ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Embedded Extended Visual Cryptography Schemes

Dr. S.Thajoddin
Associate Professor in Mathematics,
Osmania College, Kurnool.

Arif Khan
Assistant Professor in Mathematics,
Osmania College, Kurnool.

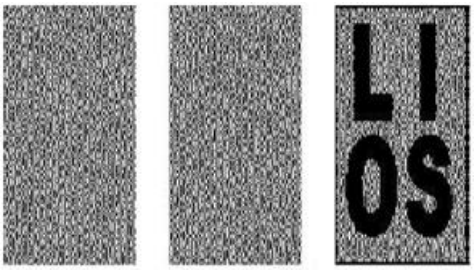
ABSTRACT:

A visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into shares distributed to participants. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. 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, we propose a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded EVCS. Experimental results compare some of the well-known EVCSs proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCSs in the literature. In addition, it has many specific advantages against these well-known EVCSs, respectively.

INTRODUCTION:

THE basic principle of the visual cryptography scheme (VCS) was first introduced by Naor and Shamir. VCS is a kind of secret sharing scheme that focuses on sharing secret images. The idea of the visual cryptography model proposed in is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation OR. We call a VCS with random shares the traditional VCS or simply the VCS. In general, a traditional VCS takes a secret image as input, and outputs shares that satisfy two 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. An example of traditional (2,2)-VCS can be found in Fig. 1, where, generally speaking, a –VCS means any out of shares could recover the secret image. In the scheme of Fig. 1, shares (a) and (b) are distributed to two participants secretly, and each participant cannot get any information about the secret image, but after



stacking shares (a) and (b), the secret image can be observed visually by the participants. VCS has many special applications, for example, transmitting military orders to soldiers who may have no cryptographic knowledge or computation devices in the battle field. Many other applications of VCS, other than its original objective (i.e., sharing secret image), have been found, for example, authentication and identification, watermarking and transmitting passwords etc. The associated secret sharing problem and its physical properties such as contrast, pixel expansion, and color were extensively studied by researchers worldwide. For example, showed constructions of threshold VCS with perfect reconstruction of the black pixels. Furthermore, Eisen *et al.* proposed a construction of threshold VCS for specified whiteness levels of the recovered pixels.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The term of extended visual cryptography scheme (EVCS) was first introduced by Naor *et al.* in, where a simple example of (2,2)-EVCS was presented. In this paper, when we refer 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. Examples of EVCS can be found in the experimental results of this paper, such as Figs. 2–9. 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.

EXISTING SYSTEM:

Visual cryptography is the art and science of encrypting the image in such a way that no-one apart from the sender and intended 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.

LIMITATIONS OF EXISTING SYSTEM:

The existing system does not provide a friendly environment to encrypt or decrypt the data (images).

PROPOSED SYSTEM:

Proposed system **Visual cryptography** provides a friendly environment to deal with images. Generally cryptography tools supports only one kind of image formats. Our application supports .gif and .png (portable network graphics) formatted images and our application has been developed using swing and applet technologies, hence provides a friendly environment to users.

ADVANTAGES OF PROPOSED SYSTEM:

EVCS is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares and between the secret image pixel expansion and the visual quality of the shares. This flexibility allows the dealer to choose the proper parameters for different applications. Comparisons on the experimental results 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 literature.

Halftoning Technique by Using Dithering Matrix

One of the main drawbacks of the VCSs proposed and is that, they cannot deal with the gray-scale image. MacPherson proposed a VCS to deal with the gray-scale image; however, it has large pixel expansion c*m, where c is the number of the gray-levels and m is the pixel expansion of the corresponding black and white VCS. In order to deal with the gray-scale image, the halftoning technique was introduced into the visual cryptography . The halftoning technique (or dithering technique) is used to convert the gray-scale image into the binary image. This technique has been extensively used in printing applications which has been proved to be very effective. Once we have the binary image, the VCS proposed , and can be applied directly. However, the concomitant loss in quality is unavoidable in this case. Many kinds of halftone algorithms have been proposed in the literature. In this paper, we make use of the patterning dithering . The patterning dithering makes use of a certain percentage of black and white pixels, often called patterns, to achieve a sense of gray scale in the overall point of view. The pattern consists of black and white pixels, where different per-

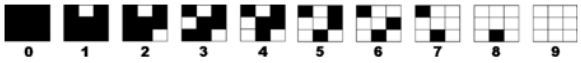


Fig 1. Halftoned patterns of the dithering matrix D_0 of the gray-levels .

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

centages of the black pixels stands for the different graynesses. The halftoning process is to map the gray-scale pixels from the original image into the patterns with certain percentage of black pixels. The halftoned image is a binary image. However, in order to store the binary images one needs a large amount of memory. A more efficient way is by using the dithering matrix. The dithering matrix is a $c \times d$ integer matrix, denoted as D. The entries, denoted as $D_{i,j}$ for ≤ i ≤ c-1 of the dithering matrix are integers between 0 and (cd-1) , which stand for the gray-levels in the dithering matrix. Denote $g \in$ {0,..,cd} as the gray-levels of a pixel in the original image. The halftoning process is formally described in Algorithm 1. Generally, for an input image of size , the halftoning process runs on each pixel in I as follows.

Algorithm 1: The halftoning process for each pixel in I :

Input: The c*d dithering matrix D and a pixel x with gray-level g in input image I

Output: The half toned pattern at the position of the pixel x

For i=0 to d-1 do

For j=0 to d-1 do

If g=≤D then print a black pixel at position (I , j);

Else print a white pixel at position (i,j);

To describe the half toning process clearer, take the dithering matrix with 10(=3*3+1) gray-levels as an example, where the gray-levels of the original image range from 0 to 9.

Example 1:

Dithering matrix with 10 gray-levels D_0 is shown in MatrixI.

MATRIX I

DITHERING MATRIX WITH TEN GRAY –LEVELS D_0

$$D_0 = \begin{bmatrix} 7 & 0 & 5 \\ 2 & 4 & 6 \\ 3 & 8 & 1 \end{bmatrix}$$

In Algorithm 1, the half toning process causes the cd pixel expansion on the input image. We call it the halftone pixel expansion. In the rest of the paper, we denote s as the halftone pixel expansion, i.e.. x=cd Take the above dithering matrix D_0 as an example, the half toned patterns of the gray-levels 0,…,9 are shown in Fig 1.

CONCLUSION:

We proposed a construction of EVCS which was realized by embedding the random shares into the meaningful covering shares. 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. According to comparisons with many of the well-known EVCS in the literature the proposed embedded EVCS has many specific advantages against different well-known schemes, such as the fact that it can deal with gray-scale input images, has smaller pixel expansion, is always unconditionally secure, does not require complementary share images, one participant only needs to carry one share, and can be applied for general access structure.

Furthermore, our construction is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares and between the secret image pixel expansion and the visual quality of the shares.

REFERENCES:

[1] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11,pp. 612–613, 1979.

[2] G. R. Blakley, “Safeguarding cryptographic keys,” in Proc. National Computer Conf., 1979, vol. 48, pp. 313–317.

[3] M. Naor and A. Shamir, " Visual cryptography," in Proc. EU-ROCRYPT'94, Berlin, Germany, 1995, vol. 950, pp. 1–12,Springer-Verlag, LNCS.

[4] M. Naor and B. Pinkas, "Visual authentication and identification," inProc. CRYPTO'97, 1997, vol. 1294, pp. 322–336, Springer-VerlagLNCS.

[5] T. H. Chen and D. S. Tsai, "Owner-customer right protection mech-anism using a watermarking scheme and a watermarking protocol,"Pattern Recognit., vol. 39, pp. 1530–1541, 2006.

[6]P.Tuyls,T.Kevenaar,G.J.Schrijen,T.Staring,andM.VanDijk,"Security displays enabling secure communications," in Proc. First Int. Conf. Pervasive Computing, Boppard Germany, Springer-Verlag.

[7]C.Blundo,A.DeBonis,andA.DeSantis,"Improvedschemesfor visual cryptography," Designs, Codes and Cryptography , vol. 24, pp. 255–278, 2001.

[8] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryp-tography for general access structures," Inf. Computat., vol. 129, pp. 86–106, 1996.

[9] N. K. Prakash and S. Govindaraju, "Visual secret sharing schemes for color images using halftoning," in Proc. Int. Conf. Computational Intelligence and Multimedia Applications (ICCIMA 2007), 2007, vol. 3,pp. 174–178.

[10] H. Luo, F. X. Yu, J. S. Pan, and Z. M. Lu, "Robust and progressive colorimage visual secret sharing cooperated with data hiding," in Proc. 2008 Eighth Int. Conf. Intelligent Systems Design and Applications, 2008, vol. 3, pp. 431–436.

[11] Y. C. Hou, "Visual cryptography for color images," Pattern Recognit., vol. 1773, pp. 1–11, 2003.

[12] F. Liu, C. K. Wu, and X. J. Lin, "Color visual cryptography schemes," IET Inf. Security, vol. 2, no. 4, pp. 151–165, 2008.

[13]S.J.Shyu,S.Y.Huang,Y.K.Lee,R.Z.Wang,andK.Chen,"Sharing multiple secrets in visual cryptography," Pattern Recognit., vol. 40, no.12, pp. 3633–3651, 2007.

[14] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," Designs, Codes and Cryptography , vol. 25, pp. 15–61, 2002.

[15] S. Droste, "New results on visual cryptography," in Proc. CRYPTO'96,1996, vol. 1109, pp. 401–415, Springer-Verlag Berlin LNCS.

[16] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," ACM Theoretical Comput. Sci.,vol. 250, no. 1–2, pp. 143–161, 2001.