International Conference on Information Engineering, Management and Security
2015 [ICIEMS 2015]

ISBN	978-81-929742-7-9	**VOL**	01
Website	www.iciems.in	**eMail**	iciems@asdf.res.in
Received	10 - July - 2015	**Accepted**	31- July - 2015
Article ID	ICIEMS032	**eAID**	ICIEMS.2015.032

Application of Color Segregation in Visual Cryptography using Halftone Technique and RGB Color Model

Mr. Prasun Kumar Mitra[1], Mr. Souradeep Sarkar[2], Mr. Debasish Hati[3]
[1,2,3]Lecturer, CST Department, Technique Polytechnic Institute
Hooghly,WB-712102,India

Abstract: *Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. This experiment describes a secret visual cryptography scheme for color images based on halftone technique. Firstly, a chromatic image is decomposed into three monochromatic images in tones of Red, Green and Blue. Secondly, these three images are transformed into binary images by halftone technique. Finally, the traditional binary secret sharing scheme is used to get the sharing images. This scheme provides a more efficient way to hide natural images in different shares. Furthermore, the size of the shares does not vary when the number of colors appearing in the secret image differs.*

Keywords: Visual cryptography, secret sharing, color image, halftone technique.

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (pictures, text etc.) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers. As network technology has been greatly advanced, much information is transmitted via the Internet conveniently and rapidly. At the same time, the security issue is a crucial problem in the transmission process. For example, the information may be intercepted from transmission process. This method aims to build a cryptosystem that would be able to encrypt any image in any standard format, so that the encrypted image when perceived by the naked eye or intercepted by any person with malicious intentions during the time of transmission of the image is unable to decipher the image.

Visual Cryptography Scheme (VCS), introduced by Naor and Shamir in 1994, is a type of secret sharing techniques for images. The idea of VCS is to split an image into a collection of random shares (printed on transparencies) which separately reveal no information about the original secret image other than the size of it. The image is composed of black and white pixels, and can be recovered by superimposing a threshold number of shares without any computation involved. Here is an example using a dithered black-and-white Lena image as the original secret image (Fig. 1).

Cite this article as: Prasun Kumar Mitra, Souradeep Sarkar, Debasish Hati. "Application of Color Segregation in Visual Cryptography using Halftone Technique and RGB Color Model." *International Conference on Information Engineering, Management and Security (2015)*: 195-198. Print.

Fig. 1. Original Secret Image

Fig. 2. Dithered

By applying the Naor-Shamir 2-out-of-2 visual cryptography algorithm, two shares (printed on transparencies) are created, which separately reveal no information about the original image. It can only be recovered when both of the shares are obtained and superimposed. Fig. 3 shows the two shares and the superimposition of them. Note that the size of the images is expanded by a factor of 4.

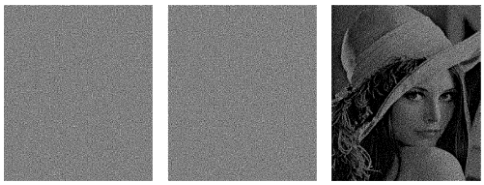

Fig. 3. Two Shares and the Superimposition of the Shares

The technology makes use of the human vision system to perform the OR logical operation on the superimposed pixels of the shares. When the pixels are small enough and packed in high density, the human vision system will average out the colors of surrounding pixels and produce a smoothed mental image in a human's mind. For example, a block of 2 × 2 pixels shown below will be viewed as a gray-like dot as the two black pixels and the two nearby white pixels are averaged out. If we print the 2×2 pixel blocks shown in Fig. 4 separately onto two transparencies and superimpose them. This effect is equivalent to performing a pixel-wise OR logical operation on each of the four pairs of pixels between these two transparencies. The result is shown in Fig. 5. One of the unique and desirable properties of VCS is that the secret recovery process can easily be carried out by superimposing a number of shares (i.e. transparencies) without requiring any computation.

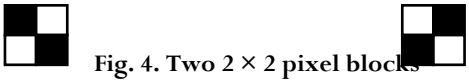

Fig. 4. Two 2 × 2 pixel blocks

Fig. 5. Superimposed Image

Besides black-and-white images, a natural extension of this research problem is to perform secret sharing on color images. Hou proposed three VCS for color images. Among them, the first one uses four shares to split a secret image. The four shares are called black mask, C (Cyan) share, M (Magenta) share and Y (Yellow) share. This scheme reproduces the best quality among the three in terms of image contrast during secret image recovery process. It is also the only one supporting a practically useful feature called two-level security control. This feature allows an authority to keep a particular share, the black mask, secret and release the other three shares to the public, without worrying about exposing the concealed image. In particular, the author claimed that this scheme is secure as long as the black mask is kept secret. There would have no information leaked even if all the other three shares, namely C, M, Y shares, are exposed regardless of the color composition of the original secret image.

Advantage of Visual Cryptography:

- Simple to implement.
- Encryption doesn't require any NP-Hard problem dependency.
- Decryption algorithm not required (Use a human Visual System).
- So a person unknown to cryptography can decrypt the message.
- We can send cipher text through FAX or E-MAIL.
- Infinite Computation Power can't predict the mess.

Cite this article as: Prasun Kumar Mitra, Souradeep Sarkar, Debasish Hati. "Application of Color Segregation in Visual Cryptography using Halftone Technique and RGB Color Model." *International Conference on Information Engineering, Management and Security (2015)*: 195-198. Print.

II. RELATED WORKS

The most traditional visual cryptography schemes are used for black and white images. Recently, some visual cryptography schemes for gray or color images have been proposed.

Verheul and Tilborg present a secret sharing scheme for images with c colors. The principle of this scheme is to transform one pixel of image to b sub-pixels, and each sub-pixel is divided into c color regions. In each sub-pixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacked sub-pixels. A major disadvantage of this scheme is that the number of colors and the number of sub-pixels determine the resolution of the revealed secret image. If the number of colors is large, coloring the sub-pixels will become a very difficult task.

Naor and Shamir propose a secret sharing scheme, which reconstructs a message with two colors by arranging the colored or transparent sub-pixels. Both approaches assign a color to a sub-pixel at a certain position, which means that displaying m colors uses m-1 sub-pixels. The resulting pixels contain one colored sub-pixel and the rest of the sub-pixels are black. Therefore the more colors are used; the worse the contrast of the images becomes significantly. Their approaches cannot be applied to the extended visual cryptography either. Rijmen and Preneel presented a scheme which enable multicolor with relatively less sub-pixels (24 colors with m = 4). However each sheet must contain color random images, which means applying this approach to the extended visual cryptography is impossible.

For this reason, Chang, Tsai and Chen recently proposed a new secret color image-sharing scheme based on the modified visual cryptography. In that scheme, through a predefined Color Index Table (CIT) and a few computations they can decode the secret image precisely. Using the concept of modified visual cryptography, the recovered secret image has the same resolution as the original secret image in their scheme. However, the number of sub-pixels in their scheme is also in proportion to the number of colors appearing in the secret image, i.e., the more colors the secret image has, the larger the shares will become. Another disadvantage is that additional space is needed to store the Color Index Table (CIT).

III. EXPERIMENTAL RESULTS

Our experiment is based on the RGB color model and the halftone technique. Firstly, a chromatic image is decomposed into three monochromatic images in tones of red, green and blue. Secondly, these three images are transformed into binary images by halftone technique. Finally, the traditional binary secret sharing scheme is used to get the sharing images. Halftone technique is a method to display a gray image with black-and-white spots. Figure 6 shows the basic principle of the halftone technique. The more black spots the image includes, the more the image will be alike the true gray image. Construct to the other two binary images shown in Fig. 6(c) and (d), Fig. 6(b) is closest to the true gray image.

(a) The true gray image **(b) Binary image1** **(c) Binary image2** **(d) Binary image3**

Fig. 6: Basic principle of halftone technique

In this paper, we use the Floyd-Steinberg Algorithm to get the halftone images. The algorithm is given below:

For an 8-bit gray scale image, the gray value of the image is from 0(black) to 255(white).

Letting b=0,

w=255,

t= int [(b+w)/2] =128.

Assuming g is the gray value of the image, which location is P (x, y), e is the difference between the computed value and the correct value. Then the Floyd-Steinberg Algorithm can be described as following:

If g > t then
print white;
e=g-w;
else
print black;
e=g-b;
(3/8 × e) is added to P (x+1, y);
(3/8 × e) is added to P (x, y+1);
(1/4 × e) is added to P (x+1, y+1);
End if

For example, a point with the gray value of 130 in an image should be gray point. Since the intensity of general image changes continuously, so the values of adjacent pixels are likely close to 130, and the surrounding region is also gray. According to the Algorithm, the number 130 is bigger than 128, then a white point is printed on the new image. But 130 are away from the real white 255. While -46 (-125 multiplied by 3/8) added to adjacent pixel, the value of adjacent pixel is close to 0; the adjacent pixel comes to black. Next time, e also become positive, the adjacent pixel comes to white, so a white one after a black one, gray is demonstrated. If not transmitting the error, the pixel in the new image is white. Take another example; if the gray value of a point is 250, it should be white in gray image, and e equals to -5, it has little impact on the adjacent pixel. This certificates the correctness of the algorithm. In the experiment, First a color image is decomposed into three basic components R, G and B. Then the above Floyd-Steinberg

Cite this article as: Prasun Kumar Mitra, Souradeep Sarkar, Debasish Hati. "Application of Color Segregation in Visual Cryptography using Halftone Technique and RGB Color Model." *International Conference on Information Engineering, Management and Security (2015)*: 195-198. Print.

Algorithm is used to get the halftone images of the corresponding components. After that we get the halftoned red, halftoned green and halftoned blue images.




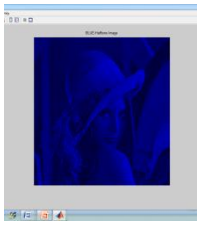

Fig. 7 (a) **Fig. 7 (b)** **Fig. 7 (c)** **Fig. 7 (d)**

Fig. 7 (a) Original Inputted Chromatic Image **Fig. 7 (b) Halftone Image of Red**
Fig. 7 (c) Halftone Image of Green **Fig. 7 (d) Halftone Image of Blue**

If we compose these three monochromatic images into a chromatic image, we can get the following image.

Fig. 7 (e) Merged image of R-G-B Halftones

We can consider every monochromatic image as a secret image and can use the traditional binary image-sharing scheme to divide it into three secret shares with same color, and then, we can choose any three different colors of which to compose them into three colored shares. The original secret information will be visible by stacking any 2 or 3 transparencies, but none secret information will be revealed by only one transparency.

IV. FUTURE SCOPE OF FURTHER IMPROVEMENT

Our future work is to generate shares in such a way so that it can be hidden within different cover images. It will look like some picture, not just a share. So, the original secret shares will be transmitted as hidden within different pictures. Finally, by super imposing these shares, the original secret image will be generated.

ACKNOWLEDGMENT

We would like to thank our respected Executive Director Mr.S.N.Basu ,Principal Dr. Abhijit Chakrabortty and Administration of Technique Polytechnic Institute for motivating us in this research work. We would also like to thank all the members of Technique Polytechnic Institute for their support and co-operation. We thank all mighty God and our parents for their blessings in our life.

REFERENCES

[1] R. Floyd and L. Steinberg, "An adaptive algorithm for spatial greyscale". Journal of the Society for Information Display. pp. 36-37, 1976.
[2] M. Mese and P. P. Vaidyanathan, "Optimized Halftoning Using Dot Diffusion and Methods for Inverse Halftoning". IEEE Trans. On image processing. Vol. 9, No. 4, pp. 691-709, 2000.
[3] Visual Cryptography and Its Applications by Jonathan Weir, WeiQi Yan & Ventus Publishing ApS : 2012.ISBN : 978-87-403-0126-7.
[4] Visual Cryptography and Secret Image Sharing by Stelvio Cimato and Ching-Nung Yang.CRC Press - 2012 by Taylor & Francis Group, LLC

Cite this article as: Prasun Kumar Mitra, Souradeep Sarkar, Debasish Hati. "Application of Color Segregation in Visual Cryptography using Halftone Technique and RGB Color Model." *International Conference on Information Engineering, Management and Security (2015)*: 195-198. Print.