An Improved Method for Secret Image Sharing in Color Image through Error Diffusion

Ashwini N. Waghmare[1], Prof. Akhil Anjikar[2], Dr. M. Raghuwanshi[3]

Abstract: ***Visual Cryptography is the technique that divides the secret image into n number of shares. Each share consists of some information and when k shares out of n stack together the secret will reveal. However; less than k shares are not work. Color visual cryptography (VC) is a scheme of providing security to a color secret image by encrypting it into n color halftone image shares. A visual cryptogram scheme consists of an encryption algorithm by which a secret image is divided into a set of shares and a decryption algorithm which is used to recover the secret image by staking the shares. In this paper we introduced 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. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the 3 color channels and error diffusion diffuses the errors generates shares pleasant to human eyes.***

Keywords: Visual Cryptography Scheme, halftone, visual information pixel, error diffusion, secret sharing, meaningful color shares, digital halftoning

1. Introduction

VISUAL CRYPTOGRAPHY (VC) is a type of secret sharing scheme introduce by Naor and Shamir[1]. Visual cryptography is based on cryptography in which n images are divided into n number of shares where each share consists of some information about the original image. When k share out of n stack together secret will reveal less than k share does not reveal secret.

Consider a binary secret message image E and a set of n participant sharing E. A k out of n visual secret sharing scheme encrypt E into n transparencies (called shares) which are distributed to the n participant one by one in a such a way that only when k or more share are stacked together can the participant see E by their visual system .while less than k share does not reveal the secret information about E.

There are several method of visual cryptography such as optimal contrast k out of n scheme, general access structure scheme, halftone image scheme, extended visual cryptography scheme, extended EVC scheme [2]-[3][4][5]

This paper introduces a color VC encryption method which leads to meaningful shares and is free of the previously mentioned limitations. The method is simple and efficient. It relies on two fundamental principles used in the generation of shares, namely, error diffusion and VIP synchronization. Error diffusion is a simple but efficient algorithm for image halftone generation

1.1 VIP Synchronization

It is also called visual information pixel synchronization. VIP synchronization is used to carry the information about the original value of pixel. Synchronization of the VIPs across the color channels improves the visual contrast of shares. In color VC schemes, the colors of encrypted pixels and the contrast can be degraded due to random matrix permutation [6]. Random matrix permutations are key security features in VC schemes. In grayscale VC schemes, it does not affect the visual quality; however, in color schemes, independent execution of random matrix permutation for each color channel can cause color distortion by placing VIPs at random positions in sub pixels which finally degrades the visual quality. VIP synchronization prevents the color and contrast of original images from degradation even with matrix permutation.

Random matrix permutations are key security features in VC schemes. In grayscale VC schemes, it does not affect the visual quality; however, in color schemes, independent execution of random matrix permutation for each color channel can cause color distortion by placing VIPs at random positions in sub pixels which finally degrades the visual quality. VIP synchronization prevents the color and contrast of original images from degradation even with matrix permutation.

1.2 Error Diffusion

Error Diffusion is simple and effective technique used to improve the quality of generated shares[7]. The quantization error at each pixel is filtered and fed back to future input. The error filter is designed in a way that the low frequency differences between the input and output images are minimized and consequently it produces pleasing halftone images to human vision.

2. Related Work

Some previous work related to visual cryptography is described in this section. Several new methods for VC have been introduced recently in the literature. Blundo [3] proposed an optimal contrast k-out-of-n scheme to alleviate the contrast loss problem in the reconstructed images. Ateniese [4] 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 [5]–[6]. Blundo [7] proposed VC schemes with general access structures for grayscale share images. Hou [8] 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 [9] 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 [10] generalized the Ateniese's scheme using concatenation of basis matrices and the extended matrices collection to achieve more simpler deviation of basis matrices. Nakajima [11] extended EVC to a scheme with natural grayscale images to improve the image quality. Zhou *et al.* [12] used halftoning methods to produce good quality halftone shares in vc.

3. Proposed Work

3.1 Architecture of Proposed System

Visual cryptography scheme for secret image sharing using

Error diffusion required following steps.

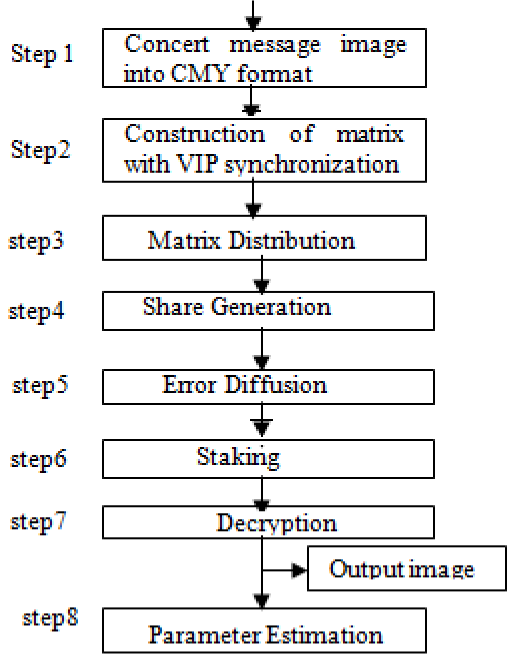


Figure 1: Step required for proposed systems

3.1.1 RGB to CMY conversion

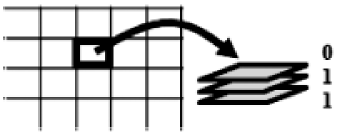
First convert the message image into CMY (cyne ,magenta. yellow) format.

3.1.2 Construction of matrix with VIP synchronization

The encryption method focuses on VIP synchronization across 3 color channels. VIPs are pixels on the encrypted shares that have color values of the original images, which make the encrypted shares meaningful. In each of the m sub pixels of the encrypted share, there are ƛ number of VIPs, denoted as Ci and the remaining (m-ƛ) pixels deliver the message information of the secret message image. Here each sub pixel m carries visual information as well as message information, while other methods extra pixels are needed in addition to the pixel expansion to produce meaningful shares. Since each VIP is placed at the same bit position in sub pixels across the three color channels, VIP represents accurate colors of the original image.

3.1.3 Stribution of matrices across color channel

This algorithm produces encryption shares Xi An example of the matrices distribution for (2, 2)-color EVC scheme shows the matrices distribution along with each message pixel. Each binary bit on three color channels of message pixel is expanded into four sub pixels on corresponding color channels throughout the encryption shares by taking the matrix S0 and S1 according to its bit value. Since the VIPs are placed at the same spot on the row in matrices S0 and S1 each encrypted sub pixels has the VIPs at the same positions throughout the color channels, where colored in gray in the figure. This feature makes the shares carry accurate colors of the original image after encryption. the decryption mechanism by the unit of sub pixels showing how they present the desired color of the original message pixel. Regardless of the VIP values which will be decided in the error diffusion stage, the decrypted sub pixels reveal the color of the message pixel X(p,q) with contrast loss. Since the matrices S1 and S0 with contrast loss. Since the matrices are derived in a way way that the contrast difference is α , the decrypted sub pixels show the intended color of the message pixel with probability α .



Message bit

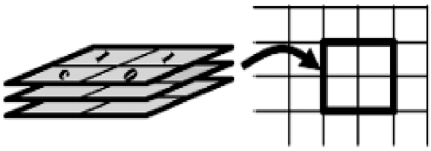
$$S_1^{c_1c_2} = \begin{bmatrix} 1 & 1 & c_1 & 0 \\ 0 & c_2 & 1 & 1 \end{bmatrix} \quad S_0^{c_1c_2} = \begin{bmatrix} 1 & 1 & c_1 & 0 \\ 1 & c_2 & 1 & 0 \end{bmatrix}$$

Random column permutation P(S0,S1)

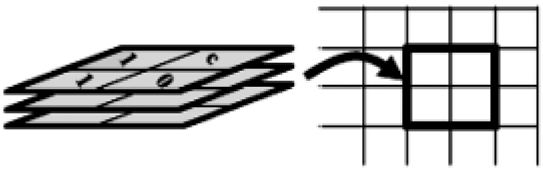
x^C	1	1	C_1	0
x^M	1	1	C_1	0
x^Y	1	1	C_1	0

x^C	1	C_2	1	0
x^M	0	C_2	1	1
x^Y	0	C_2	1	1

**Subpixels X1(p', q')of Subpixels X2(p', q')of
Share 1 share2**



Encrypted subpixel of share 1



Encryped subpixel of share 2

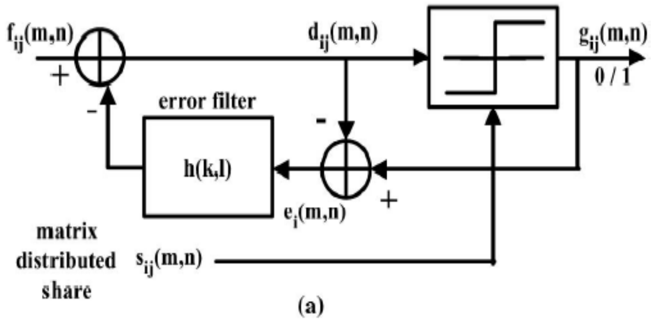
Fig 2 General illustration of matrices distribution of (2, 2)-color EVC. (a) Matrices distribution along with a message pixel. Every message pixel composed of 3 b is encoded into four subpixels for each color channel by referring the bit value on each channel of message bit. The positions of VIPs across color channels where colored in gray are preserved after encryption.

3.1.4 Generation of shares via Error Diffusion

Once the matrices S0,S1 processed across the channels completed ,a half toning algorithm is applied to generate the final encrypted shares. Error diffusion is used in our scheme as it is simple and effective. The quantization error at each pixel is filtered and fed back to future inputs. Fig. 4 shows a binary error diffusion diagram designed for our scheme. To produce the ith halftone share, each of the three color layers are fed into the input. The process of generating halftone shares via error diffusion is similar to that shown in Fig.1 except that Fi.j(m, n) is a (m, n) i th pixel on the input channel j(1≤ i ≤ n, 1≤ j ≤ 3) of ith share.

The other difference between our scheme from standard error diffusion is that the message information components, non , are predefined on the input shares such that they are not modified during the halftone process, i.e., the process is applied when the input is ci Fig. 4 depicts this process. 1s and 0s in black are message information pixels that should not be modified and those are in red are VIPs that are already defined by the error diffusion. The ci are also VIPs whose values are to be decided by referring the corresponding pixel values of original images and errors from neighboring pixels when the error filter window comes. Non Ci elements, however, still affect di,j(m, n) and the quantization error ei,j(m, n) when they are calculated in the filter window.

The non elements may increase quantization errors added to the shares, but in turn, these errors are diffused away to neighboring pixels. The visual quality of shares via error diffusion can be improved through edge enhancement methods. The measure of a particular half toning algorithm is its performance in DC regions and its performance near edges or in areas of high frequency image content can be manipulated through pre filtering the image prior to half toning.



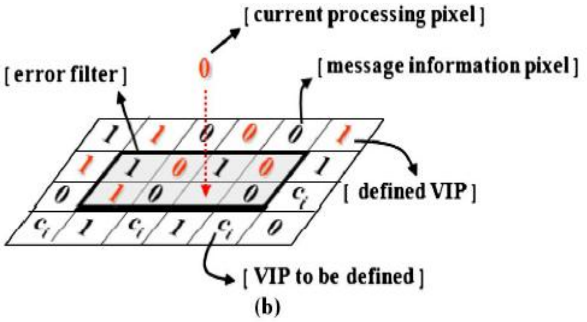


Figure 4: (a) Block diagram of error diffusion with share encryption (b)Visualization of error diffusion with VIP

3.1.5 Decryption of shares

Decryption of share perform by simply stacking share1 and share 2 it reveal the secret of original image.

x^C	1	1	C_1	0
x^M	1	1	C_1	0
x^Y	1	1	C_1	0

⊗

x^C	1	C_2	1	0
x^M	0	C_2	1	1
x^Y	0	C_2	1	1

Subpixels X1(p’, q’)of Subpixels X2(p’, q’)of Share 1 share2

↓

x^C	1	1	1	0
x^M	1	1	1	1
x^Y	1	1	1	1

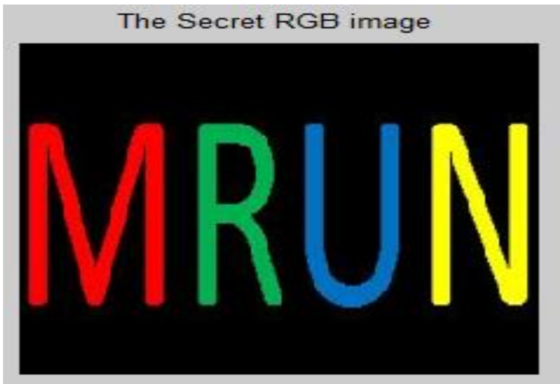
Decrypted subpixel

Fig3:- Decryption example of subpixels. Regardless of VIP values, the decrypted subpixels represent the intended color, the same as that of the original message pixel, where colored in gray. The ⊗ represents the logical “OR” operation.

4. Simulation Results

This section presents the information regarding input secret image for encryption, meaningful shares or half toned shares used for encryption process and reconstructed image.

A. Original Secret Image for 2 out of 2 and 4 out of 4 VCS



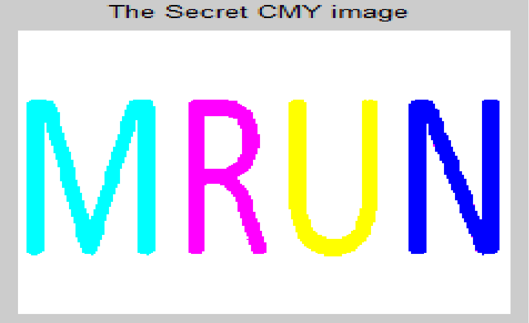


Figure A: Original Secret Image

B. Colour Images

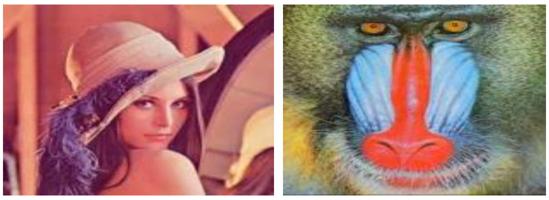
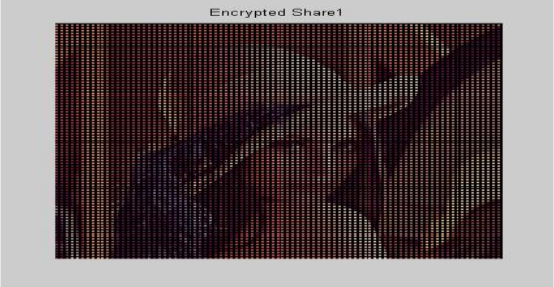
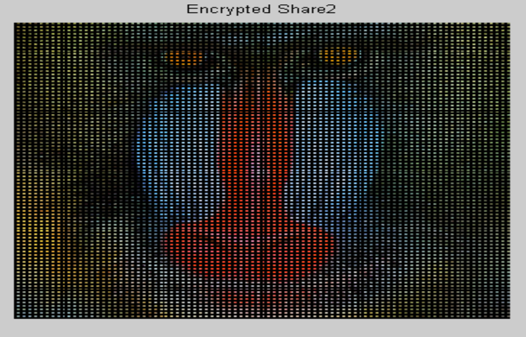


Figure B: Actual Colour Image

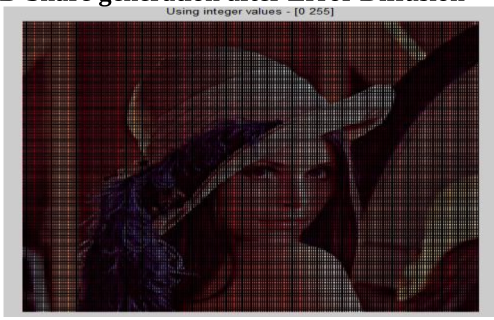
C. After Embedding Secret image into Shares

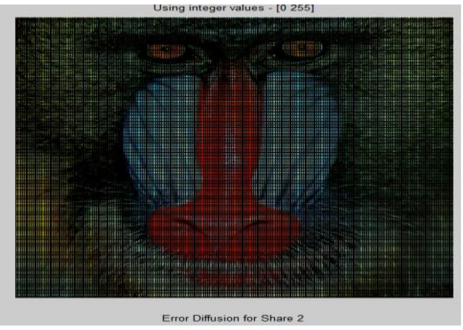
I. Meaningful Shares for 2 out of 2 VCS after Encryption



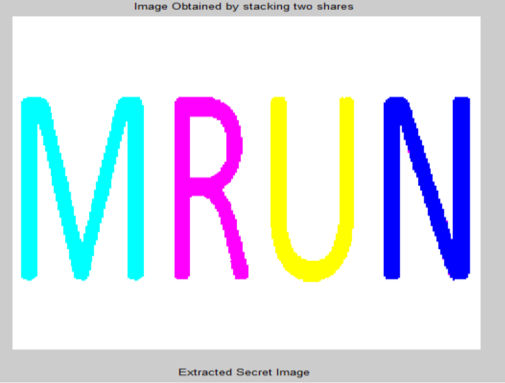


D Share generation after Error Diffusion





E. Decryption if share



5. Conclusion

From the above result it is clear that visual information pixel synchronization and error diffusion technique improves the quality of shares. There is trade of contrast between the encryption and decryption of shares. 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, pp. 1–12.

[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] 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] L. A. MacPherson, "Gray level visual cryptography for general access structrue," M. Eng. thesis, Univ. Waterloo, Ontario, Canada, 2000.

[10] 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.

[11] Inkoo Kang, Gonnzoalo R..Arce, Heun-Kyu Lee "Color Extened Visual Cryptography Using Error Diffusion" IEEE Trans, Image Process., vol. 20 No.1, pp.132-145,2011.

[12] D.s Wang, F.Yi, and X.Li,"On general construction for extended visual cryptography schemes"Pattern Recognit., pp.3071-3082,2009.

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

[14] 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.

[15] C. N Yang, " A note on efficient color visual encryption," J. Inf. Sci.Eng., vol. 18, pp.367-372,2002.

[16] E. R.Verheul and H.C.A vanTilborg, "Construction and properties of k out of n visual secret sharing schemes, " Des. Codes Cryptogr., vol. 11, no. 2, pp. 179-196, May 1997.

[17] 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. 06, pp. 1262-1269, Jun. 1998.

[18] C. N Yang and T.S . Chen, "Visual Cryptography Scheme based on additive color mixing," Pattern Recognit., vol. 41, pp. 3114-3129,2008.