# Image Encryption Technique Based on Visual Cryptography

Mrunali T. Gedam
Assistant Professor, Information Technology, SRMCEW, Maharashtra, India
mrunaligedam40@gmail.com

**ABSTRACT**

*Visual Cryptography is a new Cryptography technique which is used to secure the images. In Visual Cryptography, the Image is divided into parts called shares and then they are distributed to the participants. The Decryption side just stacking the share images gets the original image. In this paper process on color image and convert into gray-scale images then divided it in to shares. Total number of shares to be created is depending on the (2, 2) scheme. Stacking shares produce binary image as a decoded image.*

**Keywords**

Image Security; secret sharing scheme; halftoning; visual cryptography VC

## 1. INTRODUCTION

Today, encryption is becoming very important in the present era in which information security. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images.

In VCS the secret image which to be shared secretly is divided into parts called shares. Dividing into parts exactly mean each and every pixel of the secret image is copied in to share images in a combination of m number of black and white pixel combinations. This is called dividing the image into parts to from share images and the process is called pixel expansion. Dividing/copying a pixel into share images as a combination of black and white pixels is called sharing a pixel.

The basic principles of Visual Cryptography, each pixel of secret binary image are cryptographically encoded into m black and white subpixel in each share. If secret image pixel is white, encode with a set of four subpixel each subpixel has equal probability it contains two of them white and two of them black, thus,

the subpixel set gives no clue as the original value of pixel. When a decrypted subpixel has two white and two black pixels indicate that the decoded pixel is a white. On the other hand a decrypted subpixel having four black pixels indicates that the decoded pixel is black.

The important parameters of VC scheme are:

a) Pixel expansion 'm', which refers to the number of pixels in a share used to encrypt a pixel of the secret image. This implies loss of resolution in the reconstructed image.

b) Contrast 'α', which is the relative difference between black and white pixels in the reconstructed image. This implies the quality of the reconstructed image.

Generally, smaller the value of m will reduce the loss in resolution and greater the value of 'α' will increase the quality of the reconstructed image. If 'm' is decreased, the qualities of the reconstructed image will be increased the two importance components are. 1. To have good quality reconstructed image. 2. To increase security with minimum pixel expansion.

## 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 halftoning 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. This method expand every pixel of a color secret image into a 2×2 block in the sharing images and keep two color and two transparent pixels in the block.

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. PRELIMINARIES

In this section, we give a brief description of VC, color models in VC.

### *3.1 Fundamentals of VC*

Visual cryptography scheme encrypts a secret message into shares to be distributed to participants. By stacking the sufficient numbers of shares reveal the secret image. A black and white (k,n) VC scheme consists of two collections of binary matrices and, having elements 0 for a black pixel and 1 for a white pixel. To encrypt a white (black) pixel, a user randomly chooses one of the matrices and distributes its rows to the participants.

### *3.2 Color Models*

The additive and subtractive color models are widely used to describe the constitutions of colors. In terms of RGB model, each color is mixed with red, green, and blue, which are the three primary colors of light. This model is commonly used for on-screen display. Therefore, RGB model is also called additive model. On the other hand, CMY model is called subtractive model. For CMY model, each color is mixed with cyan, magenta, and yellow, which are the three primary colors of pigments. This model is commonly used for color printing.

## 4. PROPOSED SYSTEM

The grayscale system consists of three main blocks as halftone, encryption, and decryption.

### *4.1 Halftone Conversion*

The general printer, such as dot matrix Printers, laser printers, and jet printers, can only control single pixel to be printed (black pixel) or not to be printed (white pixel), instead of displaying the gray level or the color tone of an image directly[1]. As such, the way to represent the gray level of images is to use the density of printed dots; Transform the continuous-tone

image into a binary image is called halftoning. The main idea of halftoning is to utilize the density of Printed dots to simulate the grey scale of pixels. For human eyes, the denser the dots are, the darker the image and sparser dots are lighter the image.

### *4.2 Encryption*

In encryption, transform gray-level images into halftone ones before printing, the transformed halftone images are black-and-white only, such an image format is very suitable for generating the shares of visual cryptography.

In grayscale system architecture, I have to first convert the original input image into grayscale and Transform the gray-level image into a black-and-white halftone image. For each black or white pixel in the halftone image, decompose it into a 2×2 block of the two transparencies according to the (2, 2) visual cryptography scheme. The basic assumption here is that the image is a collection of black and white pixels and each pixel is handled separately. Each original pixel appears in *n* modified versions, one for each share. Each share is a collection of *m* black and white sub-pixels that are printed in close proximity to each other so that the human visual system averages their individual black/white contributions. The input binary image has black and white pixels encoded with *m* sub-pixel called shares.

A visual cryptography scheme can then be constructed by encrypting shares in the following manner:

a) If the pixel of the original binary image is white (0), randomly encoded with four subpixel of Sw1 in share1 and Sw2 in share2. It is important to encode the patterns randomly in order to make the pattern random.

b) If the pixel of the original image is black (1), encoded with four subpixel of Sb1 in share1 and Sb2 in share2.

There are two matrices, one matrix for white pixel and one matrix for black pixel in input image as given below:

$$Sw1=\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \qquad Sw2=\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$Sb1=\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \qquad Sb2=\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

### *4.3 Description*

Decryption is just the reverse process of encryption. The aim of decryption is to make the encrypted information readable again (i.e. to make it unencrypted). In which I have to stack both shares of encryption. Decryption is a procedure of getting original image by stacking the transparencies using logical OR operation.

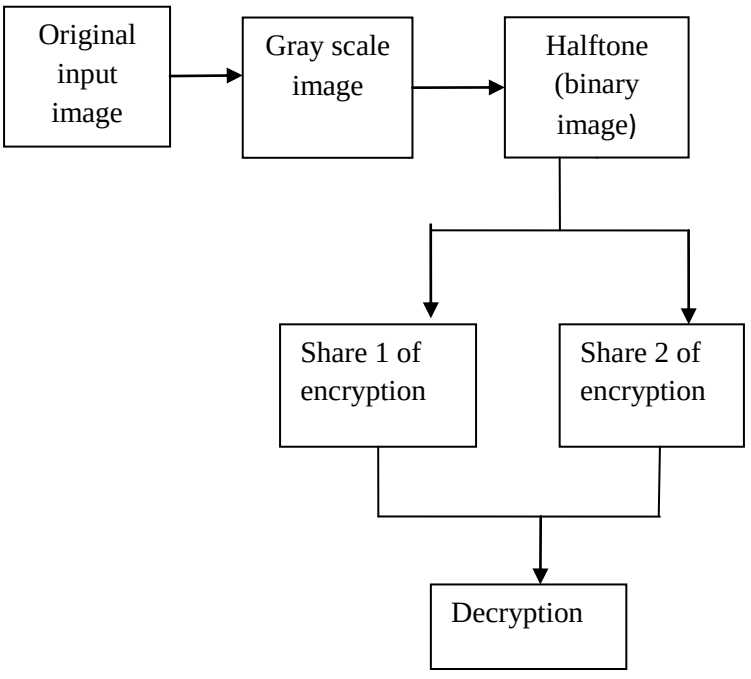


Fig.1 Block diagram of proposed system

## 5. SIMULATION RESULTS

In this section, we provide some experimental results to illustrate the effectiveness of the proposed method.

Fig 2: (a) original color image (b) Grayscale image

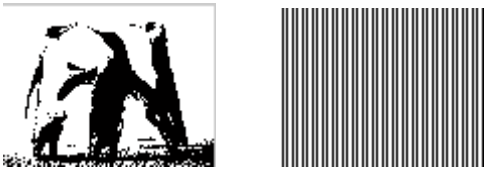

Fig 3**:** (a) Binary image (b) Share 1 of Encryption

Fig 4: (c) Share 2 of Encryption (d) Decoded image

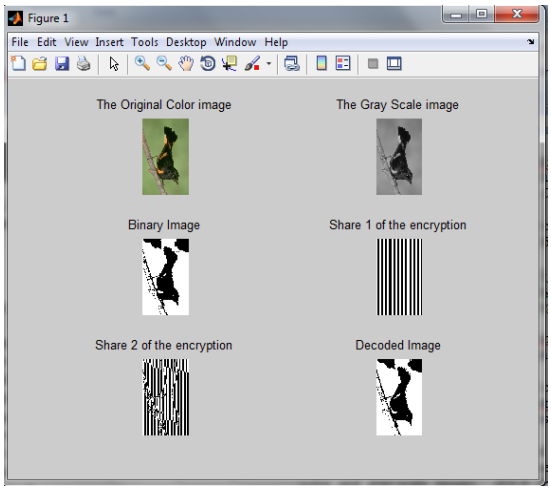


Fig 5. Resultant output image

## 6. CONCLUSION

Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement. In this paper we have process on color image to grayscale image and created the shares of binary image when we stack the share better quality decrypted image is obtained.

## 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. Multimedia Expo*, 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].

[13] H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images," *IEICE Trans. Fundamentals*, vol. E81-A, no. 6, pp. 1262–1269, Jun. 1998.