International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 4, August 2012 www.ijcsn.org ISSN 2277-5420

Construction of Extended Visual Cryptography Scheme for Secret Sharing

[1]T.Rajitha, [2]Prof P.Pradeep Kumar, [3]V.Laxmi

[123]Department of CSE, Vivekananda Institute of Technology and Science
Karimnagar, AP, India

Abstract

Visual Cryptography facilitates hiding a secret image into n number of shares distributed to n number of participants. This kind of scheme is very useful as the participants in such security systems need not know the cryptographic knowledge in order to recover the secret image from the shares. This phenomenon is known as VCS (Visual Cryptography Scheme). An extended VCS is the one which is capable of generating meaningful shares when compared with the shares of the VCS. This paper proposes construction of EVCS by embedding the random shares (result of VCS) into covering images. The empirical results revealed that the proposed EVCS is more secure and flexible than the EVCSs found in literature.

Index Terms – VCS, random shares, covering shares, secret sharing.

1. INTRODUCTION

VCS was first introduced by Naor and Shamir. As described in [1] and [2], it is a secret sharing scheme which focuses on sharing secret images. This idea as proposed in [3] is to divide a secret image into number of random shares. These shares can't provide any information about secret image. However, they can bestow the size of the secret image. By stacking two shares the secret image which has been divided can be recovered. Therefore, it is understood that VCS takes an image as input and generate random shares that satisfy the conditions such as a) Secret image can't be obtained from any forbidden subset of shares. b) Secret image can be recovered from a subset of shares. The specialty of VCS is that, the secret image in Fig. 1 has two random shares namely (a) and (b). When they are distributed to different participants, they can't individually recover image. By stacking both the shares, it is possible to obtain original secret image.

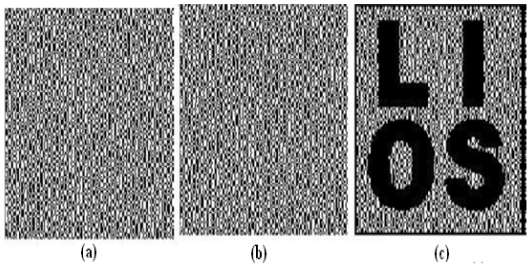

Fig. 1: Traditional VCS

As can be seen in fig.1, the VCS system converts given IMGE into random shares. To the naked eye, the random shares do not providing meaning. The VCS system has many applications in the real world. They include transmission of military orders securely, authentication and authorization [4], transmitting passwords [5] and so on. The researchers worldwide focused in physical properties like color, pixel expansion etc. For instance in [12] proposed a construction of VCS based on threshold for levels of whiteness; color VCS was considered in [8]-[10]. In [11] a scheme is proposed which allows sharing of multiple secret images.

Naor et al. [3] introduced EVCS (Extended Visual Cryptography Scheme) with a simple example. This paper proposes EVCS corresponding to VCS. The EVCS takes a secret image and the original share images as input and generates shares that can satisfy the criteria given below.

- Secret image can be recovered from any subset of shares.
- Forbidden shares can't be used to obtain secret image.
- All the shares are meaningful images.

Fig. 2: Shares and original secret image

EVCS is something similar to stereography where covering shares are meaningful and people do not suspect and detect the images that actually contain secret image. In [13], [14], [15], [16] and [17] EVCSs were proposed. In [18] half toning techniques were used by Zhou et al. in their EVCS. They also used complementary images for covering sharing images'

visual information. Error diffusion technique was used by Wang et al. to propose three EVCSs [19] and that resulted in nice looking shares. Complementary shares are also used by their first EVCS as proposed in [18]. Auxiliary black pixels are used in their second EVCS for covering shares information. Wang et al. proposed the method of their third EVCS. Each qualified subset in method 2 of Wang et al. does not require complementary images. Instead this method is only used for threshold access structure. The process of generating auxiliary black pixels of the method is similar to the approach followed in this paper. In case of third method od Wang et al. the shared images are changed besides getting extra black pixels in order to cover visual information. The drawback of this method is the fact that each share gets affected in terms of visual effect by the content of other shares. That is also affected by the content of original share images.

Fig. 3 Proposed EVCS

Fig. 4: Experimental results of EVCS of [21]

Fig. 5: Proposed EVCS for fine share images

Fig. 3, 4 and 5 show the experimental results of EVCS of various kinds. Fig. 5 shows EVCS results for fine share images where the size of images is 768 x 768. For the same size images experimental results are shown in fig. 4 which is taken from [19]. For the same size images the fig. 3 also shows the result of proposed scheme.

2.VCS AND HALFTONING TECHNIQUE

In this section the conventional VCS and Half toning technique are described before presenting the proposed scheme in the next section. In traditional VCS the participants of secret sharing scheme are represented as V = {0, 1, 2, …, n-1). The qualified and forbidden subsets are represented as (Γ_{Qual}, Γ_{Forb}). The minimal qualified access structure and the maximum forbidden access structure are computed as follows:

$\Gamma_m = \{ A\varepsilon\, \Gamma_{Qual}: \square B\square\ A\rightarrow B\ !\varepsilon\, \Gamma_{Qual}\}$

and

$\Gamma_M = \{ A\varepsilon\, \Gamma_{Forb}: \square B\square\ A\rightarrow B\ !\varepsilon\, \Gamma_{Forb}\}$

3. Half toning Technique using Dithering Matrix

The drawbacks of VCSs proposed in [3], [6], [7] and [14] is that they can't work with gray scale image. The VCS that works with gray scale images was proposed by MacPherson [20]. Its main drawback is that it has long pixel expansion. Another technique introduced to work with gray scale images for visual cryptography is known as half toning technique used in [9], [16], [21], [22] and [23]. The half toning technique is also known as dithering technique. It is best used to covert a gray scale image into a binary image. This approach is every effective as the binary image allows the VCS to be applied as described in [3], [7], [6] and [14]. There are many types of algorithms existed on halftone technique. However, in this paper we make use of a technique known as dithering [24]. It makes use of certain amount of black and white pixels in the form of patterns in order to achieve the grayscale. The percentages of black and white pixels represent different grayness.

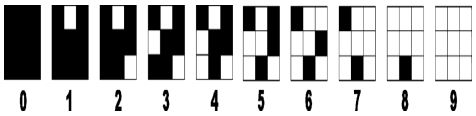

Fig. 6: Half toned patterns of dithering matrix with gray levels 0 to 9

The process of half toning is to map the pixels of gray scale from the original image into the black pixels with patterns. However, this process needs lot of memory. To overcome this problem, we use dithering matrix which a kind of integer matrix. The half toning process is described in algorithm 1 and the half toned patterns of dithering matrix with gray levels 0 to 9 is visualized in fig. 6.

Algorithm 1: The half toning process for each pixel in :

Input: The dithering matrix and a pixel with

gray-level in input image

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

For I = 0 to c -1 do

For j = 0 to d - 1 do

If g≤ Dij then print a black pixel at position (i,j);

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

Fig. 7: Half toning process

4. MAIN IDEA OF PROPOSED EVCS

The main idea in the proposed EVCS is to use the VCS to encode secret image. Then generating covering shares with visual meaning that are ready for embedding. Afterwards embedding the random shared into covering shares that have been generated earlier. This process is known as embedded process. The extraction process is very simple. A subset of covering shares is stacked in order to get the original image.

5. GENERATING COVERING SHARES BY USING THE DITHERING MATRICES

This section describes a procedure to construct covering shares by using **n** original shares. Dithering matrix is the technique used to achieve this. N number of dithering matrices is developed. Covering shares are obtained by half toning technique.

6. EMBEDDING VCS INTO THE COVERING SHARES

Once meaningful covering shares are generated using the dithering matrices, the realization of embedding process is described in algorithm 2 as shown in fig. 8.

Algorithm 2: The embedding process:

Input: The covering shares constructed in Section IV,

the corresponding VCS(C0,C1) with pixel expansion and the secret image I .

Output: The embedded shares e0,e1,…..en-1 .

Step 1: Dividing the covering shares into blocks that contain t(≥m) sub pixels each.

Step 2: Choose m embedding positions in each block in the n covering shares.

Step 3: For each black (respectively, white) pixel in I

, randomly choose a share matrix M Є C1 (respectively, M Є C0).

Step 4: Embed the m sub pixels of each row of the share

Matrix M into the m embedding positions chosen in Step 2.

Fig. 8 : Embedding Process

Embedding process is described in fig. 8. According to this embedding does mean that the pixels found in the embedding positions are replaced by share matrix's sub pixels. First of all the covering share is divided into blocks and sub pixels. In case if the pq is not multiple of t, padding is applied. In each t sub pixels, m positions are chosen. Such positions are known as embedding positions in this paper. All of the embedding positions must be same in order to support decode secret image correctly. By stacking embedded shares, the unused sub pixels are always black. The m pixels that are not participated in embedding process can recover secret image as part of VCS. The embedding process is visualized in the following figure.

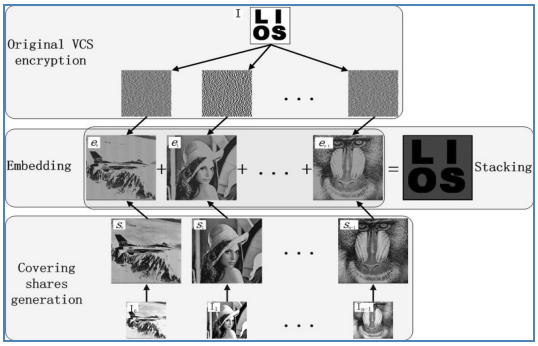

Fig. 9: Shows result of algorithm 2

As can be seen in the above figure, it is evident that first of all original VCS encryption is applied on secret image in order to generate random shares which have no visual meaning. Then the converting shares are generated by taking some images as input. Afterwards, the random shares are embedded into covering shares by following steps given in algorithm 2. The result of the embedding is the collection of meaningful covering

shares. By stacking a subset of covering shares, it is possible to obtain secret image as shown in fig. 9.

7. IMPROVING VISUAL QUALITY OF THE SHARES

In order to reduce black ratio, the steps given in fig. 10 are used.

The construction of the dithering matrix with reduced black ratio:

Step 1: Choose the m(<s) embedding positions in the

starting dithering matrix, and denote the gray-levels

in the embedding positions as(g0,…,gm-1) .

Remove these positions from the universal

set ς, and denote the new universal set asς1=(g0,g1,g2,…,gs-m-1), i.e., the rest gray-levels other than that in the embedding positions.

Step 2: Generate the covering subsets A1 for the universal setς1

, by using the methods proposed in Section IV-A,

where i=0,…,n-1.

Step 3: Convert the covering subsets into the dithering

Matrix Di , by using the method proposed in

Section IV-B, where i=0,…,n-1 .

Step 4: For each dithering matrix Di , swap the gray-levels{g0,…,gm-1}

in the embedding positions with

gray-levels {s-IAiI -1,…s-IAiI –m} in a similar

way as that of Construction 5. Denote the final

Dithering matrix as Di , where i=0,….,n-1.

Fig. 9: The construction of the dithering matrix with reduced black ratio

After the construction of the dithering matrix with reduced black ratio, the next needful step is the construction of the lcm(s,t)/s dithering by using steps provided in fig. 9.

The construction of the lcm(s,t)/s dithering

matrices for each input original share image for s≠t:

Step 1: Concatenatelcm(s,t)/s starting dithering matrices

with entries, and divide these starting dithering

matrices intolcm(s,t)/tblocks.

Step 2: Choose the m embedding positions in each block.

Step 3: Concatenate the lcm(s,t)/t blocks, and divide them

Intolcm(s,t)/s dithering matrices.

Step 4: For each dithering matrix, remove the embedding positions, and the rest of the positions in each dithering matrix constitute the universal set for this dithering matrix.

Step 5: Generate the dithering matrixes according to Construction 6.

Fig. 10: The construction of the lcm(s,t)/s dithering

The result of embedding process with different covering images which are meaningful is shown in fig. 11. The original share images are pertaining to boat, ruler, lena, baboon, and airplane. The secret image is also shown in fig. 11.

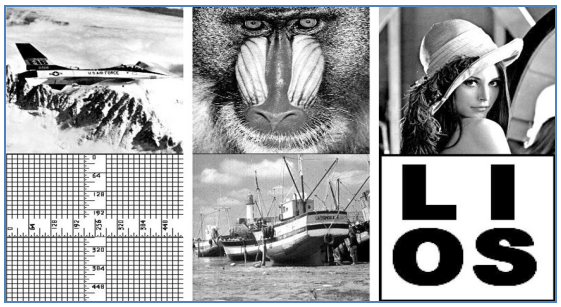

Fig. 11: Original sharing images and also secret image

EXPERIMENTAL RESULTS AND COMPARISONS

For measuring visual quality of covering shares, we provide two numerical measurements which are well known. They are Peak Signal-to-Noise Ratio (PSNR) and Universal Quality Index (UQI) [25]. The PSNR is defined as follows:

$$PSNR = 10 \log \frac{255^2}{MSE}$$

The results of the experiments with given measurements reveal that the proposed EVCS has competitive visual quality when compared with existing EVCS reviewed in the literature [13]–[15], [18], [16], [26], [19], [27]. It can deal with gray scale images; pixel expansion is small; complementary share images are not required by the proposed scheme. These are the specific advantages of our scheme when compared with other EVCS.

8. CONCLUSIONS

In this paper, we proposed a new scheme for construction of EVCS. This EVCS is realized by generating meaningful covering shares by embedding random shares into them. The qualified subset of meaningful covering shares can be stacked to obtain the original secret image that has been embedded. Two methods have been proposed to generate meaningful covering shares besides the method that improves visual quality of shares. The EVCS found in literature such as [13]–[15], [18], [16], [26], [19], [27] are compared with our scheme and the results revealed that our scheme has particular advantages over the well-known EVCSs available. Some of the advantages of our scheme include the ability to work with gray scale images; pixel expansion is smaller; always secure; no necessity for complementary shares. General access structure can be applied and each participant needs only one share to be carried. The proposed scheme is flexible and there are trade-offs between visual quality and secret image pixel expansion and between visual quality and share pixel expansion. The experimental results revealed that the proposed scheme is capable of providing high visual quality of shares which is competitive when compared with other EVCSs reviewed in the literature.

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. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.

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

[5] P. Tuyls, T. Kevenaar, G. J. Schrijen, T. Staring, and M. Van Dijk, "Security displays enabling secure communications," in Proc. First Int. Conf. Pervasive Computing, Boppard Germany, Springer-Verlag Berlin LNCS, 2004, vol. 2802, pp. 271–284.

[6] C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," Designs, Codes and Cryptography, vol. 24, pp. 255–278, 2001.

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

[8] 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.

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

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

[11] 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.

[12] 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.

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

[14] 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.

[15] D. S. Wang, F. Yi, and X. B. Li, "On general construction for extendedvisual cryptography schemes," Pattern Recognit., vol. 42, pp*3071–3082, 2009.*

[16] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," in *Proc. WSCG Conf. 2002*, 2002, pp. 303–412.

[17] D. S. Tsai, T. Chenc, and G. Horng, "On generating meaningful shares in visual secret sharing scheme," *Imag. Sci. J.*, vol. 56, pp. 49–55, 2008.

[18] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography,"*IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[19] Z.M.Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[20] L. A. MacPherson, "Grey Level Visual Cryptography for General Access Structures,"Master Thesis, University ofWaterloo,Waterloo, ON, Canada, 2002.

[21] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography,"in *Proc. 2003 Int. Conf. Image Processing*, 2003, vol. 1, pp. I-521–I-524.

[22] D. Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," *J. Electron. Imag.*, vol. 14, no. 3, p. 033019, 2005.

[23] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level imagesby dithering techniques," *Pattern Recognit. Lett.*, vol. 24, no. 1-3, pp.349–358, 2003.

[24] J. O. Limb, "Design of dither waveforms for quantized visual signals,"*Bell Syst. Technol. J.*, vol. 48, no. 7, pp. 2555–2582, 1969.

[25] W. Zhou and A. C. Bovik, "A universal image quality index,"*IEEE Signal Process. Lett.*, vol. 9, no. 3, pp. 81–84, Mar. 2002.

[26] Z. M. Wang and G. R. Arce, "Halftone visual cryptography through error diffusion," in *IEEE Int. Conf. Image Processing*, 2006, pp. 109–112.

[27] Z.M.Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via direct binary search," in *Proc. EUSIPCO'06*, Florence, Italy, Sep. 2006.