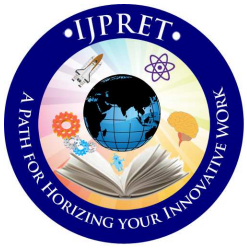
Research Article *ISSN: 2319-507X*
Mrunali Gedam, IJPRET, 2013; Volume 1(8): 1073-1081 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

VISUAL CRYPTOGRAPHY FOR COLOR IMAGES USING ERROR DIFFUSION

MRUNALI T. GEDAM, VINAY S. KAPSE

Department of Computer Science and Engineering, Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur, India.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Color Meaningful Shares,
Digital Half toning,
Secret Sharing,
Error Diffusion Visual Cryptography (VC).

Corresponding Author

Ms. Mrunali T. Gedam

Abstract

The important issue of visual cryptography is visual quality of recovered image. Color visual cryptography (VC) scheme is used to encrypt a color secret message into n color halftone shares image. This paper presents Visual Cryptography for color images to generate two meaningful shares with better visual quality of recovered image. a new simple VIP algorithm is proposed to generate meaningful shares. (VIP) synchronization technique to generate meaningful color share with high visual quality and Error Diffusion is used to produce halftone image. This method produce better decrypted image compared to other half toning methods and reduces computational complexity. Error diffusion generates shares pleasant to human eyes.

1. INTRODUCTION

Cryptography is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptography can be defined as the conversion of data into a scrambled code that can be sent across a public or private network and deciphered by the intended receiver. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. The correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. This technique divided the image into parts called shares and then they are distributed to the participants. The Decryption side just stacking the shares gets the decoded image.

The basic principles of Visual Cryptography, each pixel of secret binary image are cryptographically encoded into m black and white sub pixel in each share. If secret image pixel is white, encode with a set of four sub pixel each sub pixel has equal probability it contains two of them white and two of them black, thus, the sub pixel set gives no clue as the original value of pixel. When a decrypted sub pixel has two white and two black pixels indicate that the decoded pixel is a white. On the other hand a decrypted sub pixel having four black pixels indicates that the decoded pixel is black.

2. RELATED WORK

Several new methods for VC have been introduced recently in the literature.

Visual cryptography (VC) is a type of secret sharing scheme introduced by Naor and Shamir [1] proposed a k-out-of-n scheme of visual cryptography, a secret binary image is encoded in to n shares and distributed amongst n participants, one for each

participant. No participant knows the share given to another participant. By stacking the k shares decode the secret image. Less than k shares cannot be decoded by secret image. Ateniese [2] 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 of forbidden subset cannot recover secret image.

Chang-Chou Lin, Wen-Hsiang Tsai [3] 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 binary images and a visual cryptography method for binary images is then applied to the resulting dither image. The advantages of this scheme reduce the size of image in ordinary situations. The decoded images can reveal most details of original images.

M. S. Fu and O. C. Au, [4] proposed Joint visual cryptography and watermarking (JVW) algorithm. In this paper use a watermarking technique for visual cryptography. Both halftone watermarking and visual cryptography involve a hidden secret image. For visual cryptography secret image encoded into shares, more shares are required to decode the secret image. For watermarking secret image embedded into watermark halftone image. The (JVW) algorithm has the merits of visual cryptography and watermarking. It embeds the hidden pattern in two high visual quality halftone share images to prevent from hackers. Both shares must be required to extract the secret image.

C. S. Hsu and Y. C. Hou [5] proposed a copyright protection scheme for digital images based on visual cryptography and sampling method. This method can register multiple secret images without altering the host image and can identify the rightful ownership without resorting to the original image.

Nakajima [6] proposed extended visual cryptography for natural images constructs meaningful binary images as shares. This will encode secrets image more securely in

to a shares and also describes the contrast enhancement method to improve the quality of the output images.

Zhou et al. [7] used half toning methods to produce good quality halftone shares in VC. In halftone visual cryptography a secret binary pixel is encoded into an array of Q1 x Q2 sub pixels, is called 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.

E. Myodo [8] proposed a method to generate meaningful halftone images using threshold arrays.

Hou [9] proposed a new approach on visual cryptography for colored images. In this paper two techniques used halftone technology and color decomposition for both gray-level and color visual cryptography. In color decomposition, every color on a color image can be decomposed into three primary colors: C, M, and Y. With the halftone technology, we can transform a gray-level image into a binary image.

Wang et. al. [10] produced halftone share images by using error diffusion techniques. This scheme generates more pleasing halftone shares and diffused errors to neighbor pixels.

Jin, D., Yan, and Kankanhalli [11] proposed a new encoding method that transform gray-scale and color images into monochrome image without loss of any information. This new encoding scheme allows perfect recovery of the secret grayscale or color image.

V. Rijimen [12] presented a 2-out-of-2 VC scheme by applying the idea of color mixture. Stacking two shares with different colors rises a third mixed color.

Koga and Yamamoto [13] used a lattice structure to define the mixing result of arbitrary two colors. It is more desirable to generate meaningful shares which are less suspicious of encryption.

3. THE PROPOSED APPROACH

In this section, we describe the encryption method for color meaningful shares with VIP synchronization. The secret color message is cryptographically encoded into

cover image; this encryption process is called shares. By using VIP synchronization generating meaningful shares image. We describe the VC matrix derivation method for VIP synchronization from a set of standard VC matrices

3.1 Matrix Derivation with VIP Synchronization

Our encryption method focuses on VIP synchronization across color channels. In each of the m sub pixels of the encrypted share, there are λ number of VIPs, denoted as Ci and the remaining (m -λ) pixels deliver the message information of the secret message image. This method, each m sub pixel carries visual information as well as message information.VIP represents accurate colors of the original image.

*Example1 (2,2)- Color EVC Matrices Derivation):*Consider the basis matrices S0 and S1 of (2, 2)-VC scheme with m=4, λ=1 such that:

m - total number of sub-pixel in each share of matrices, λ - VIP pixel show color information

$$S1=\begin{pmatrix}1 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{pmatrix} S0=\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & 1 & 0 & 0\end{pmatrix}$$

The first row in each of the matrices S1 & S0 are (1100) and (1100). We begin by inserting the C1's in the first row of each matrix as (1 1 C1 0) and (1 1 C1 0) the 0s at third position in each row is replaced with C1.

$$S1^{c1,c2} = \begin{pmatrix}1 & 1 & c1 & 0\\ 0 & 0 & 1 & 0\end{pmatrix}$$

$$S0^{c1,c2} = \begin{pmatrix}1 & 1 & c1 & 0\\ 1 & 1 & 0 & 0\end{pmatrix}$$

For the second rows, the condition of S0 & S1 is 0 not found then Switch the second and the third bits of s1. The condition S0 &S1 is 0 found at third position and replace them with C2 resulting in (0 C2 1 1) for S1 and (1 C2 1 0) for S0 the matrices $S1^{c1,c2}$ and $S0^{c1,c2}$ as:

$$S1^{c1,c2} = \begin{matrix}1\\ 0\end{matrix}\begin{pmatrix}1 & c1 & 0 & \\ c2 & 1 & 1 & \end{pmatrix}$$

$$S0^{c1,c2} = \begin{pmatrix}1 & 1 & c1 & 0\\ 1 & c2 & 1 & 0\end{pmatrix}$$

In the example, sub pixels on three color channels of the first share have VIPs at the third pixel and those of the second share have VIPs at the second pixel throughout all channels.

3.2 Distribution of Matrices across Color Channels

The encryption process starts with basis matrices distribution by referring secret message pixels. The encryption shares should be in a form of 3-b per pixel because they will be the results of the half toned shares. Furthermore, the secret message of size k1*k2 should be halftone ahead of the encryption stage as:

$X(p,q)=[xC(p,q),xM(p,q),xY(p,q)] \in \{0,1\}^3$

Where, 1 ≤ p ≤ k1, 1 ≤ q ≤ k1. is a pixel of the message image at location(p,q) composed of three binary bits $xC(p,q),xM(p,q),xY(p,q)$ representing values for Cyan, Magenta and yellow color channels. Each message pixel composed of 3 b is encoded and expanded to sub pixels of length *m* in the encrypted shares *i* as

$X^i(p',q') = \in \{S0^{c1,\dots cn}[i],S1^{c1,\dots cn}[i]\}3$

Each $X^i(p',q')$ corresponds to subpixels on three channels starting at the position(p',q') and each subpixel takes one of the rows in $S0^{c1,\dots cn}$or $S1^{c1,\dots cn}$ according to the bit value of the corresponding color channel of the message pixel.

4. SHARE GENERATION VIA ERROR DIFFUSION

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. In this process of generating halftone shares via error diffusion is that the message information components, are predefined on the input shares such that they are not modified during the halftone process.

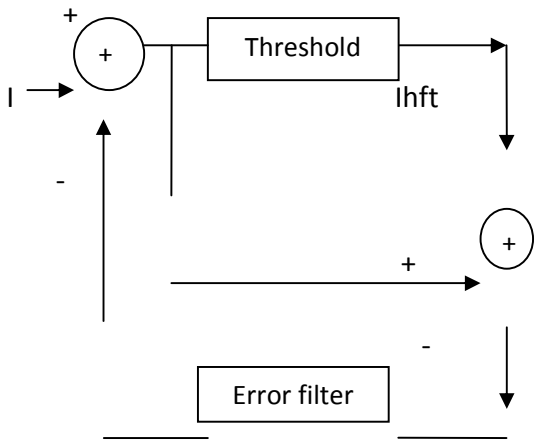


Fig 1. Error Diffusion

$$\begin{pmatrix} 1\ 1\ C1\ 0 \\ 0\ C2\ 1\ 1 \end{pmatrix} \quad \begin{pmatrix} 1\ 1\ C1\ 0 \\ 1\ C2\ 1\ 0 \end{pmatrix}$$

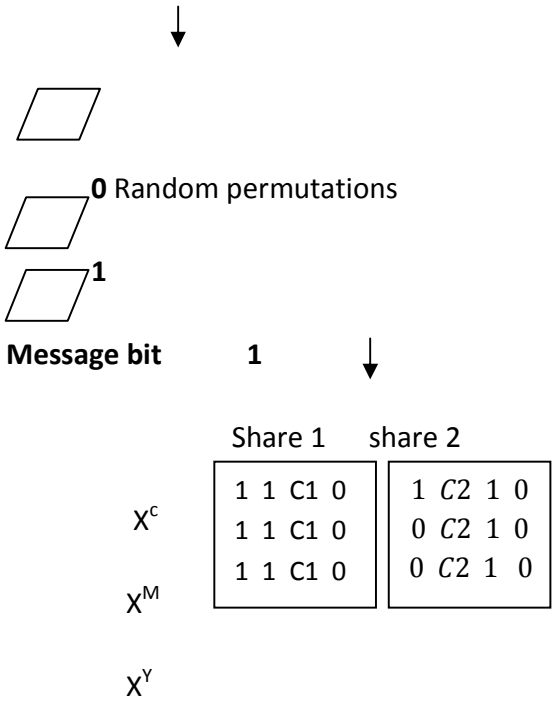


Fig 2(a) matrices distribution with msg pixel

.Share 1 share 2 Extracted pixel

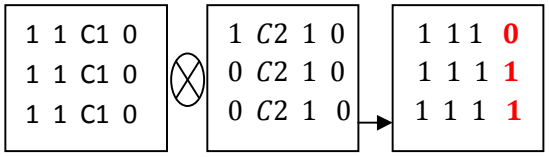


Fig.2.(b) General illustration of matrices distribution of (2, 2)-color EVC.Decryption example of subpixels. Regardless of VIP values. The represents the logical "OR" operation.

5. SIMULATION RESULT

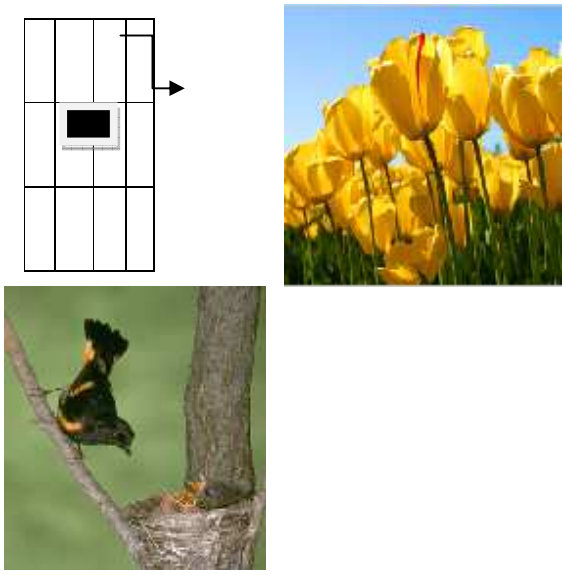


Fig 3. (a) Cover image 1(b) Cover image 2

Fig 4. (a) Secret RGB image (b) Secret CMY image

Fig 5. Encrypted share1and share 2

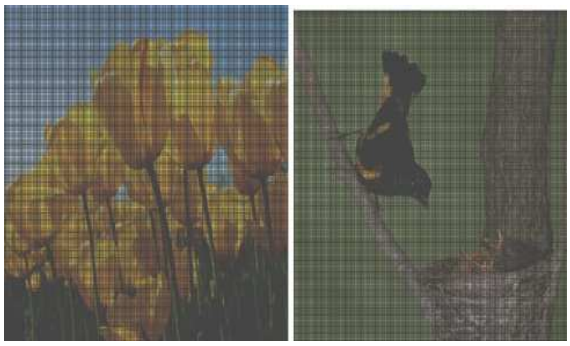


Fig 6. Error diffusion for share 1 & share 2

Fig 7. Extracted secret image

6. CONCLUSION

In this paper we have created the shares using VIP synchronization for visual quality improvement. VIPs synchronize the positions of pixels that carry visual information of original images across the color channels and apply error diffusion on encrypted shares to diffused error so as, we can recognize the colorful secret messages having even low contrast.

7. REFERENECS

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.*, pp. 86–106, 1996.

3. C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, pp. 349–358,2003.

4. M. S. Fu and O. C. Au, "Joint visual cryptography and Watermarking," in *Proc. IEEE Int Conf. Multimedi* 2004, pp. 975–978.

5. C. S. Hsu and Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Opt.Eng.*vol.44, p.077003, 2005.

6. M. Nakajima and Yamaguchi, "Extended VC for natural images," *J. WSCG*, vol. 10, no. 2, 2002.

7. 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.

8. E. Myodo, S. Sakazawa, and Y. Takishima, "Visual cryptography based on void-and-cluster halftoning technique," in *Proc. IEEE Int. Conf. Image Process.*, 2006, pp. 97–100.

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

10. Z. M. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4 pp 383–396, Sep. 2009.

11. Jin, D., Yan and Kankanhalli, M.S., Progressive color visual cryptography. J. Electron. Imaging. v14.

12. V. Rijimen and B. Preneel, "Efficient color visual encryption for shared colors of benetton," presented at the Proc. Eurocrypto Rump Session, 1996 [Online].