

# Image Encryption – An Intelligent Approach of Color Visual Cryptography

<sup>1</sup>Mohd. Junedul Haque, <sup>2</sup>Mohd. Muntjir, <sup>3</sup>Mohd. Rahul  
College of Computers and Information Technology  
Taif University  
Taif, Saudi Arabia

## ABSTRACT

Visual cryptography is a secret sharing method that uses human eyes to decrypt the secret. It has computation-free decoding process to decrypt the images. Generally visual cryptographic methods utilize the technique of secret sharing in which secret image is divided into shares and when  $k$  shares out of  $n$  stack together the secret image will reveal. In this paper we proposed a method of visual cryptography for colored images. We are using RGB color model for color images. First of all, image is divided into monochromatic channels then converts each individual image to binary image. After this we can apply basic VCS scheme. The secret image can be recovered by stacking share images. We are using Matlab7.4 for implementing our scheme.

## Keywords

Visual Cryptography, Secret Sharing, RGB, Image processing.

## 1. INTRODUCTION

The traveling salesman problem (TSP) is to find a tour of a given number of cities (visiting each city exactly once) where the length of this tour is minimized. The TSP is defined as a task of finding of the shortest Hamiltonian cycle or path in complete graph of  $N$  nodes. It is a classic example of an NP-hard problem. So, the methods of finding an optimal solution involve searching in a solution space that grows exponentially with number of city [1].

Visual Cryptography, Secret Sharing, RGB Cryptography is the enciphering and deciphering of data and information with secret code. Visual cryptography uses the same concept except that it is applied to images. Visual cryptography is a cryptographic technique which applies on such information like 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.

Visual cryptography can also be somewhat deceiving to the inexperienced eye, in such a way that, if an image share were to fall into the wrong hands, it would look like an image of random noise or bad art. Visual Cryptography Scheme (VCS) proposed by the Naor and Shamir serves as a basic model and has been applied to many applications. Naor and Shamir proposed [2] the  $(t, n)$  threshold scheme or  $t$  out of  $n$  threshold scheme, a secret binary image (SI) is cryptographically encoded into  $n$  shares of random binary patterns. The shares are Xeroxed onto  $n$  transparencies, respectively, and distributed amongst participants, one for each participant. No participant knows the share given to another participant. Any  $t$  or more participants can visually reveal the secret image by superimposing any  $t$  transparencies together. The secret cannot be decoded by any  $t-1$  or fewer participants, even if infinite

Computational power is available to them. After this basic concept many researcher find out different schemes for the visual cryptography [1]. This improvement goes to gray scale image to color images and different ways and techniques were developed with amazing ideas.

Verheul and Van Tilborg [3] proposed the scheme that extends the basic visual cryptography scheme from binary image to color

image. In this scheme each pixel is expanded into  $m$  sub pixels. Each sub pixel may take one of the colors from the set of colors.

In 2000 C.N. Yang [8] proposed new VCS scheme for the color images. This scheme is implemented on the basis of a black and white VCS scheme and gets much better block length than the Verheul-Van Tilborg scheme.

## 2. RELATED WORKS

Naor and Shamir [2] provided their constructions of visual cryptographic solutions for the general  $t$  out of  $n$  secret sharing problem. One can assume that every secret message is just a collection of black and white pixels i.e. a binary image. To illustrate the principles of VC, consider the simplest  $(2, 2)$  visual threshold scheme where each pixel  $p$  of the SI is encoded into a pair of sub pixels in each of the two shares as shown in the Fig. 1. The first two pairs of sub pixels in the selected column are assigned to share 1 and share 2, respectively. Since, in each share,  $p$  is encoded into a black–white or white–black pair of sub pixels, independent of whether  $p$  is black or white, an individual share gives no clue as to the value of  $p$ . Now consider the superposition of the two shares as shown in the last row of Fig. 1. If a pixel  $p$  is white, the superposition of the two shares always outputs one black and one white sub pixel, no matter which column of sub pixel pairs is chosen during encoding. If  $p$  is black, it yields two black sub pixels.

There is a contrast loss in the reconstruction; however, the decoded pixel is readily visible Black and white pixels using this basic VCS Scheme we cannot completely recover the white Secret pixel which causes loss in contrast. In XOR based VCS scheme where the share images are superimposed using XOR operation which results in perfect reconstruction of both. Fig. 2 shows an example of  $(2, 2)$  VCS scheme where the share images are larger than the original secret image and decrypted images using XOR operation in superimposition produces the less distorted image.


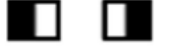


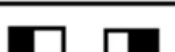

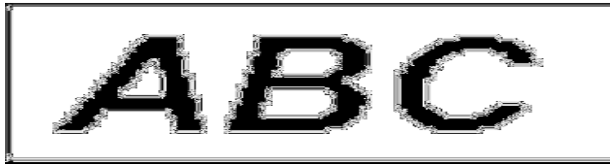
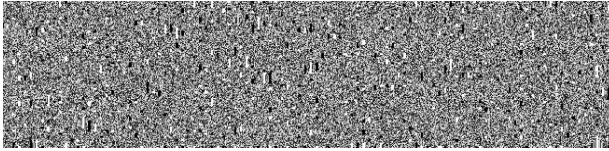
Pixel	White	Black
Share1		
Share2		
Stack Share 1 & 2		

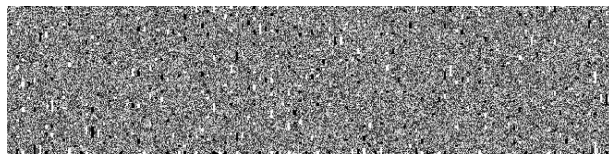
Fig. 1. Construction of a two-out-of-two VC scheme: a secret pixel can be encoded into two sub pixels in each of the two shares.



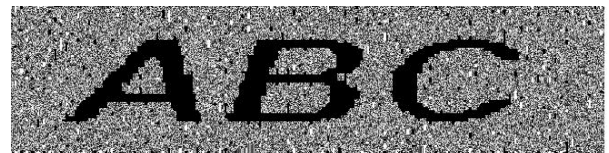
(a) Original binary image



(b) Share 1



(c) Share 2



(d) Decrypted image using OR operation



(e) Decrypted image using XOR operation

Fig. 2 Example of (2, 2) VCS scheme for binary image

### 3. OUR APPROACH

The proposed color image-sharing scheme is based on the RGB color model and the technique which convert the gray scale image to binary image. 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 is the approach presented in [7].

The alternative approach would be to directly apply color half toning, and 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.

#### A. RGB Color Model

There are two color models, additive and subtractive color models. RGB is an additive color model; the three primary colors are red, green and blue. 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. In the subtractive 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. The color printer is a typical application of the subtractive model and hence the visual

cryptography model of Naor and Shamir [2] is also of such kind. Mat lab does not support CVM color model so we use RGB color model. We split the secret image into red, green and blue channel. Each split image is a gray scale image[8].

[SI] Split – to – RGB

$[I_R, I_G, I_B]$

$I_R, I_G, I_B$  – Gray scale Image

#### B. Half Tone Technology

Half toning [4], [6] is the process of transforming an image with greater amplitude resolution to one with lesser amplitude resolution. The halftone is applied to the given image to render the illusion of the continuous tone images on the devices that are capable of producing only binary image elements. A large number of techniques for halftoning have been presented in the literature. These techniques can broadly be divided into two categories: Threshold matrix methods and error-diffusion methods. With threshold matrix [4] methods of half-toning each gray- scale value is approximated using a predefined black and white pixel distribution. These pixel distributions are defined using a threshold matrix representation. In general, this is a satisfactory approach but not without its limitations.

The regular structure of the threshold matrix is apparent and becomes more apparent as the size of the thresholding matrix increases. An alternate approach to this problem is to generate the half-tone approximation of the image one segment at a time. Errors in an image segment's approximation are compensated for when the neighboring image segments are processed. There are a number of techniques based on this approach and they are known as error-diffusion half-toning methods. The classic error-diffusion technique is the Floyd Steinberg method [5].

$$I_{hft}^G \rightarrow (2, 2) \text{ VCS} \rightarrow [S_{0}^G, S_{1}^G]$$

$$I_{hft}^B \rightarrow (2, 2) \text{ VCS} \rightarrow [S_{0}^B, S_{1}^B]$$

Where,  $S_{0}^R, S_{1}^R$  are shares of red channel,  $S_{0}^G, S_{1}^G$  are shares of green channel and  $S_{0}^B, S_{1}^B$  are shares of blue channels respectively.

#### a) Encryption

This stage is for the reconstruction of the original secret image. First stacking all the shares of each channel using XOR operation. There are many other half toning techniques available for selection like dispersed-dot dithering, clustered-dot dithering. In this paper, we use the Floyd-Steinberg Algorithm to get the halftone images. For an 8-bit gray scale image, the gray value of the image is from 0(black) to 255(white).

Letting  $b=0$ ,

$w=255$  &

$t = \text{int} [(b+w)/2] = 128$

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;

$e = g - b$ ;

$(3/8 \times e)$  is added to  $P(x+1, y)$ ;

$(3/8 \times e)$  is added to  $P(x, y+1)$ ;  $(1/4 \times e)$  is added to  $P(x+1, y+1)$ ;

end if

## b) Decryption

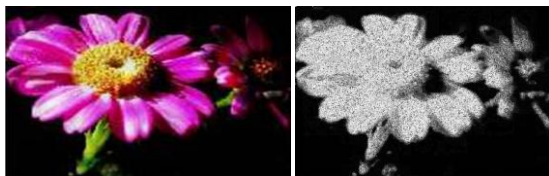
This stage is for the creation of shares. First split the color channel then apply half toning on each channel

[SI] Split – to – RGB [ $I_R, I_G, I_B$ ]

[ $I_R, I_G, I_B$ ] Halftone [ $I_R, I_G, I_B$ ]

Fig. 3(a) is an original chromatic image. Fig. 3(a), (b) and (c) are the decomposed monochromatic images in tones of red, green and blue. Figure 4 shows the halftone image obtained after applying Floyd Steinberg error-iffusion technique to R, G and B channel.

Fig 5 shows the decrypted image after stacking all share of each channel.



(a) Secret image (RGB)

(b) Red channel img

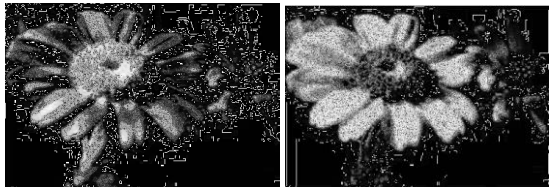
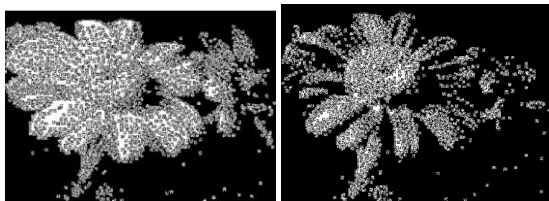
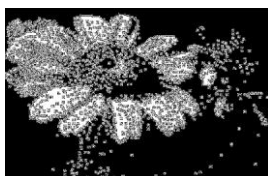


Fig. 3 Color image and its R, G, B channel



(a) Red channel

(b) Green channel



(c) Blue channel

Fig. 4 Halftone image obtained after applying Floyd Steinberg error-iffusion technique to R, G and B channel

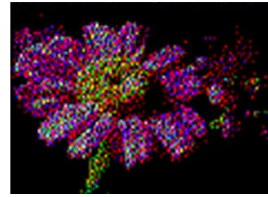


Fig. 5 Decrypted image after stacking all share of each channel.

It is clear that our technique, though independently developed, is quite similar in spirit to the one described in [7]. So both share the same drawback that digital half toning always leads to permanent loss of information which means that the original image can never be perfectly restored. Inverse half toning is a possible solution that can attempt to recover the image.

## 4. CONCLUSION

In this paper we proposed VCS scheme for the color images which uses the error diffusion technique on color channels. The use of color error diffusion technique improves the quality of encrypted image. The XOR operation is used in stacking which produces the better quality of image and there is no expansion in the size of decrypted image. The basic  $(k, n)$  threshold VCS is used for color images in which the size of share image is  $nk-1$ . Further work can be done to reduce the size of share image and improve the quality of halftone shares. The quality of halftone image can be improved by applying the fuzziness to halftones.

## 5. REFERENCES

- [1] C.N. Yang, C.S. Lai, New colored visual secret sharing Scheme, Design, codes and cryptography, vol. 20, pp.325-335, 2000.
- [2] M. Naor, A. Shamir, Visual cryptography, Advances in Cryptology, Eurocrypt 94, Lecture Notes in Computer Science, Vol. 950, pp. 1-12, 1995.
- [3] Verheul, Van Tilborg, Construction and Properties of  $k$  out of  $n$  visual secret sharing scheme Designs, Codes and Cryptography, Vol. 11, pp. 179-196, 1997.
- [4] R. Ulichney. Digital Halftoning. MIT Press, Cambridge, Massachusetts, 1987.
- [5] R.W. Floyd and L. Steinberg. "An adaptive algorithm for spatial grey scale". Proc. Soc. Inf. Display, Vol. 17, pp. 75-77, 1976.
- [6] H. Kang, Digital Color Halftoning, Bellingham, WA: SPIE—The International Society for Optical Engineering, 1999.
- [7] Y. C. Hou, C. Y. Chang, and S. F. Tu, "Visual cryptography for color images based on halftone technology," in International Conference on Information Systems, Analysis and Synthesis. World Multiconference on Systemics, cybernetics and Informatics. Image, Acoustic, Speech And Signal Processing: Part II, 2001.
- [8] Mohd Junedul Haque, Sultan Aljahdali: An Approach for Reconstructed Color Image Segmentation using Edge Detection and Threshold Methods. International Journal Of Computer Applications 68(11): 32-36 (2013).