www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2. Issue 10 October 2013 Page No. 3066-3069

Color Extended Visual Cryptography Using Error Diffusion With VIP Synchronization

***Grishma R. Bhokare* [1] *, Prof. C. J. Shelke* [2]**

[1]M.E. 2 nd year
Department of Computer Science & Engg.,
P R PATIL COET, Amravati
Grishma.bhokare@gmail.com

[2]Prof. C. J. Shelke
Department of Computer Science & Engg.,
P R PATIL COET, Amravati
Chetanshelke7@gmail.com

Abstract :*Visual cryptography (VC) schemes encrypt a secret image into two or more cover images, general access structures for grayscale called shares. The secret image can be reconstructed by stacking the shares together, In extended visual cryptography, the share images are constructed to contain meaningful cover images, thereby providing opportunities for integrating visual cryptography and biometric security techniques. Visual cryptography is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed. Color visual cryptography (VC) encrypts a color secret message into n color halftone image shares. Previous methods in the literature show good results for black and white or gray scale VC schemes, however, they are not sufficient to be applied directly to color shares due to different color structures. This paper introduces the concept of visual information pixel (VIP) synchronization and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality.*

1. Introduction

In a *k* -out-of- *n* scheme of VC, a secret binary image is cryptographically encoded into *n shares* of random binary patterns. The shares are xeroxed onto *n* transparencies, respectively, and distributed amongst *n* participants, one for each participant.

Visual cryptography (VC) is a type of secret sharing scheme introduced by Naor and Shamir.

Several new methods for VC have been introduced recently in the literature. Blundo proposed an optimal contrast k-out-of-n scheme to alleviate the contrast loss problem in the reconstructed images. Ateniese proposed a more general method for VC scheme based upon general access structure. The access structure is a specification of qualified and forbidden subsets of shares. The participants in a qualified subset can recover the secret image while the participants in a forbidden subset cannot. The VC scheme concept has been extended to grayscale share images rather than binary image shares . Blundo proposed VC schemes with share images. Hou transformed a gray-level image into halftone images and then applied binary VC schemes to generate grayscale shares. Although the secret image is grayscale, shares are still constructed by random binary patterns carrying visual information which may lead to suspicion of secret encryption.

Atenies developed a method of extended visual cryptography (EVC) in which shares contain not only the secret information but are also meaningful images. Hypergraph colorings are used in constructing meaningful binary shares. Since hypergraph colorings are constructed by random distributed pixels, the resultant binary shares contain strong white noise leading to inadequate results. Wang

generalized the Ateniese's scheme using concatenation of b hieve more simpler deviation of basis matrices. Nakajima extended EVC to a scheme with natural grayscale images to improve the image quality. Zhou *et al.*used halftoning methods to produce good quality halftone shares in VC. Fu generated halftone shares that carry visual information by using VC and watermarking methods. Myodo proposed a method to generate meaningful halftone images using threshold arrays. Wang et. al. produced halftone shares showing meaningful images by using error diffusion techniques. This scheme generates more pleasing halftone shares owing to errors diffused to neighbor pixels.

2. Fundamentals of VC

Generally, a (k,n)-VC scheme encrypts a secret message into n shares to be distributed to n participants. Each share shows noise-like random black and white patterns and does not reveal any information of the secret image by itself. In a k-out-of-n scheme, access to more than k shares allows one to recover the secret image by stacking them together, but access to less than k shares is not sufficient for decryption. A black and white (k,n)-VC scheme consists of two collections of n×m binary matrices S0 and S1, having elements denoted by 1 for a black pixel and 0 for a white pixel. To encrypt a white (black) pixel, a dealer randomly chooses one of the matrices in S0(S1) and distributes its rows to the n participants. More precisely, a formal definition of the black and white (k,n) -VC scheme is given next.

2.1 Visual cryptography for general access structures

In (k, n) Basic model any 'k' shares will decode the secret image which reduces security level. To overcome this issue the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, where an access structure is a specification of all qualified and forbidden subsets of 'n' shares. Any subset of 'k' or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. Construction of k out of n threshold visual cryptography scheme for general access structure is better with respect to pixel expansion than .

2.2 Visual cryptography for gray level images

Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. Chang- ChouLin, Wen-HsiangTsai proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality.

2.3 Recursive Threshold visual cryptography

The (k, n) visual cryptography explained in section I needs 'k' shares to reconstruct the secret image.This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography proposed by Abhishek Parakh and Subhash Kak eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application,
network load is reduced.

2.4 Extended visual cryptography for natural images

All of the VC methods suffer from a severe limitation, which hinders the objectives of VC. The limitation lies in the fact that all shares are inherently random patterns carrying n visual information, raising the suspicion of data encryption. Mizuho NAKAJIMA and Yasushi YAMAGUCHI proposed extended visual cryptography for natural images constructs meaningful binary images as shares. This will reduce the cryptanalysts to suspect secrets from an individual shares. While the previous researches basically handle only binary images, establishes the extended visual cryptography scheme suitable for natural images.

2.5 Halftone Visual Cryptography

The meaningful shares generated in extended visual cryptography proposed by Mizuho NAKAJIMA and Yasushi YAMAGUCHI was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel 'P' is encoded into an array of QI x Q2 ('m' in basic model) sub pixels, referred to as halftone cell, in each of the 'n' shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security.

3. Error Diffusion

Error diffusion is a simple yet efficient way to halftone a grayscale image. The quantization error at each pixel is filtered and fed into a set of future inputs. Fig. shows a binary error diffusion diagram where f(m,n) represents the pixel at (m,n) position of the input image.d(m,n) is the sum of the input pixel value and the diffused errors g(m,n), is the output quantized pixel value. Error diffusion consists of two main components. The first component is the thresholding block where the output g(m,n) is given by

$$g(m,n) = \begin{cases} 1\ , if\ d(m,n) \geq t(m,n) \\ 0\ ,\ otherwise \end{cases}$$

The threshold t(m,n) can be position dependant. The second component is the error filter h(k,l) where the input is the difference between d(m,n) and g(m,n) . Finally, we compute as

$$d(m,n) = f(m,n) - \sum_{k,l} h(k,l)e(m-k,n-l)$$

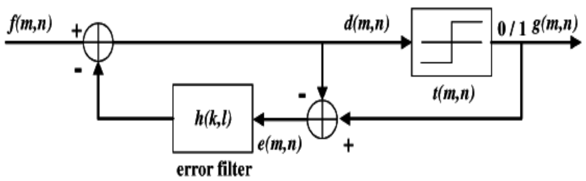

Figure 1: Error diffusion block diagram. The pixel f(m,n) is passed through a quantizer to obtain the corresponding pixel g(m,n) . The difference between these two e(m,n), is diffused away to the neighboring pixels by the filter h(k,l). The threshold value t(m,n) determines g(m,n).

4. Color vc encryption based upon pixel synchronization and error diffusion

In this section, we describe the encryption method for color meaningful shares with a VIP synchronization and error diffusion. First, we describe the VC matrix derivation method for VIP synchronization from a set of standard VC matrices. We then introduce an error diffusion process to produce the final shares. The halftone process is independently applied to each cyan (C), magenta (M), and yellow (Y) color channel so each has only one bit per pixel to reveal colors of original images. A secret message is halftoned ahead of the encryption stage.

5. Advantages of Our Scheme

The scheme proposed generates high quality of meaningful color shares as well as the colorful decrypted share using VIP synchronization and error diffusion methods. The VIPs are pixels that carry pixel values of original images to make shares meaningful. When these VIPs are not assigned during the halftone stage, the resultant shares are the same as that of standard VC schemes except the colorful decrypted messages. Other schemes deal with EVC schemes in color, however, they do not consider relationship throughout color channels. Some schemes produce colorful noise-like random patterns. Our scheme deals with all these considerations. Furthermore, most color EVC schemes and need extra pixel expansion in addition to , the pixel expansion of standard VC schemes, however, we need only . This feature reduces needless space for one pixel encryption and finally produces shares with as less as possible pixel expansion.

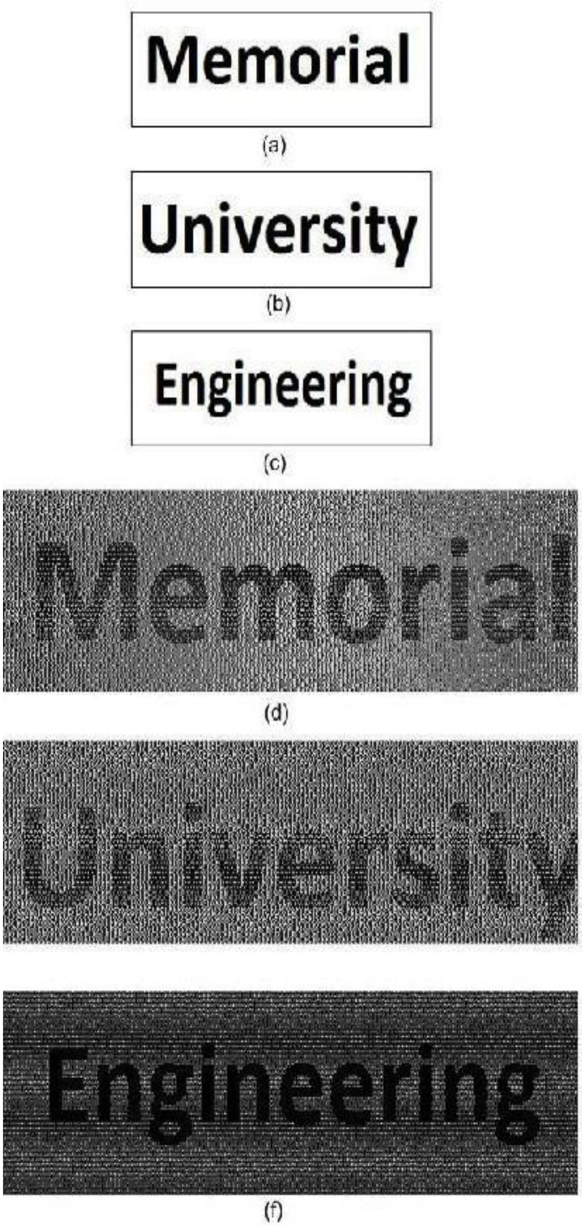

Figure 2: Example of (2; 2) EVC Scheme: (a) first cover image; (b) second cover image; (c) secret image; (d) share 1; (e) share 2; (f) recovered secret image

6. Coclusion

In this paper, we have explored extended visual cryptography without expansion.
we have proposed a new VC scheme for color images using meaningful shares. VIPs synchronize the positions of pixels that carry visual information of original images across the color channels so as to retain the original pixel values the same before and after encryption.
Error diffusion is used to construct the shares such that the noise introduced by the preset pixels are diffused away to neighbors when encrypted shares are generated.

References

[1] M. Naor and A. Shamir, “Visual cryptography,” in *Proc. EUROCRYPT*, 1994.

[2] 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.

[3] A. Houmansadr and S. Ghaemmaghami, “A novel video watermarking method using visual cryptography,” in *Proc. IEEE Int. Conf. Eng. Intell. Syst.*, 2006, pp. 1–5.

[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.

[6] M. Naor and B. Pinkas, “Visual authentication and identification,” *Adv. Cryptol.*, vol. 1294, pp. 322–336, 1997.

[7] 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.

[8] 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.

[9] Nitty Sarah Alex and L. Jani Anbarasi, “Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography,” ICECT’11, Vol. 6, pp. 393-397, April 2011.

[10] P.S. Revenkar, A. Anjum and W.Z. Gandhare, “Secure Iris Authentication Using Visual Cryptography,” IJCSIS, Vol. 7, No.3, pp. 217-221, 2010.

[11] C. Sasivarnan, A. Jagan, Jaspreet Kaur, Divya Jyoti, and Dr. D.S. Rao, Image Quality Assessment In Spatial Domain," IJCST, Vol. 2, Issue 3, September 2011.

[12] 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.

[13] D. S.Wang, F. Yi, and X. Li, "On general construction for extended visual cryptography schemes," *Pattern Recognit.*, pp. 3071–3082, 2009.

[14] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *J. WSCG*, vol. 10, no. 2, 2002.

[15] 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.