International Journal of Electronics and Electical Engineering

Volume 2 | Issue 2 Article 16

October 2013

VISUAL CRYPTOGRAPHY FOR COLOR IMAGES

ASHWATHIMESANGLA AO
Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering,,
aswath.ar@gmail.com

VISUAL CRYPTOGRAPHY FOR COLOR IMAGES

ASHWATHIMESANGLA AO

Telecommunication HOD, Mtech, Digital electronics communication,E&C Dept.,
Dayanand Sagar College of EngineeringDayanand Sagar College of Engineering
Bangalore, IndiaBangalore, India
E-mail : Aswath.ar@gmail.comimelongs@gmail.com

Abstract -Visual cryptography is a secret sharing scheme for encrypting a secret image, it is a perfectly secure way that allows secret sharing without any cryptographic computation, which is termed as Visual Cryptography Scheme (VCS). In this paper secret image is divided into shares (printed on transparencies), and each share holds some information. At the receiver this shares are merged to obtain the secret information which is revealed without any complex computation. The proposed algorithm is for color host image, divided into three color planes Red, Green, Blue and merged with secret image which is binarized and divided into shares. The decoding requires aligning the result obtained by merging color host image and shares, so as to obtain the secret image.

Keywords-*component*: *visual cryptography; secret shari.*

I. INTRODUCTION

Visual cryptography is a popular solutionfor image encryption. Visual cryptography was proposed in 1994 by Naor and Shamir who introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, which they termed as Visual Cryptography Scheme (VCS) [1].Using secret sharing concepts, the encryption procedure encrypts asecret image into the shares(printed on transparencies) which are noise-like secure images which can be transmitted or distributed over anuntrusted communication channel. Using the properties of the HVS to force the recognition of a secret message from overlapping shares, the secret image is decrypted without additional computations and any knowledge of cryptography [2].

VC technique is for binary images where α is the secret image, γ is a randomly generated share while β is the other share such that:

$$\alpha_i + \beta_i = \gamma_i,\ i = 0, 1, 2, \ldots, n$$

Thus without β and γ, α cannot be deduced at all [3]. This scheme provides perfect security with simplicity [4]. Visual cryptography possesses these characteristics:

- Perfect security
- Decryption without the aid of a computing device
- Robustness against lossy compression and distortion due to its binary attribute [4].

In a k-out-of-n scheme of VC, a secret binary image is cryptographicallyencoded into n shares of random binary patterns.The n shares are Xeroxed onto n transparencies, respectively,and distributed among 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 imageby superimposing any k transparencies together. The secretcannot be decoded by any k-1 or fewer participants [5].

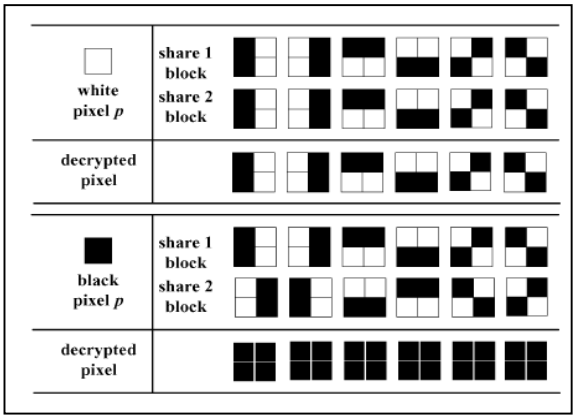

Figure 1: (2, 2) Visual Cryptography scheme

To illustrate basic principles of Visual Cryptography scheme, consider a simple (2, 2)-VC scheme in Fig. 1. Each pixel p from a secret binaryimage is encoded into m black and white subpixels in eachshare. If p is a white (black) pixel, one of the six columns is selectedrandomly with equal probability, replacingp. Regardless of the value of the pixel p, it is replaced by a set of four subpixels,two of them black and two white. Thus, the subpixel set givesno clue as to the original value of p. When two subpixels originatingfrom two white p are superimposed, the decrypted subpixelshave two white and two black pixels. On the other hand,a decrypted subpixel having four black pixels indicates that thesubpixel came from two black p pixels [5].

In applications of image processing, the gray levels of pixels belonging to the object are substantially differentfrom the gray levels of the pixels belonging to the background.Thresholding then becomes a simple but effective tool to separate objects from the background. The output of the thresholding operation is a binary image whose one state will indicate the foreground objects like printed

textwhile the complementary state will correspondto the background. Depending on the application, theforeground can be represented by gray-level 0, that is,black as for text, and the background by the highest luminance for document paper that is 255 in 8-bit images or conversely the foreground by white and the background byblack [6].

Iterative thresholding is being used based on two-class Gaussian mixture models. At iteration n, a new threshold T_n is established using the average of the foreground and background class means [7]. Two similar methods are proposed in [8] [9]. Yanni and Horne [10] initializes the midpoint between the two assumed peaks of the histogram as $g_{mid}=(g_{max}+g_{min})/2$, where g_{max} is the highest nonzero gray level and g_{min} is the lowest one, so that $(g_{max}-g_{min})$ becomes the span of nonzero gray values in the histogram. This midpoint is updated using the mean of the two peaks on the right and left, that is, as $g^*_{mid} = (g_{peak1}+g_{peak2})/2$.

II. ALGORITHM FOR ENCRYPTING COLOR IMAGE

In this paper, assuming an input 24-bit bitmap color image which each 3-byte sequence in the bitmap array represents the relative intensities of red, green, and blue, respectively for image sized 512×512 RGBpixel for the host image and 256×256 for secret image[2].

Step 1: Firstly the color host image Fig.2 is decomposed into three planes under additive model, namely, red, green, blue, RGB. Fig.3shows the three primitive color components of Lena image, where each image has 256 levels of the corresponding primitive color, and each pixelrepresented by three bytes. Converting to (R, G, B),where R, G, B {0-255}.

Figure 2: color host image

Figure 3: primitive color (R, G, B) component

Step 2: Simultaneously secret image is converted to grayscale image, ifit is color image or consider grayscale secret image instead, Fig. 4.

Figure 4: Secret image converted to gray image

Step 3: Converted gray image is further binarized into blocks or pixels, Fig.5, it is done by comparing with local threshold and global threshold, for block if localThresh<= globalContrast and mid_gray >=128, then pixel = 1 or else pixel = 0. For pixel,if pixel>= mid_graythen pixel = 1 or pixel = 0.

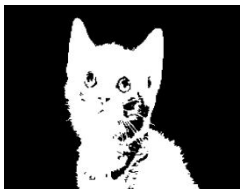

Figure 5: Binarized image

Step 4: Inorder to mix or encrypt three plane of host image with secret image, pixel expansion of secret image has to be done, this is done using (2, 2) VC scheme on binarized block. Hence two shares will be generated namely, share 1 and share 2, each share contains apart of secret image. To generate these shares, secret images are read pixel by pixel and mixing (OR operation) together with pixel of host or cover image.

Step 5: After mixing share 1 and share 2 with three planes RGB we obtain user 1 and user 2. Fig. 6,which when merged together gives the secret image.

Figure 6: user 1 and user 2

Figure 7: Decrypted image

III. EXPERIMENTAL RESULT

Here we consider host image to be color image and secret image converted to binary image so that its size is smaller than the host image. Color host image is merged with secret image to generate shares. In this paper we are using (2, 2) visual cryptography scheme to obtain 2 shares of which 2 user should be present to get back the secret image shown in Fig. 7,the PSNR value of user1 is found to be +21.8000b dB and for user2 is +22.0408 dB . This is a simple method for applying with color image but is not free from pixel expansion and contrast loss hence further improved implementation has to be applied to obtain better result.During binarization process quantization error and noise might be generated hence it has to be minimized.

IV. FUTURE WORK

Future work will be to implement Error diffusion and VIP synchronization 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 shares pleasant to human eyes.

V. CONCLUSION

A visual cryptography technique for color image processing is introduced. This method operates in the decomposed bit levels of the input color vectors of the share outputs. The decryption process satisfies the perfect reconstruction property and recovers the original cover image by logically decrypting the decomposed bit vector-array of the color shares.

REFERNCES

[1] JIM CAI 2003. A Short Survey on Visual Cryptography Schemes,www.wisdom.weizmann.ac.il/naor/PUZZLES /visual.html.

[2] Sozan Abdulla, "New Visual Cryptography Algorithm For Colored Image" JOURNAL OF COMPUTING, VOLUME 2, ISSUE 4, APRIL 2010, ISSN 2151-9617HTTPS://SITES.GOOGLE.COM/SITE/JOURNALOFCOMPUTING/

[3] A. Shamir, "How to share a secret," *Communicationsof the ACM*, vol. 22, no. 11, pp. 612–613, Nov 1979.

[4] 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.

[5] InKoo Kang, Gonzalo R. Arce, and Heung-Kyu Lee "Color Extended Visual Cryptography Using Error Diffusion" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 1, JANUARY 2011.

[6] Mehmet sezgin and bulent sankur "survey over image thresholding techniques and quantitative performance evaluation" journal of electronic imaging, vol 13(1), January 2004.

[7] T. W. Ridler and S. Calvard, ''Picture thresholding using an iterative selection method,'' *IEEE Trans. Syst. Man Cybern.* SMC-8, 630–632, 1978.

[8] C. K. Leung and F. K. Lam, ''Performance analysis of a class of iterative image thresholding algorithms,'' Pattern Recogn. 29(9), 1523–1530, 1996.

[9] H. J. Trussel, ''Comments on picture thresholding using iterative selection method,'' IEEE Trans. Syst. Man Cybern. SMC-9, 311, 1979.

[10] M. K. Yanni and E. Horne, ''A new approach to dynamic thresholding,'' *EUSIPCO'94: 9th European Conf. Sig. Process.* 1, 34–44, 1994.

◈◈◈