Error Diffusion Based Cryptography for color images

Ashan Muhukumara, Jinliang Li

College of mechanical and electronic Engineering, Shandong University of Science and Technology Qingdao, China

shan_muthukumara86@yahoo.com

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. As a result of rapid advancement of various kinds of Internet technologies, more information is transmitted to all parts of the world from everywhere through the Net. Visual cryptography (VC) plays a vital role in present days where security is required. Color visual cryptography encrypts a color secret message into n color halftone image shares. Halftone is the process of transforming an image with greater amplitude resolution to one with lesser amplitude resolution. Color VC scheme implemented in this dissertation encrypts informative color image in such a way that result of encryption is in the form of shares. Shares do not reflect any information directly, information is scrambled instead. Each share carries some information which in unreadable. This dissertation 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. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates high quality shares. In this Dissertation visual cryptography is implemented using MATLAB. code is written for encryption and decryption process.

Keywords

Meaningful color shares, error diffusion, visual cryptography, Encryption, Decryption.

1. 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 copyright protection and general access structures and so on. Visual cryptography scheme takes a secret image as input and generate two or more shares.

Those shares are not meaningful generally. 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 that can reduce the contrast loss problem in the images that have been reconstructed.

Little research has been carried out on VC, a more general method for VC scheme is 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. But this technique gives good result on binary images. In extended visual cryptography (EVC) method, a share contains not only the secret information but are also some meaningful binary images are developed. In this method Hypergraph colorings are used for constructing meaningful binary shares. Since, hypergraph colorings are constructed by random pixels distribution, the resultant binary shares contain strong white noise leading to insufficient results. A VCS for color images based upon an additive color This paper introduces a color VC encryption method to generates meaningful shares. It 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.

This paper is organized as follows. Section II describes the proposed method which uses error diffusion and VIP synchronization. Section III shows experimental results of the new method and comparisons of Error diffusion methods. Finally, we conclude this paper in Section IV.

2. Implementation

The System is designed into 2 phases. The first phase generates shares by using the error diffusion algorithm and Pixel Synchronization. The Figure 1 explains the working of the system.

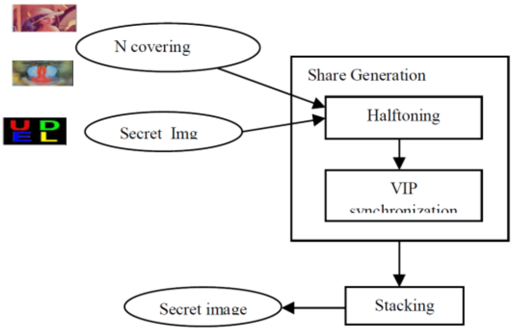


Figure 1 : Block diagram of system design

2.1 Error Diffusion Halftoning

Error diffusion produces halftone images of much higher quality than other halftone. It quantifies each pixel using a neighborhood operation. A schematic diagram of error diffusion method is given in figure 2. 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.

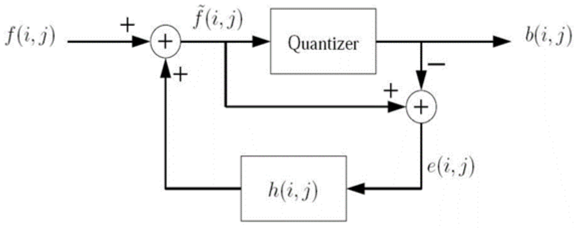
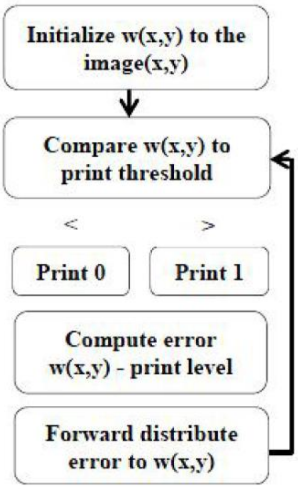


Figure 2: Error Diffusion block diagram

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 neighbor and how this error is pushed is decided by an error diffusion matrix.


Initialize w(x,y) to the image(x,y)
Compare w(x,y) to print threshold
<
>
Print 0
Print 1
Compute error w(x,y) - print level
Forward distribute error to w(x,y)

In the CMYK colored halftone process 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 more patterns, each screen is set to a different angle as shown in figure 3.

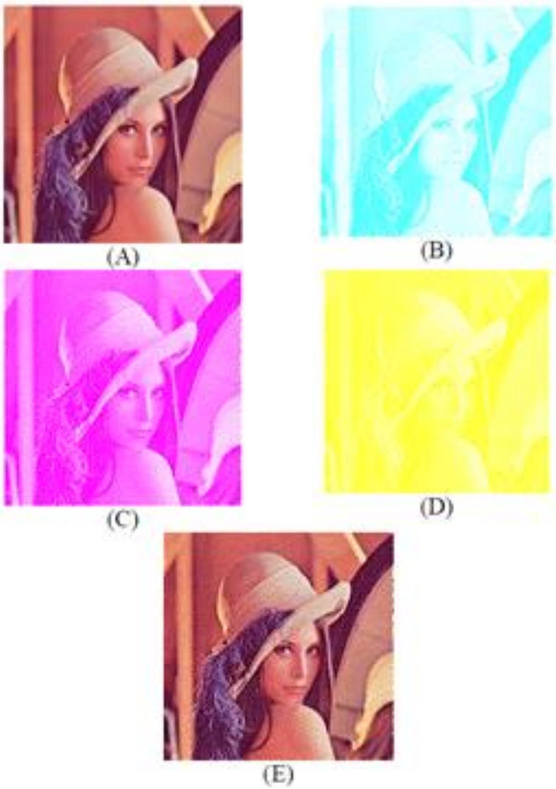


Figure 3 A: original image B: cyan halftone C: magenta Halftone D: Yellow halftone E: color halftone

2.2 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 [4] extra pixels are needed in addition to the pixel expansion *n* to produce meaningful shares.

Algorithm: VIP synchronization

```
Input: C1, C2 covering Images of size n x m, Sc secret  image of size K1xK2.
Output: 2 meaningful shares
1: procedure: VIP Synchronization and Matrix Distribution
2: for p=1,………..K1 and for q=1,………K2 do
3:   for the color channel R of the secret image ScR(p,q) do
4:     if the bit ScR(p,q)=1 then
         for i=1,………..K1 do for j=1,……….K2 do
           if C1(i,j)=C2(i,j) then
             Randomly select any one Ci and complement Ci(i,j)
           end if
5:       end for end for
6:     else if ScR(p,q)=0 then
         for i=1,………..K1 do
           for j=1,……….K2 do
             if C1(i,j) then
               Randomly select any one
               Ci and make them equal i.e.C1(i,j)=C2(i,j) or
               C2(i,j)= C1(i,j)
             end if
         end for end for
       end if
7:   Repeat 3 to 6 for the channel G and Y.
8: end for 9: end for
10: end procedure
```

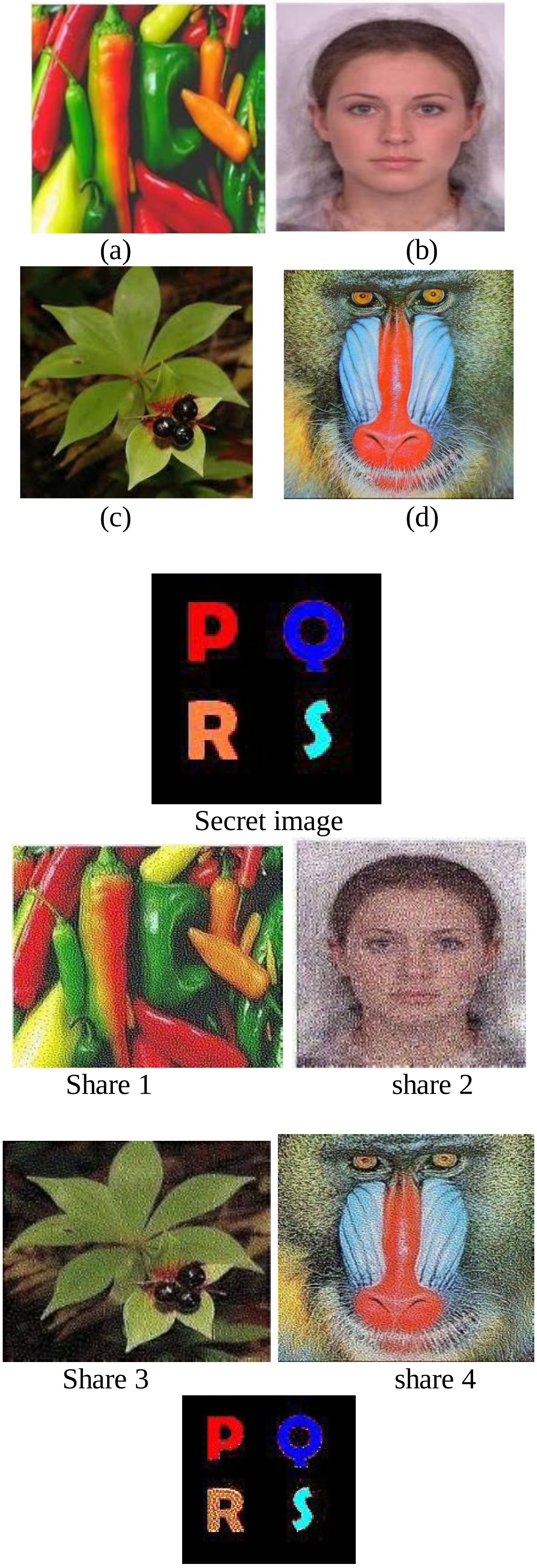
This algorithm takes the input as halftone images which are created by error diffusion method. It decomposes the color images into 3 basic colors (Red, Green, and Blue) and then it executes VIP Synchronization algorithm on each color bit. The output of this block are meaningful shares. Now each bit on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

3. Results and analysis

The algorithms discussed above are implemented using MATLAB 2013. To test the performance of these algorithms 4 color images belonging to different classes of size 128x128 are used

3.1 Results

In this section, we provide some experimental results to illustrate the effectiveness of the proposed method. Example are composed with ((3,4) color VC. The secret message of size 128x128 pixels and covering images of size 256x256 in natural colors are provided for the share generation. Figure 5 and 6 represent the results of each step of the system. Size of images is resized to fit in the paper.



(a) (b)

(c) (d)

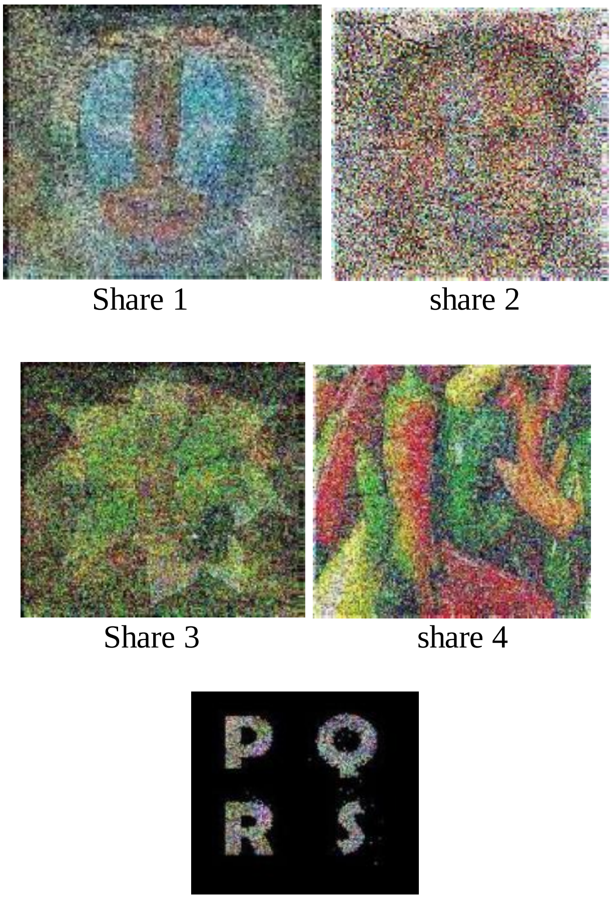
Secret image

Share 1 share 2

Share 3 share 4

Secret image

Figure5: Result of Halftonning images



Share 1 share 2

Share 3 share 4

Reconstructed secret image

Figure 6: Result of encrypted images and reveled secret image

4. Conclusion

The proposed system presents an encryption method for color Visual Cryptography scheme with Error diffusion and VIP Synchronization for visual quality improvement. 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.

Acknowledgment

Author sincerely thank Prof. Li Jin Liang for his valuable assistance and guidance in preparing this paper.

References

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

[2] M.S. Fu and O. C. Au, “Joint visual cryptography and watermarking,” in Proc. IEEE Int. Conf. Multimedia Expo, 2004, pp.

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

[4] S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.