A Rumination of Error Diffusions in Color Extended Visual Cryptography

P.Pardhasaradhi[#1], P.Seetharamaiah[*2]

[#]*Department of CSE, Bapatla Engineering College, Bapatla, AP, India*
**Department of CS&SE, Engineering of College, AU Visakhapatnam, AP, India*

***Abstract*— Color visual cryptography (VC) is a secret sharing scheme which uses to encrypt a secret message into n halftone image shares. The users can recover the secret image by stacking their shares, and then secret image can be revealed. In extended visual cryptography, the share images are constructed to contain meaningful cover images. Halftoning and visual information pixel (VIP) is the important feature, which provides immunity at the early stage of cryptography. In this paper we make a rumination of various error diffusions and visual information pixel (VIP) synchronization techniques to generate meaningful color shares with high visual quality and compare the respective algorithms for parameters such as PSNR and perceived error.**

***Keywords*— Color meaningful shares, halftoning, error diffusion, visual cryptography (VC)..**

I. INTRODUCTION

Visual cryptography (VC), first proposed in 1994 by Naor and Shamir [1], is a secret sharing scheme, based on black and white or binary images. Secret images are divided into share images which, on their own, reveal no information of the original secret. Shares may be distributed to various parties so that only by collaborating with an appropriate number of other parties, can the resulting combined shares reveal the secret image. Recovery of the secret can be done by superimposing the share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is of particular interest for security applications based on biometrics [2]. For example, biometric information in the form of facial, fingerprint and signature images can be kept secret by partitioning into shares, which can be distributed for safety to a number of parties. The secret image can then recovered when all parties release their share images which are then recombined.

A basic 2-out-of-2 or (2-2) visual cryptography scheme produces 2 share images from an original image and must stack both shares to reproduce the original image. More generally, a (k- n) scheme produces n shares, but only requires combining k shares to recover the secret image. To preserve the aspect ratio for the recovered secret image for a (2-2) scheme each pixel in the original image can be replaced in the share images by a 2-2 block of subpixels. As shown in Table I.

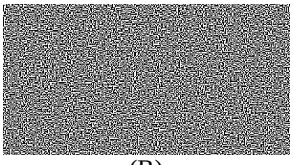
TABLE I.
ILLUSTRATION OF A (2-2) VC SCHEME WITH 4 SUBPIXELS

Pixel	Probability	Share 1	Share 2	After Stacking
White	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
Black	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
	1/6			

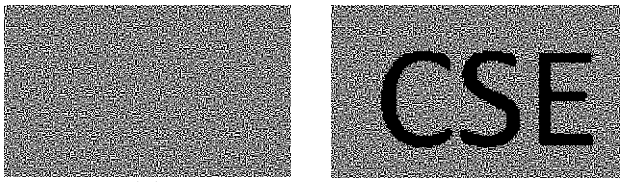
If the original pixel is white, one of six combinations of share pixels is randomly created. Similarly, the possible share combination for black pixels is also shown. After stacking the shares with white transparent and black opaque, the original secret image will be revealed. Stacking can be viewed as mathematically ORing, where white is equivalent to “0” and black is equivalent to “1”. The process is illustrated in Figure 1 for a simple binary image.

Note that the resulting share images and the recovered secret image contain 4 times more pixels than the original image (since each pixel of the original image was mapped to four subpixels) [3]. It may also be noted that the recovered image has a degradation in visual quality (specifically, the contrast between white and black is decreased) since a recovered white pixel is actually comprised of 2 white and 2 black subpixels, while a black pixel is represented by 4 black subpixels in the recovered image.

(A)



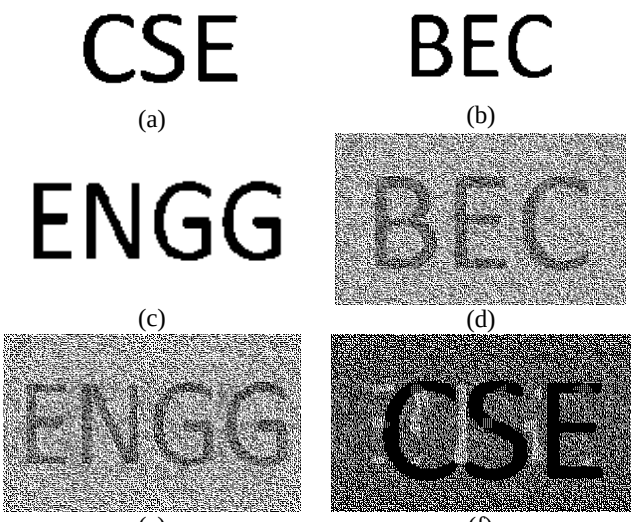
(B)



(C) (D)

FIG. 1. EXAMPLE OF A (2; 2) VC SCHEME WITH 4 SUBPIXELS: (A)SECRET IMAGE; (C) FIRST SHARE; (D) SECOND SHARE (B) RECONSTRUCTED IMAGE;

In 1996, Ateniese, Blundo, and Stinson [4] [10] proposed extended visual cryptography (EVC) schemes that can construct meaningful share images. The (2-2) EVC scheme proposed in [4] required expansion of one pixel in the original image to 4 subpixels which can then be selected to produce the required images for each share. It can be shown that the resulting scheme is, in fact, also perfectly secure, and in that, no share image leaks any information of the original secret image. Figure 2 illustrates a (2; 2) scheme containing the original binary secret image, "CSE", with two cover images, "BEC" and "ENGG", embedded into the shares. Although visual cryptography operates on binary images, it can be applied to gray-scale images by using a halftoning algorithm to first convert the gray-scale image to a binary image [5]. This allows for use of visual cryptography schemes to biometric images which are naturally and meaningfully gray-scale, such as facial images. Hence, using halftoning techniques to convert gray-scale images to binary images is a useful pre-processing step for visual cryptography.



(a) (b)

(c) (d)

(e) (f)

FIG. 2. EXAMPLE OF (2; 2) EVC SCHEME: (A) SECRET IMAGE; (B) FIRST COVER IMAGE; (C) SECOND COVER IMAGE; (D) SHARE1; (E) SHARE2; (F) RECOVERED SECRET IMAGE

Recently, Chang et al. [6] [7] proposed a color image sharing technique. The algorithm first creates a palette of a secret image and assigns a unique code to each color on the palette. It then selects two colored cover images, S1 and S2; with size the same as the secret image.

This paper introduces a color VC encryption method to generate meaningful shares. It based on two fundamental concepts used in the generation of shares they are error diffusion [7] and pixel synchronization [9] . Error diffusion is a procedure that produces pleasing halftone images to human vision. Synchronization of the pixels of secret image and covering images across the color channels improves visual quality of shares. Visual Information Pixel (VIP) synchronization prevents colors and contrast of original shares from degradation even with matrix permutation.

This paper is organized as follows. Section II describes the various error diffusion methods and VIP Synchronization. Section III shows experimental results of the comparisons of various Error diffusion methods. Finally, we conclude this paper in Section IV.

II. PRE-PROCESSING HALFTONE IMAGES & VIP SYNCHRONIZATION

In this section, we consider the application of visual cryptography to color images by first converting the images to a halftone image using a halftoning algorithm. After creating a halftone image, in order to preserve the image size when applying extended visual cryptography using error diffusion and Visual Information Pixel (VIP) synchronization

A. Error diffusion Halftoning

Error diffusion [7],[8],[9] produces halftone images of much higher quality than other halftone. It quantifies each pixel using a neighbourhood operation. A schematic diagram of error diffusion method is given in figure 3. The error diffusion scans the image one row at a time and one pixel at a time. The current pixel is compared to a threshold (127) value. If it is above the value a white pixel is generated in the resulting image. If the pixel is below the half way value, a black pixel is generated. The generated pixel is either full bright or full black.

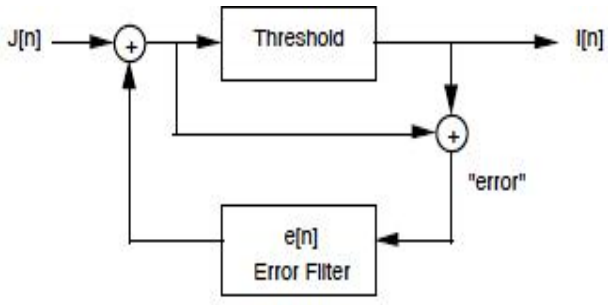


FIG.3: ERROR DIFFUSION BLOCK DIAGRAM

Error is calculated which is the difference between original image and halftone image. The error is then added to the next pixel in the image and the process repeats. To which neighbour and how this error is pushed is decided by an error diffusion matrix as show figure 4 and figure 5.

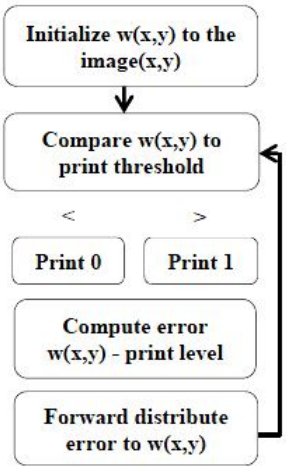


FIG.4: PROCESS OF HALFTONING

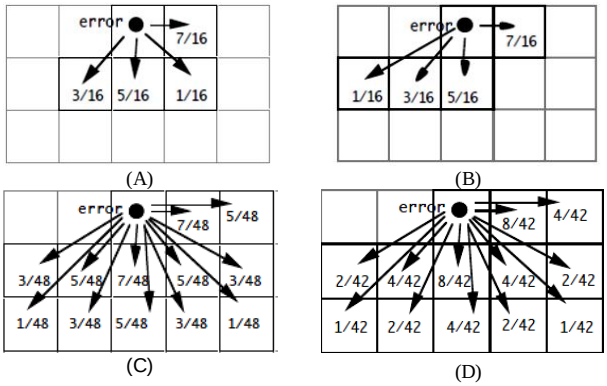


FIG.5: ERROR DIFFUSION WEIGHT MATRIXES (A) FLOYD AND STEINBERG (B) MODIFIED FLOYD (C) JARVIS, JUDICE, AND NINKE (D) STUCKI

Algorithm: Floyd and Steinberg error diffusion halftoning

```
for i = 1 to n
        for j = 1 to m
                I[i,j] = (J[i,j] < 128)? 0 : 1
                err = J[i,j] - I[i,j]*255
                J[i+1,j] += err*(7/16)
                J[i-1,j+1] += err*(3/16)
                J[i,j+1] += err*(5/16)
                J[i+1,j+1] += err*(1/16)
        end for
end for
```

Modified Floyd, Jarvis Judice & Ninke and Stucki error diffusion method follow the same algorithm except that while distributing error it uses matrices as shown in figure 5

In the CMYK colored halftone process[8] four separations (also called screens) are made, one for each process color. Different sizes of the dots of ink are used to produce the different levels of color. These dots are not large enough to be seen without magnification. After different adjustments are made to the separations, the article being printed goes through a process where each color gets printed in succession, one on top of the other. To prevent moire patterns, each screen is set to a different angle as shown in figure 6.

FIG.6: COLOR IMAGE HALFTONING
(A)ORIGINAL IMAGE (B) CYAN HALFTONE
(C) MAGENTA HALFTONE (D) YELLOW HALFTONE
(E) COLOR HALFTONE IMAGE.

B. VIP Synchronization

Visual Information Pixel (VIP) is pixel on the encrypted shares that have color values of the original images, which make shares meaningful. In the proposed method each subpixel n carries visual information as well as message information ,while other methods in [1] and [5] extra pixels are needed in addition to the pixel expansion n to produce meaningful shares.

Algorithm: VIP Synchronization

Given S_1,S_2 are covering images of size m x n, S_c secret image of size k_1 x k_2

Procedure VIP_Synchronization(S_1,S_2,S_c)

for p=1 to k_1 do for q=1 to k_2 do

for the color channel cyan of the secret image $S_c^C(p,q)$ do

if $S_c^C(p,q)=1$ then

for i=1 to k_1 do for j=1 to k_2 do

if $S_1(i,j)=S_2(i,j)$ then

Randomly select any one S_i and complement S_j

end_if

end_for end_for

else if $S_c^C(p,q)=0$ then
for i=1 to k_1 do for j=1 to k_2 do
if $S_1(i,j) \neq S_2(i,j)$ then
Randomly select any one Si and make them equal
end_if
end_for end_for
end_if

Repeat the above process for the channel magenta and yellow

end_for end_for
end_procedure.

This algorithm takes the input as halftone images which are created by error diffusion method. It decomposes the color images into 3 subtractive colors (Cyan, Magenta and Yellow) and then it executes VIP Synchronization algorithm on each color bit. The output of this block is meaningful shares. Now each bit on share contains information regarding covering image as well as secret image without giving any clue about encryption.

C. Stacking

Decoding does not need any algorithm. The meaningful shares are XORed to reconstruct the secret image by simply human vision system.

III. SIMULATION RESULTS

In this section, we provide some experimental results to illustrate the effectiveness of the above method using various error diffusion methods. Example is composed with a (3-4)-color EVC scheme. The secret message of size 128 x 128 pixels shows letters "U," "D," "E" and "L" in red, blue, green, and yellow, respectively. Original images "Lena," "Baboon," "Pepper," and "Flower "of size 256 x 256 in natural colors are provided for the share generation. We use two different metrics for visual quality comparison between the original images and the encrypted shares. First, we use the peak noise-to-signal ratio (PSNR) distortion measure and assume that the value of original images belong to a Gaussian distribution with N (0, 1). Second, we measure the visual quality of the encrypted shares using the perceived error method between the original images and the encrypted shares. All the images are halftone before encryption process. Halftone images create a space so that we can embed secret message into covering image.

(A)

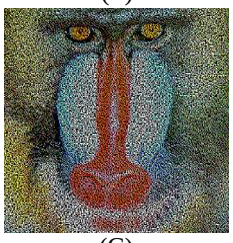

(B)

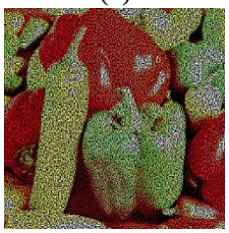

(C)

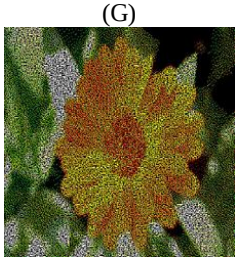

(D)


(E)


(F)


(G)


(H)


(I)

(J)

FIG.7: (A) SECRET MESSAGE (B)-(E) COVER IMAGES (F) SHARE1 (G) SHARE2 (H) SHARE3 (I) SHARE4 AND (J) DECODED MESSAGE FROM SHARES

TABLE II: PSNR AND PERCEIVED ERROR USING FLOYD AND STEINBERG

Image	PSNR(dB)	Perceived error
Secret Image	23.3159	5.4418e+005
Lena	12.0620	8.3079 e+006
Baboon	12.5327	8.2712 e+006
Pepper	13.7752	7.2422 e+006
Flower	15.6987	5.4762 e+006

TABLE III: PSNR AND PERCEIVED ERROR USING MODIFIED FLOYD

Image	PSNR(dB)	Perceived error
Secret Image	23.3160	5.44182e+005
Lena	12.0618	8.3081 e+006

Baboon	12.5325	8.2713 e+006
Pepper	13.7749	7.2424 e+006
Flower	15.6987	5.4763 e+006

TABLE VI: PSNR AND PERCEIVED ERROR USING JARVIS, JUDICE, AND NINKE

Image	PSNR(dB)	Perceived error
Secret Image	23.3173	5.4417 e+005
Lena	12.0625	8.3079 e+006
Baboon	12.5341	8.2712 e+006
Pepper	13.7757	7.2422 e+006
Flower	15.6992	5.4762 e+006

TABLE V: PSNR AND PERCEIVED ERROR USING STUCKI

Image	PSNR(dB)	Perceived error
Secret Image	23.3170	5.4417 e+005
Lena	12.0624	8.3079 e+006
Baboon	12.5338	8.2712 e+006
Pepper	13.7756	7.2422 e+006
Flower	15.6990	5.4762 e+006

IV. CONCLUSIONS

The above mentioned process presents an encryption method for color Visual Cryptography scheme with various Error diffusion methods and VIP Synchronization for visual quality improvement. Floyd and Steinberg, modified Floyd, Jarvis and Stucki error diffusion methods are compared. Visual quality of shares and secret image is higher when Jarvis algorithm is used, but processing is very fast when Floyd-Steinberg is used. For encryption VIP synchronization is used. It holds the original pixels in the actual VIP values to produce meaningful shares. The secret information is revealed by overlapping of meaningful shares.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography", in EUROCRYPT '94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 1-12, 1995.

[2] A. Ross and A. A. Othman, "Visual Cryptography for Biometric Privacy", IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70-81, 2011.

[3] N. Askari, C. Moloney and H.M. Heys,"A Novel Visual Secret Sharing SchemeWithout Image Size Expansion", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, pp. 1-4, 2012.

[4] G. Ateniese, C. Blundo, A. De Santis and D.R. Stinson, "Extended Capabilities for Visual Cryptography", Theoretical Computer Science, vol. 250, pp. 143-161, 2001.

[5] R. W. Floyd and L. Steinberg, "An Adaptive Algorithm for Spatial Gray Scale", in Proceedings of the Society for Information Display, vol.17, no. 2, pp.75-77, 1976.

[6] C.C. Chang, C.S. Tsai, T.S. Chen, A technique for sharing a secret color image, Proceedings of the Ninth National Conference on Information Security, Taichung, May 1999, pp. LXIII–LXXII.

[7] Inkoo Kang, Gonzalo R Arce and Heung-Kyu Lee," Color Extended Visual Cryptography using Error Diffusion", in IEEE Transactions on Image Processing, Vol. 20, no.1,pp.132-145,2011

[8] Pankaja P, Bharati P, "Visual Cryptography for Color Images using Error Diffusion and Pixel Synchrpnization", in IJLTET, vol. 1, no.2, pp 1-10,2012.

[9] Young-Chang Hou,"Visual Cryptography for Color images", in Pattern Recognition 36(2003) 1619-1629.

[10] N.Askari, H.M.Heys and C.R.Moloney, "Extended visual cryptography scheme without pixel expansion for Halftone Image", in 26th IEEE conference, pp. 1-6,2013