Extended Visual Cryptography for Color Images and its PSNR Analysis

L M Varalakshmi
Associate Professor
ECE Dept, SMVEC
Pondicherry University
Pondicherry, India

Prithy R
Final year student
ECE Dept, SMVEC
Pondicherry University
Pondicherry, India

Radhika Parameswari
Final year student
ECE Dept, SMVEC
Pondicherry University
Pondicherry, India

ABSTRACT
Visual cryptography (VC) is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Color visual cryptography encrypts a color secret message into n color halftone image shares. Some methods for color visual cryptography are not satisfactory in terms of producing either meaningless shares or meaningful shares with low visual quality, leading to suspicion of encryption. In order to reduce the size and the distortion of decrypted image we propose the visual cryptography for color image using visual information pixel (VIP) synchronization and floyd error diffusion dithering technique. This technique improves the quality of decrypted image compared to other dithering techniques. Comparisons with previous approaches show the superior performance of the new method.

Keywords
Color meaningful shares, digital halftoning, floyd error diffusion, secret sharing, visual cryptography (VC).

1. INTRODUCTION
It is now common to transfer multimedia data via the Internet. There is a need to solve the problem of ensuring information safety in today's increasingly open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content cannot be detected even though unauthorized persons steal the data.

Naor and Shamir proposed a new cryptography area, visual cryptography [1], in 1994. The most notable feature of this approach is that, it exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography.

The threshold scheme [10] makes the application of visual cryptography more flexible. In a k-out-of-n scheme of VC, a secret binary image is cryptographically encoded into n shares of random binary patterns. The n shares are xeroxed onto n transparencies, respectively, and distributed amongst n participants, one for each participant. No participant knows the share given to another participant. Any k or more participants can visually reveal the secret image by superimposing any k transparencies together. The secret cannot be decoded by any k-1 or fewer participants, even if infinite computational power is available to them.

Aside from the obvious applications to information hiding, there are many applications of VC, which include general access structures, copyright protection, watermarking visual authentication and identification, print and scan applications, etc. There have been many published studies of visual cryptography. Most of them, however, have concentrated on discussing black-and-white images, and just few of them have proposed methods for processing gray-level and color images.

There is a general method for VC scheme based upon general access structure [4]. 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. 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.

The concept of extended visual cryptography (EVC) [5] is developed in which shares contain not only the secret information but are also meaningful images [2]. Hypergraph colorings are used in constructing meaningful images by random distributed pixels, the resultant binary shares contain strong white noise leading to inadequate results.

This paper introduces a color VC encryption method to generate meaningful shares. It is based on two fundamental concepts used in the generation of shares they are error diffusion and pixel synchronization. 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 and also maintains the pixel position throughout the channels.

2. EXTENDED VC
Fig 1 illustrates the concept of Extended Visual Cryptography. A (k,n) - EVC scheme takes a n original image and secret images as input and produces n encrypted shares with approximation of original images. This type of visual cryptography, which reconstructs the image by stacking some meaningful images together, is especially called Extended Visual Cryptography, that satisfy the following three conditions:

• Any k out of n shares can recover the secret image;

• Any less than k shares cannot obtain any information of the secret image;

• All the shares are meaningful images; encrypted shares and the recovered secret image are colored.

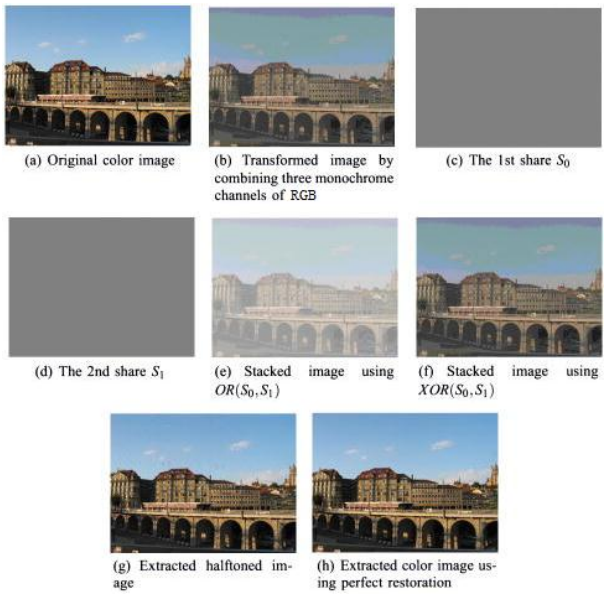


Fig 1: Concept of Extended VC

3. COLOR MODELS

3.1 Additive Model

In this color model, the three primary colors are red, green, and blue (RGB) [7], with desired colors being obtained by mixing different RGB channels as in Fig 2. By controlling the intensity of red, green, blue channels, we can modulate the amount of red, green, blue in the compound light. The more the colors are mixed, the more the brightness of the light. When mixing all red, green and blue channels with equal intensity, white color will result. The computer screen is a good example of the additive color model.

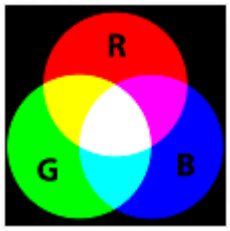


Fig 2: Additive model

(0; 0; 0) represents full black
(255; 255; 255) represents full white

3.2 Subtractive Model

In this model, color is represented by applying the combination of colored-lights reflected from the surface of an object. By mixing cyan, magenta and yellow pigments, we can produce a wide range of colors as in Fig 3. The more the pigments are added, the lower the intensity of the light is and, thus, the darker the light is. This is the reason it is called the subtractive model. Cyan, magenta, and yellow are the three primitive colors of pigment which cannot be composed from other colors. The color printer is a typical application of the subtractive model.

Fig 3: Subtractive model

(0; 0; 0) represents full white
(255; 255; 255) represents full black

4. HALFTONE TECHNOLOGY

Halftoning is the process of transforming an image with greater amplitude resolution to one with lesser amplitude resolution as in Fig 4. In otherwords, halftone is the reprographic technique that simulates continuous tone imagery through the use of dots, varying either in size, in shape or in spacing, where continuous tone imagery contains an infinite range of colors or greys. The halftone process reduces visual reproductions to an image that is printed with only one color of ink, in dots of differing size.

For color images, there are two alternatives for applying half toning. One is to split the color image into channels of cyan, magenta and yellow. Then each channel is treated as a gray scale image to which halftoning and visual cryptography are applied independently. The alternative approach would be to directly apply color halftoning [6], then perform the separation into color channels followed by the application of visual cryptography to each channel independently. Actually, these two approaches lead to the same results finally. Error diffusion usually produces superior quality results compared to other techniques.

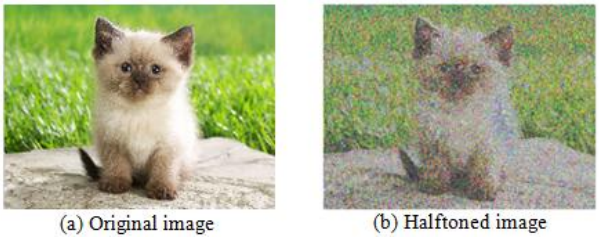


Fig 4: Example of Halftoning

5. VIP SYNCHRONIZATION

Our encryption method focuses on VIP synchronization across 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 subpixels of the encrypted share, there are λ number of VIPs, denoted as c_i and the remaining (m-λ) pixels deliver the message information of the secret message image. Thus, in our method, each subpixel carries visual information as well as message information, while in other methods, extra pixels are needed in order to produce meaningful shares, which results in pixel expansion. Since each VIP is placed at the same bit position in subpixels across the three color channels, VIP represents accurate colors of the original image.

The encryption process starts with basis matrices distribution by referring secret message pixels as in Fig 5. Subpixel encryption of three channels corresponding to each message pixel is followed by random permutation. Furthermore a set of

encrypted sub pixels for three channels should be permuted at the same time to preserve the VIP synchronization.

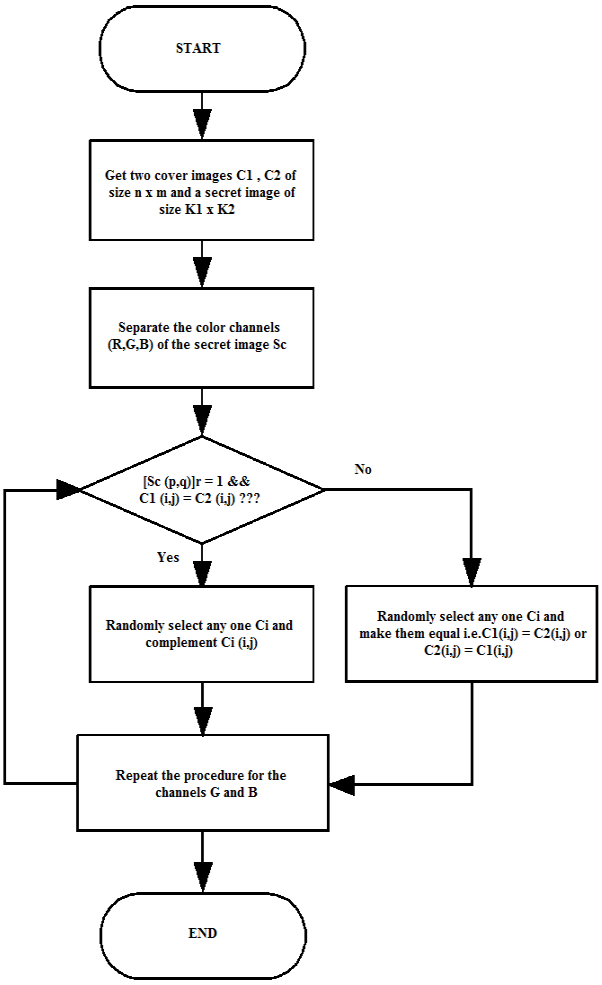


Fig 5: Procedure of VIP Synchronization

6. ERROR DIFFUSION

Error diffusion [9] is a type of halftoning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. It is classified as an area operation, because what the algorithm does at one location influences what happens at other locations. It 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.

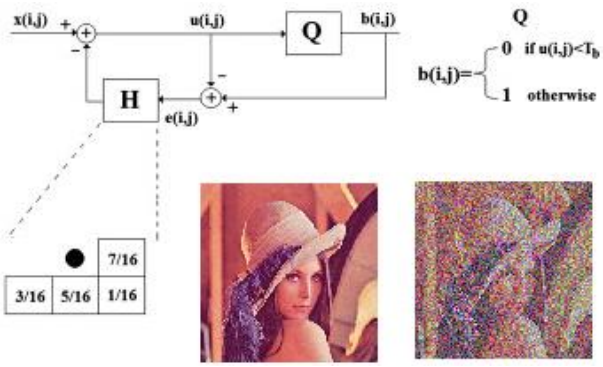


Fig 6: Block diagram of Error Diffusion with example

Fig 6 shows a error diffusion block diagram, where x(i,j) represents the current pixel position, u(i,j) is the sum of x(i,j) and the diffused errors, b(i,j) is the output quantised pixel value and its value will be 0 or 1 depending on the threshold, e(i,j) is the difference between u(i,j) and the b(i,j). And e(i,j) is the error which is the difference .This recursive structure shows the output not only depends on the present input and output but also the past input and output. By this, the error is filtered from one pixel to another and thus generate shares pleasant to human eyes.

6.1 Floyd Error-Diffusion Filter

The Floyd-Steinberg dithering algorithm is based on error dispersion. The algorithm achieves dithering by diffusing the quantization error of a pixel to its neighboring pixels, according to the distribution,

$$\text{Filter} = \frac{1}{16}\begin{bmatrix} & * & 7 \\ 3 & 5 & 1 \end{bmatrix}$$

The element indicated with a star (*) indicates the pixel currently being scanned. Here, for each one point in the image, first find the closest color available. The algorithm scans the image from left to right, top to bottom, quantizing pixel values one by one, calculate the difference between the value in the image and the color you have. Each time the quantization error is transferred to the neighboring pixels, while not affecting the pixels that already have been quantized. Hence, if a number of pixels have been rounded downwards, it becomes more likely that the next pixel is rounded upwards, such that on average, the quantization error is close to zero.

6.2 Algorithm : Floyd Error Diffusion

1**: procedure FLOYD ERROR DIFFUSION**

2: **for** i=1,……..n **do**

3: **for** j=1,……m **do** (This algorithm goes through all pixels in the original image, normally starting from the pixel up to the left and then goes through all pixels from left to right and up down).

4: **if** x(i,j) >127

then

b(i,j)=1

else

b(i,j)=0

5: Since the pixel value in *x*, which is a real number between 0 and 255, has been replaced by 0 or 1 in *b* and "error" has been calculated.

e = u(i,j) – b(i,j)

The "error" is the difference between the pixel value in *x* and *b* at that position.

6: The error occurred at the position (i,j) is weighted by 7/16 and added to the pixel value at (i, j+1). The same error is weighted by 1/16 and added to the pixel at (i+1,j+1) and so on.

$$u(i,j) = x(i,j) + \sum_{k,l \in S} h(k,l)\, e(i-k,j-l)$$

After the error has been diffused the pixel value of the next position is compared to the threshold and the same process continues until all pixels have been met.

7: **end for**

8: **end for**

9: **end procedure**

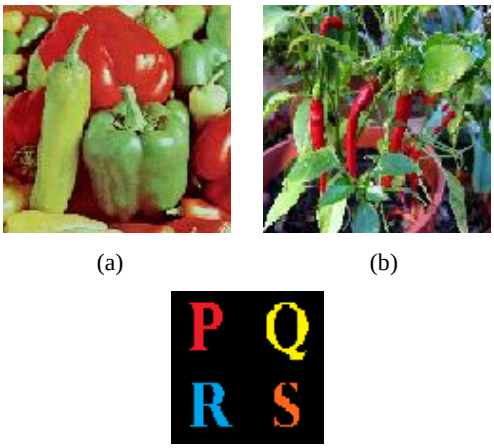
7. STACKING

Decoding does not need any algorithm. The meaningful shares are XORed to reconstruct the secret image by simply human vision system without any complex computation.

8. SIMULATION RESULTS

The algorithms discussed above are implemented using MATLAB R2011a. To test the performance of these algorithms 2 cover images "Pepper" , "Chilli" and a secret image "PQRS" belonging to different classes are used.

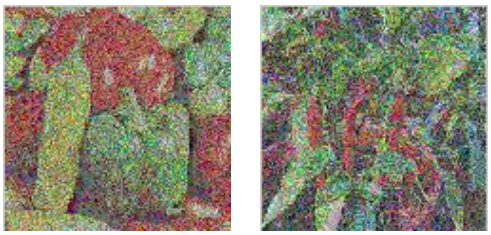
We provide some experimental results to illustrate the effectiveness of the proposed method. Example are composed with (2, 2) Color VC. The secret image of size 128x128 pixels and covering images of size 256x256 in natural colors are provided for the share generation. Fig 7 to 15 represent the results of each step of the system. Size of images is resized to fit in the paper.



(a) (b)

(c)

Fig 7: (a) & (b) Input Cover Image of size 256 x 256
(c) Input Secret Image of size 128 x 128



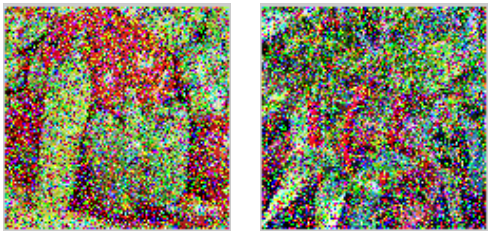
(a) (b)

Fig 8: Haftone shares of cover images

All the images are halftoned before encryption process as in Fig 8 (a) and (b). Halftone images create a space so that we can embed the secret message into cover images. The secret image "PQRS" in Fig 7 (c) has been splitted into three channels RGB [8] based on the additive color model which is shown in the Fig 9. Fig 9 (a) is the red channel of the secret image while Fig 9 (b) & (c) are green and blue channel respectively.

(a) (b) (c)

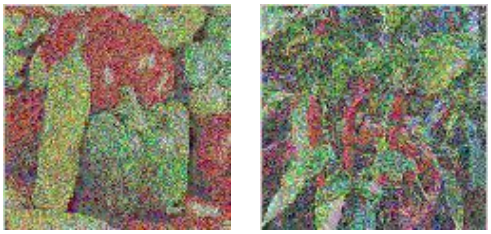
Fig 9: Color Decomposition of the secret image
(a) R channel (b) G channel (c) B channel



(a) (b)

Fig 10: Shares generated by VIP Synchronization

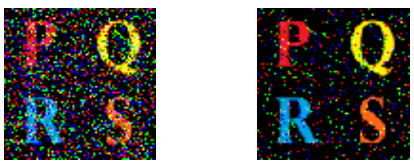
Then the pixels of the secret image has been moved to the halftoned shares which is shown in the Fig 10 (a) & (b), where Fig 10 (a) is the share of input image Fig 7(a), created by the VIP synchronization and Fig 10 (b) is for Fig 7 (b).



(a) (b)

Fig 11: Shares generated by Floyd Error Diffusion

Then the Floyd error diffusion is carried out on the shares generated by VIP synchronization, then the resultant shares would be as Fig 11 (a) & (b).



(a) (b)

Fig 12: (a) Decrypted output of Fig 10
(b) Decrypted output of Fig 11

The Fig 12 (a) & (b) are the decrypted outputs of the encrypted shares of Fig 10 (a) & (b) and Fig 11 (a) & (b) respectively. It is evident from the Fig 12 (b) that the visual quality of the image obtained by decrypting the shares of Floyd error diffusion is better than the output as in Fig 12(a) produced by the shares of VIP synchronization.

Here, the visual quality and contrast has been improved by maintaining the pixel positions and diffusing the errors to neighbouring pixels. The color of the image have been clear in comparison with the standard techniques in [3].

8.1 PSNR Analysis

Peak-Signal-to-Noise Ratio, which is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR expressed in terms of logarithmic decibel scale which is an approximation to human perception of reconstruction quality. Higher PSNR generally indicates that the reconstruction is of higher quality.

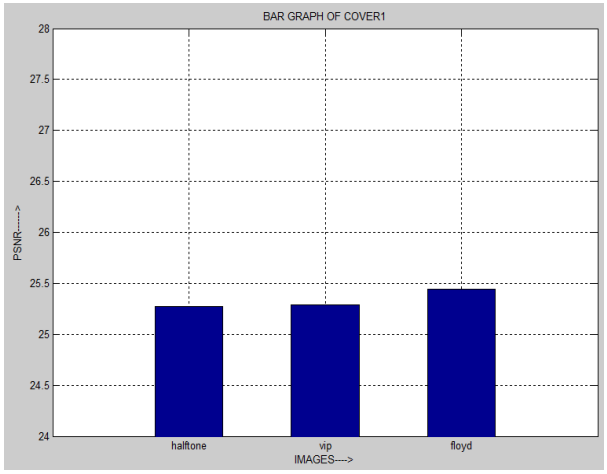


Fig 13: Different no. of share generation of cover 1 "Pepper" image

In Fig 13 and Fig 14, the PSNR values of shares generated by halftone, VIP synchronization and Floyd error diffusion for Fig 7 (a) and (b) are evaluated and their comparison is shown in bar graph.

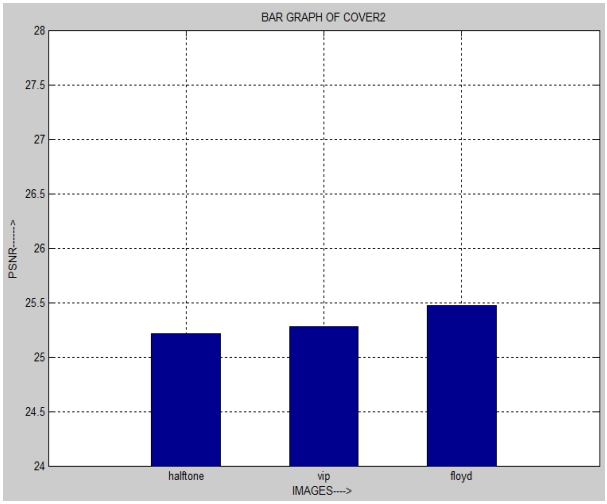


Fig 14: Different no. of share generation of cover 2 "Chilli" image

Fig 15 shows the PSNR analysis of the decrypted secret image "PQRS" produced by overlapping the shares of VIP synchronization as well as the shares of Floyd error diffusion.

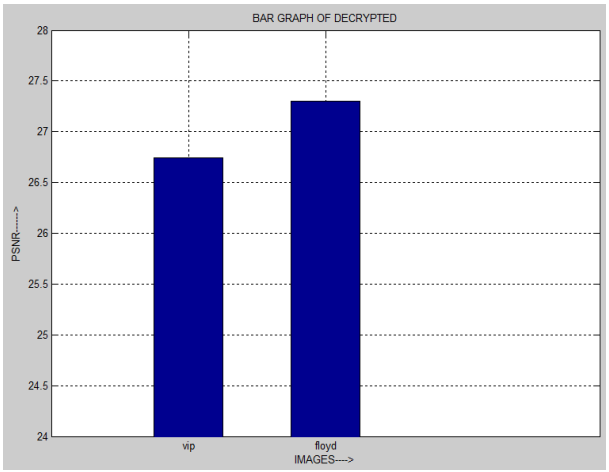


Fig 15: Decrypted output produced from shares of VIP and Floyd

In Table 1, the PSNR values of all the shares generated and the decrypted output are tabulated.

Table 1. PSNR values of different shares and decrypted output

	HALFTONE	VIP	FLOYD
COVER1	25.2733	25.2923	25.4398
COVER2	25.2106	25.2779	25.4705
DECRYPTED	NIL	26.7453	27.3044

It is obvious that the reconstructed image produced by Floyd is very much similar to original image as compared to VIP Synchronization. This means there is very small amount of data loss in Floyd halftone method.

9. CONCLUSION AND FUTURE WORK

This paper presents an encryption method for EVC scheme by proposing VIP synchronization and error diffusion to construct the meaningful shares with high visual quality that are pleasant to human eyes. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels. It also prevents the color and contrast of original images from degradation. Error diffusion is used to construct the encrypted shares such that the noise introduced by the processed pixels while processing the current pixel, are diffused away to neighboring pixels. So that it produces the halftone images with high visual quality. The obtained visual quality is better than that attained by any other available VC method. Either VIP synchronization or error diffusion can be broadly used in many VC schemes for color images.

10. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.

[2] Hsien-Chu Wu1, Hao-Cheng Wang2, and Rui-Wen Yu3, "Color Visual Cryptography Scheme Using Meaningful Shares", Eighth International Conference on Intelligent Systems Design and Applications, February 2010.

[3] SaiChandana B., Anuradha S., "A New Visual Cryptography Scheme for Color Images", International Journal of Engineering Science and Technology, Vol 2 (6), 2010.

[4] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inform. Comput.129 (1996) 86–106.

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

[6] 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.

[7] C. N. Yang and T. S. Chen, "Visual cryptography scheme based on additive color mixing," *Pattern Recognit., vol. 41, pp. 3114–3129, 2008.*

[8] Y. C. Hou, "Visual cryptography for color images," Pattern Recognit., vol. 36, pp. 1619–1629, 2003.

[9] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE, " Color Extended Visual Cryptography Using Error Diffusion," IEEE Transactions on image processing, vol. 20, no. 1, pp. 132-145, January 2011.

[10] R. Escbbach, Z. Fan, K. T. Knox, and G. Marcu, "Threshold modulation and stability in error diffusion," *IEEE Signal Process. Mag.*, vol. 20, no. 4, pp. 39–50, Jul. 2003.