visual quality of the share of the proposed embedded EVCS is competitive with that of many of the well-known EVCSs in the survey.

VI. REFERENCE

[1] Shamir, “How to share a secret.” Communications of the ACM 22 (1979), 612-613.

[2] G. R. Blakley, “Safeguarding cryptographic keys.” In “Proceedings of the National Computer Conference, 1979”, American Federation of Information Processing Societies Proceedings 48 (1979), 313-317

[3] C. Blundo, A. De Bonis, and A. De Santis, “Improved schemes forvisual cryptography,” Designs, Codes and Cryptography, vol. 24, pp.255–278, 2001.

[4] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, “Visual cryptographyfor general access structures,” Inf. Computat., vol. 129, pp.86–106, 1996.

[5] S. J. Shyu, S. Y. Huang, Y. K. Lee,R. Z.Wang, andK.Chen, “Sharingmultiple secrets in visual cryptography,” Pattern Recognit., vol. 40, no.12, pp. 3633–3651, 2007.

[6] P. A. Eisen and D. R. Stinson, “Threshold visual cryptographyschemes with specified whiteness levels of reconstructed pixels,”Designs, Codes and Cryptography, vol. 25, pp. 15–61, 2002.

[7] Y. C. Hou, “Visual cryptography for color images,” Pattern Recognition, Vol. 36, pp.1619-1629, 2003.

[8] T. Katoh and H. Imai, “An extended constructions method of visual secret sharing scheme,” IEICE Trans. Fundamentals, Vol. 179-A, No. 8, pp. 1344-1351, Aug. 1996.

[9] Color Visual Cryptography Scheme Using Meaningful Shares. Hsien-Chu Wu1, Hao-Cheng Wang2, and Rui-Wen Yu3 Eighth International Conference on Intelligent Systems Design and Applications

[10] IEEE Transactions on Information Forensics and Security, Vol. 6, no. 2, June 2011 307 Embedded Extended Visual Cryptography Schemes Feng Liu and Chuankun Wu, Senior Member, IEEE