ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Error Diffusion Based Color Visual Cryptography for Secure Communication

K.V.Ramana[1], Y.AdiLakshmi[2]

Student, CSE, Gudlavalleru Engineering College, Gudlavalleru, India[1]

Associate Professor, CSE, Gudlavalleru Engineering College, Gudlavalleru, India[2]

Abstract: Color Visual Cryptography is the latest phenomenon for encrypting color secret images. Such secret messages are converted into number of color halftone image shares. The existing extended visual cryptographic schemes focused on gray scale and black and white visual cryptography schemes. These schemes are not suitable for color shares as they have different structures. There are some existing color visual cryptography schemes that might produce either meaningful or meaningless shares that produce less visual quality which lets people to suspect any kind of encryption involved in producing such shares. To overcome this problem, recently Kang et al. introduced error diffusion and the Visual Information Pixel (VIP) synchronization techniques to achieve color visual cryptography that can produce meaningful shares besides making the shares in such a way that they are pleasant to human eyes. In this paper implement the methods proposed by Kang et al. We also build a prototype application that demonstrates the proof of concept. The empirical results reveal that the proposed color visual cryptography can be used in real world applications.

Index Terms – Meaningful color shares, error diffusion, visual cryptography, digital half toning, secret sharing

INTRODUCTION

Naor and Shamir [1] introduced the visual cryptography (VC) which is meant for sharing secret images. It is a secret sharing scheme that helps in sharing secrets securely. A secret image is converted into shares that are given to participants one each. The participants can know the secret image by superimposing all transparencies. Information hiding is the main important application of VC. Its real world applications include print and scan applications [2], identification and visual authentication [3], watermarking [4], [5], copyright protection [6] and general access structures [7] and so on. Visual cryptography scheme takes a secret image as input and generate two or more shares. Those shares are not meaningful generally. But when the As can be seen in figure 1, it is evident that the secret image is divided into two meaningless shares (a) and (b) and then encrypted to form (d). The process of making it is described here. From secret binary image have pixels. Each pixel is embedded into white sub pixels of each share.

Many new VC schemes came into existence. Optimal contrast k-out-of-n scheme was introduced by Blundo [8] that can reduce the contrast loss problem in the images that have been reconstructed. In [7] Ateniese proposed a VC scheme that makes use of general access structure for VC. Random patterns are used to encore secret image into two shares. The extended VC schemes were proposed in [9], [10], [11], and [12]. Binary VC schemes were applied to gray scale after converting into halftone in [13] proposed by Hou. Extended visual cryptography (EVC) was proposed in [14] by Ateniese with meaningful color images. Nakajima [15] extended EVC to a scheme with natural grayscale shares are stacked, the original image can be produced. For instance Figure 1 shows this concept.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

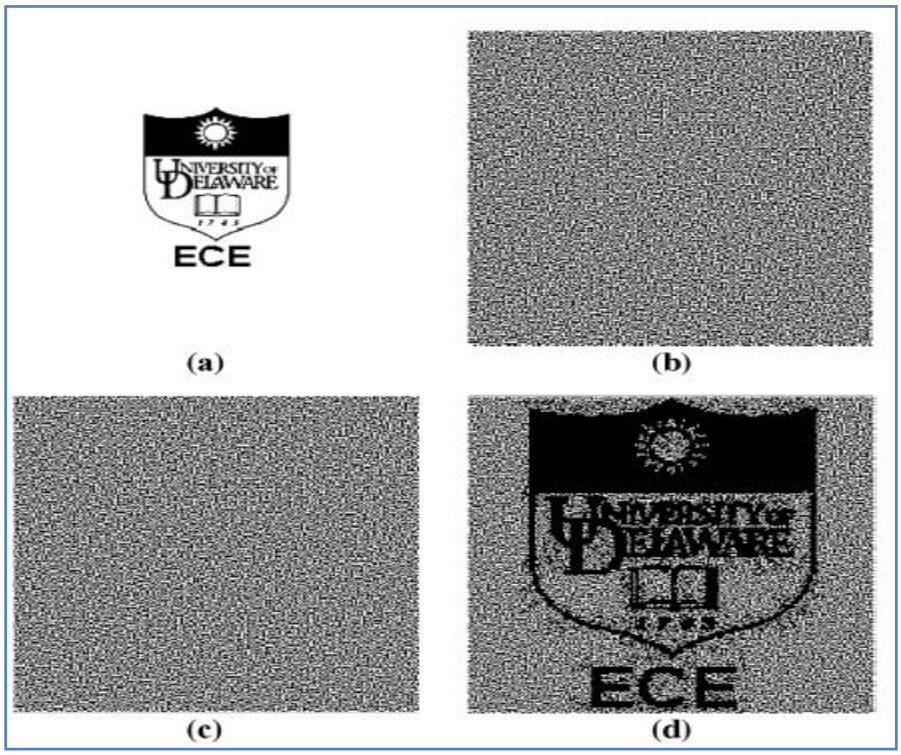

Figure 1 – Secret image is encoded into two shares and then encrypted

images to improve the image quality. Halftoning methods are used by Zhou et al. [16] for best quality shares. Fu [4] used VC and watermarking together to achieve best results.

In [17] Myodo proposed a VC scheme that makes use of meaningful shares. Error diffusion techniques are used in [18] along with halftoning shares to have meaningful images. First of all visual secret sharing for color images were explored in [19]. 2-out-of-2 VC scheme was proposed in [20] to apply the idea of color mixture. Lattice structure was used by Koga and Yamamoto [21] for combing colors arbitrarily. Random share patterns are the result of all such color visual cryptography schemes. The idea of generating meaningful color shares came into existence as the covers given good impression to human eyes [22], [23], and [14]. Recently Kang et al. [24] introduced VIP synchronization along with error diffusion technique to generate more meaningful color shares besides making them appealing.

In this paper we implement the scheme proposed in [24]. We built a prototype application that demonstrates the proof of concept. The empirical results are encouraging. The remainder of the paper is structured as follows. Section II provides Color Visual Cryptography Scheme and algorithms. Section III presents experimental results while section IV concludes the paper.

COLOR VC BASED ON PIXEL SYNCHRONIZATION AND ERROR DIFFUSION

VIP synchronization is used for color meaningful shares. For more visual quality error diffusion is used. The encryption process is based on the VIP synchronization. VIP synchronization helps in producing color meaningful shares that make sense. Moreover, they all give an illusion that they are original images and do not lead people to think about encryption. Construction of matrices with VIP synchronization for achieving proposed visual cryptography is presented in algorithm 1.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

1: **procedure** MATRICES CONSTRUCTION (S_0, S_1, λ)

2: **for** $i = 1, \cdots, n$ **do**

3: **for** $j = 1, \cdots, m$ **do**

4: (a): set $count = 0$

5: (b): if $S_0[i_j] = S_1[i_j] = 0$ is found, then $S_0[i_j] \leftarrow c_i$ and $S_1[i_j] \leftarrow c_i$ and $count = count + 1$.

6: goto (d) if $i < k$ or goto (e) if $i \geq k$.

7: (c): if $S_0[i_j] = S_1[i_j] = 0$ is not found, then switch element $S_0[i_{j1}]$ and $S_0[i_{j2}])$ $(j_1 \neq j_2)$ or

8: switch element $S_1[i_{j1}]$ and $S_1[i_{j2}])$ $(j_1 \neq j_2)$, and goto (b).

9: (d): if $count = \lambda$ and $i < k$, then goto (a) with i increased by 1.

10: (e): if $count = \lambda$ and $i \geq k$, then check if there exists an α satisfying:

$$W(S_1[i]) - W(S_0[i]) \geq \alpha \cdot m$$

if α exists, goto (a) with i increased by 1 until i reaches at n.

if α doest not exists, *undo* all changes of ith row and goto (c).

11: **end for**

12: **end for**

13: **end procedure**

Algorithm 1 – Construction of Matrices with VIP Synchronization

As can be seen in algorithm1, it is evidnet that the algorithm is meant for achieving VIP synchronization that improves the embedding process and thus produce meaningful covering shares. Afterwards, the distribution of matrices across color channels is done by algorithm 2.

As can be in algorithm 2, it is evident that the algorithm is meant for distribution of matrices across color channels with which encryption starts. In the process the VIP structure of the pixels is to be preserved. For this permutation process is carried out to reflect the preserving feature. Then error diffusion approach is used to make the shares more visually appealing to human eyes. More technical details can be found in [24].

1: **procedure** MATRICES DISTRIBUTION $(X, S_0^{c_1,\cdots,c_n}, S_1^{c_1,\cdots,c_n})$

2: **for** $p = 1, \cdots, K_1$ and $q = 1, \cdots, K_2$ **do**

3: find the starting pixel position on share X^i, $p' = p \cdot m_x - (m_x - 1)$, $q' = q \cdot m_y - (m_y - 1)$

4: conduct random column permutation, $P(S_0^{c_1,\cdots,c_n}, S_1^{c_1,\cdots,c_n})$

5: **for** the color channel C of the secret message, $x^C_{(p,q)}$ **do**

6: **if** the bit $x^C_{(p,q)} = 1$, **then**

place ith row of the $S_1^{c_1,\cdots,c_n}$ to $[x^C_{(p',q')}]^i$ of size $m_x \times m_y$

$[x^C_{(p',q')}]^i$ goes to the channel C of the ith share

7: **else if** the bit $x^C_{(p,q)} = 0$, **then**

place ith row of the $S_0^{c_1,\cdots,c_n}$ to $[x^C_{(p',q')}]^i$ of size $m_x \times m_y$

$[x^C_{(p',q')}]^i$ goes to the channel C of the ith share

8: **end if**

9: **end for**

10: Repeat 5 to 9 for the channel M and Y.

11: **end for**

12: **end procedure**

Algorithm 2 - Matrices Distribution

EXPERIMENTAL RESULTS

We built a prototype application to test the efficiency of the proposed approach. The experiments are made in terms of (2, 2) color EVC, (3, 4) color EVC. The standard images used for the experiments include Lena, Baboon, Pepper, Flower and so on. With respect to error diffusion, error filters are used.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Figure 2 – Halftone shares using color diffusion with the Floyd and Steinberg error filters

As can be seen in figure 2, it is evident that the error diffusion method along with proposed approach has generated meaningful color shares besides making them visually appealing. The error filters applied include Floyd and Steinberg.

Figure 3 – Experimental results with standard EVC and proposed method without error diffusion and proposed method with PSNR

As can be seen in Figure 3, it is evident that the (a) and (d)
are the shares produced with standard EVC, proposed

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

method without error diffusion and with PSNR. The results reveal that the shares are in color and meaningful. But they lack brightness and clear visual appealing.

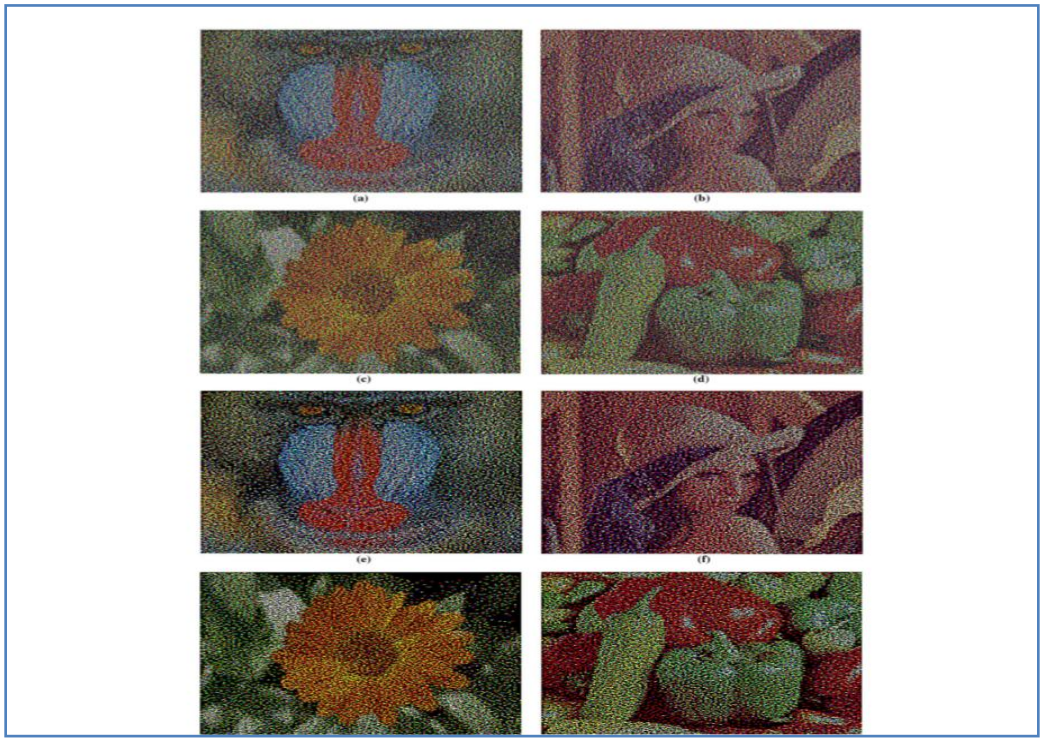

Figure 4 – Encrypted shares with standard EVC and proposed method without error diffusion and proposed method with PSNR

As can be seen in Figure 4, it is evident that the shares are the encrypted shares produced with standard EVC, proposed method without error diffusion and with PSNR. The results reveal that the shares are in color and meaningful. But they lack brightness and clear visual appealing.

As can be seen in Figure 5, it is evident they are the encrypted shares produced with standard EVC, proposed method without error diffusion and with PSNR. The results reveal that the shares are in color and meaningful. But they lack brightness and clear visual appealing.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

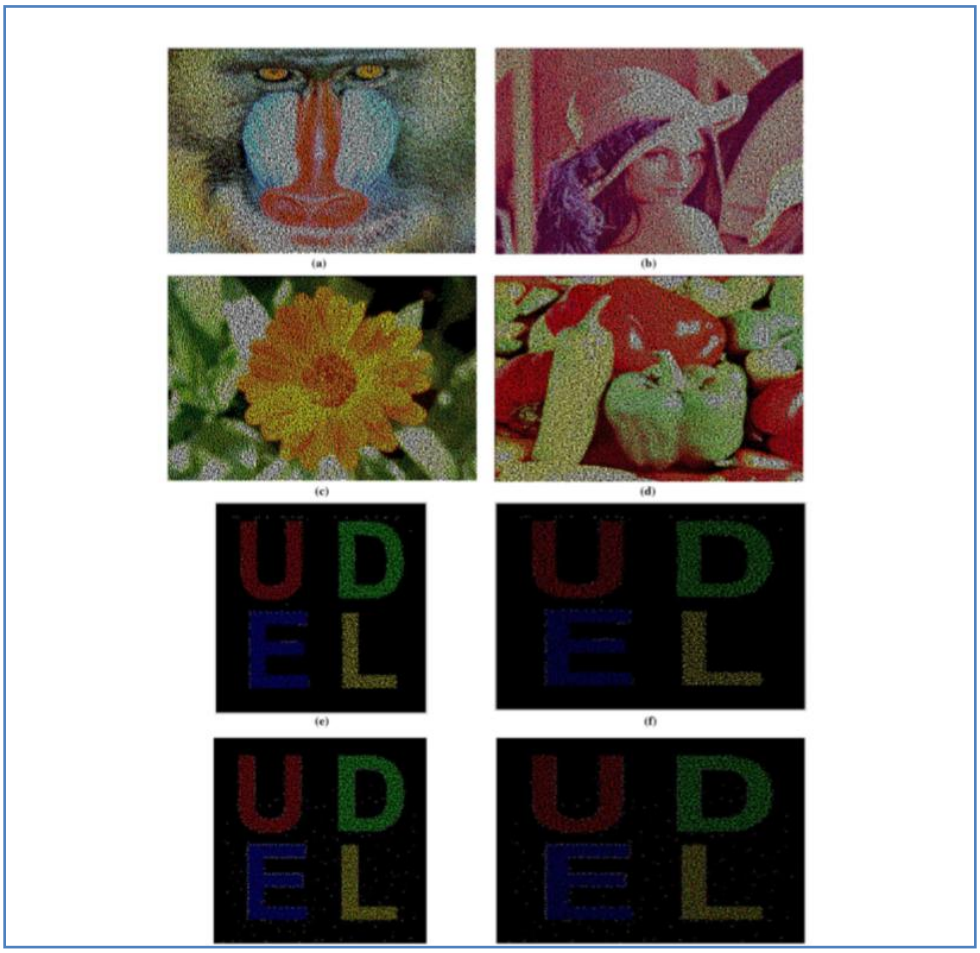

Figure 5 – Encrypted shares with standard EVC and proposed method without error diffusion and proposed method with PSNR

CONCLUSION

In this paper we studied the visual cryptography meant for secret sharing. We came to know that VIPs can synchronize the positions of the pixels that hold visual information. By using VIP synchronization it is possible to make meaningful color shares. This is because the VIPs can hold the original pixel values thus making the shares more meaningful and colorful. Moreover we used color diffusion method that ensures that the color meaningful shares are more appealing to human eyes making them intuitive. However, there is tradeoff between the contrast of encrypted and decrypted shares. We built a prototype application to demonstrate the proof of concept. The empirical results revealed that the proposed scheme is able to achieve more meaningful and appealing shares.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT , 1994, pp. 1–12.
[2] W. Q. Y, J. Duo, and M. Kankanhalli, "Visual cryptography for print and scan applications," in Proc. IEEE Int. Symp. Circuits Syst., 2004, pp. 572–575.
[3] M. Naor and B. Pinkas, "Visual authentication and identification," Adv. Cryptol., vol. 1294, pp. 322–336, 1997.
[4] M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking," in Proc. IEEE Int. Conf. Multimedia Expo, 2004, pp. 975–978.
[5] C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," Opt. Eng., vol. 44, p. 077003, 2005.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

[6] A. Houmansadr and S. Ghaemmaghami, "A novel video watermarking methodusingvisualcryptography,"inProc.IEEEInt.Conf.Eng.Intell. Syst., 2006, pp. 1–5.
[7] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, 1996.
[8] C. Blundo, P. D'Arco, A. D. S. , and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM J. Discrete Math., vol. 16, no. 2, pp. 224–261, 2003.
[9] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," Pattern Recognit. Lett., vol. 24, pp. 349–358, 2003.
[10] Y. T. Hsu and L. W. Chang, "A new construction algorithm of visual crytography for gray level images," in Proc. IEEE Int. Symp. Circuits Syst., 2006, pp. 1430–1433.
[11] C. Blundo, A. D. Santis, and M. Naor, "Visual cryptography for grey level images," Inf. Process. Lett., vol. 75, no. 6, pp. 255–259, 2000.
[12] L. A. MacPherson, "Gray level visual cryptography for general access structrue," M. Eng. thesis, Univ. Waterloo, Ontario, Canada, 2000.
[13] Y. C. Hou, "Visual cryptography for color images," Pattern Recognit., vol. 36, pp. 1619–1629, 2003.
[14] G. Ateniese, C. Blundo, A. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," ACM Theor. Comput. Sci., vol. 250, pp. 143–161, 2001.
[15] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," J. WSCG, vol. 10, no. 2, 2002.
[16] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 18, no. 8, pp. 2441–2453, Aug. 2006.
[17] E.Myodo,S.Sakazawa,andY.Takishima,"Visualcryptographybased on void-and-cluster halftoning technique," in Proc. IEEE Int. Conf. Image Process., 2006, pp. 97–100.
[18] 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.
[19] M. Naor and A. Shamir, "Visual cryptography II: Improving the contrast via the cover base," Lect. Notes Comput. Sci., vol. 1189, pp. 197–202, 1997.
[20] V.Rijimen andB.Preneel, "Efficient colorvisual encryptionforshared colors of benetton," presented at the Proc. Eurocrypto Rump Session, 1996[Online].Available:http://www.iacr.org/conferences/ec96/rump/index.html
[21] H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images," IEICE Trans. Fundamentals, vol. E81-A, no. 6, pp. 1262–1269, Jun. 1998.
[22] R. Lukac and K. N. Plataniotis, "Colour image secret sharing," Electron. Lett., vol. 40, no. 9, pp. 529–531, Apr. 2004.
[23] S. Droste, "New results on visual cryptography," in Proc. 16th Annu. Int. Cryptol. Conf. Adv. Cryptol., London, UK, 1996, pp. 401–415.
[24] InKoo Kang, Gonzalo R. Arce and Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion". IEEE Transactions On Image Processing, Vol. 20, no. 1, January 2011.