Visual Cryptography Schemes for Images

Ch.Karuna
Department of Electronics and Communication Engineering
KG Reddy College of Engineering & Technology, Moinabad, Telangana, India

Abstract- Image cryptography is emerging field of the research. As technology progresses and as more and more personal data is digitized; there is even more of an emphasis required on data security today than there has ever been. Protecting this data in a safe and secure way which does not impede the access of an authorized authority is an immensely difficult and very interesting problem. In this paper various Visual Cryptography (VC) techniques for data security method is presented. Visual cryptography provides a very powerful technique by which one secret can be distributed into two or more shares and decryption is done dome by human visual system.

Keywords – VC, Extended Visual Cryptography, Color Visual Cryptography, Progressive Visual Cryptography

I. INTRODUCTION

Visual Cryptography (VC) is a type of secret sharing scheme introduced by Naor and Shamir in 1994. Visual cryptography provides a very powerful technique by which one secret can be distributed into two or more shares. The secret image can be recovered simply by stacking the shares together without any complex computation involved. The shares are very safe because separately they reveal nothing about the secret image. These meaningful shares will not arouse the attention of hackers. Secret Hiding can be achieved in two ways: Cryptography and Steganography.

Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect e-mail messages, credit card information, corporate data, etc. More specifically, Steganography is the art and science of communicating in a way which hides the existence of the communication. A steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. On the other hand, cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

II.CRYPTOGRAPHY FOR IMAGES

Cryptography is not only used to send the text but it can be extended to images called Visual Cryptography where the image is stored in different shared images. When all the shares are stacked together then only the hidden image is received. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. Visual cryptography has two important features. The first feature is its perfect secrecy and the second is its decryption method which requires neither complex decryption algorithms nor the aid of computers. It uses only human visual system to identify the secret from the stacked image of some authorized set of shares. Therefore, visual cryptography is a very convenient. Listed below are the visual cryptography techniques for images.

A. TRADITIONAL VISUAL CRYPTOGRAPHY

In this method the encryption rules specify that a pixel is encoded into two sub pixels composing of one black and one white on each share. Consider the two out-of-two visual cryptography scheme where each pixel p of the Secret Image is encoded into a pair of sub pixels in each of the two shares. If p is white, one of the two columns tabulated under the white pixel in Fig.1 is selected. If p is black, one of the two columns tabulated under the black pixel is selected. Then, 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 with equal probabilities, independent of whether p is black or white, an individual share gives no clue as to the value of p. In addition, as each pixel is encrypted independently, no secret information can be gained by looking at groups of pixels in each share.

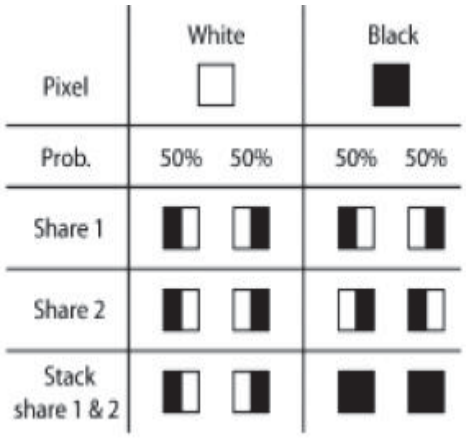


Fig.1: Construction of a two-out-of-two VC scheme

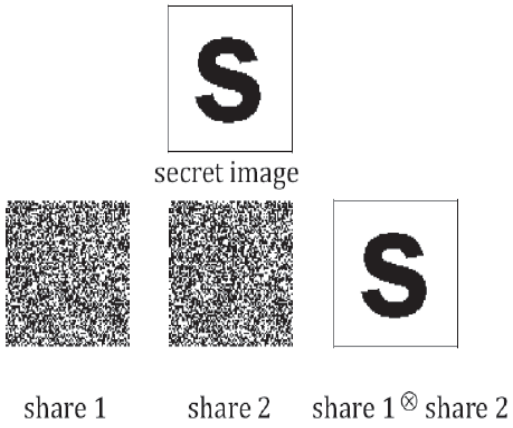


Fig.2. Encryption & Decryption of Binary Image

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. A binary image can be divided into shares which can be stacked together to approximately recover the original image.

B. EXTENDED VISUAL CRYPTOGRAPHY

Extended Visual Cryptography is a kind of visual cryptography scheme in which meaningful shares are stacked together to reconstruct the original image. Extended VC generally, a (k,n)-EVC scheme takes a secret image and n original images as input and produces n encrypted shares with approximation of original images that satisfy the following three conditions:

- any k out of n shares can recover the secret image;
- any less than k shares cannot obtain any information of the secret image;
- all the shares are meaningful images; encrypted shares and the recovered secret image are colored.

Denote S_c c_1, c_2 ,…c_n as the collection of matrices from which the dealer chooses a matrix to encrypt, where c_1,…c_n € {0,1} . For i=1,…n,c_i , is the bit of the pixel on the i^{th} original image and c is the bit of the secret message. For a black and white (k,n)-EVC scheme, we have to construct 2n pairs of such collection , one for each possible combination of white and black pixels in the original images. Here we give a definition of the black and white EVC scheme.

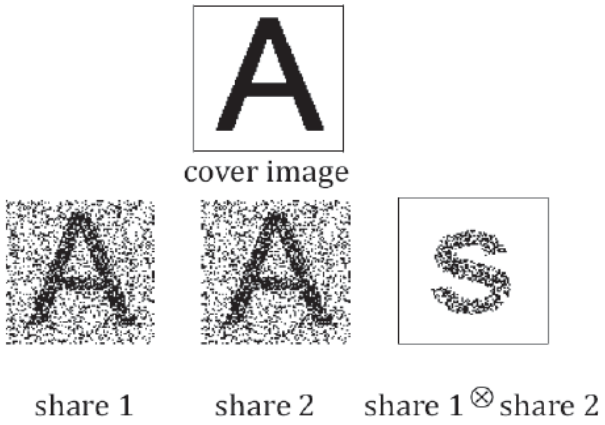


Fig.3. Encryption and Decryption using EVC

C. COLOR VISUAL CRYPTOGRAPHY

The steps to be followed for encryption and decryption of color images is as follows:

(1) Color Halftone Transformation: In this method, each input image is decomposed into three constituent planes red, green and blue. The principle of halftoning is applied to each of these planes. A color halftone image is generated by combining these three half-toned planes. Half-toning is performed using error diffusion. The error diffusion algorithm uses Jarvis filter. As per the Jarvis error diffusion algorithm, the error is diffused in the 12 neighboring cells. Visual quality of the half-toned image is higher when Jarvis algorithm is used.

(2) Encryption Process: To encode secret pixels, the secret information pixels are distributed as homogeneously as possible. In each cover image 4096 secret image pixels can be hidden. VIPs are pixels on the encrypted shares that have color values of the original images. This algorithm generates a set of random binary matrices S_0 and S_1 which are of size of cover image. In this method, secret pixels are hidden using ex-or operation. x(p,q) represents the secret image pixel. for the color channel C of the secret message

- x(p,q) do for p = 1:n:256
- for q = 1:m:256
  - (a): if the bit x(p,q,c)==0 then share_img(p,q,c) = xor (S_0(p,q), x(p,q,c))
  - (b): if the bit x(p,q,c)==1 then share_img(p,q,c) = xor (S_1(p,q), x (p,q,c))
- Repeat above process for color channel G and B
- Repeat above process for all cover images.

(3) Decryption Process: At the receiver side all the shares are collected and using the VC matrices S0, S1 the information is extracted from the meaningful shares and thus forms the reconstructed secret image. i and j represents rows and columns of the share images. n and m represents after how many rows and columns a secret image pixel should be extracted from share images and the value is same as in encryption process. If the share image value is equal to S0 matrix value at position (i , j) then perform ex-or operation of the share image and S0 matrix value else perform ex-or of the share image and S1 matrix and place it in a variable. Perform same process for all color channels and all the share images.

- for the color channel C of the share image
- for i=1:n:256
- for j=1:m:256
  - a) if share_img(i,j,c) == S0(i,j) then si_img= xor(share_img(i,j,c) , S0(i,j)
  - b) else si_img= xor(share_img(i,j,c) , S1(i,j))
- Repeat above process for channel G and B
- Repeat above process for all share images.

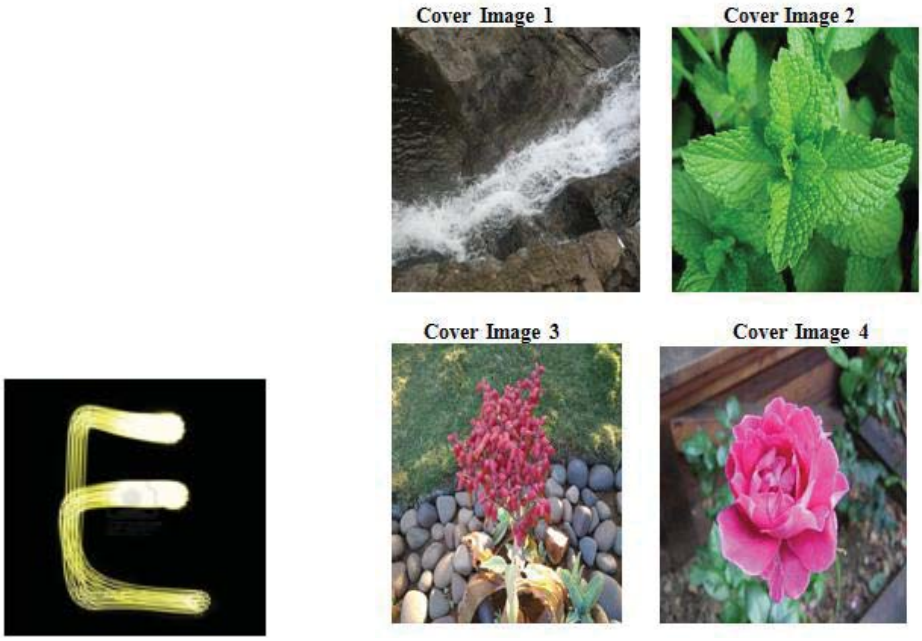


Fig.4. Secret Image

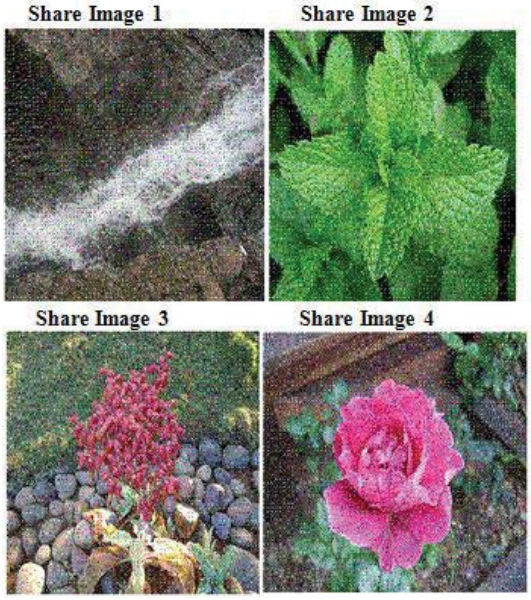


Fig.5. Share Images after halftoning and Encryption Process

Fig.6. Decrypted Image

D. PROGRESSIVE VISUAL CRYPTOGRAPHY

Progressive Visual Cryptography (PVC) scheme differs from the traditional VC with respect to decoding. In PVC, clarity and contrast of the decoded secret image will be increased progressively with the number of stacked shares. Progressive visual cryptography with unexpanded shares solves the main problems such as the leak of secret information, pixel expansion, and bad quality of recovered images and also deals with the color image. This scheme consists of following steps: At the encryption stage:

1) Chromatic image is decomposed into three monochromatic images in tones of red, blue and green.
2) These three images are transformed into binary images by halftoning technique.
3) Creating the sharing images.
4) Cover images are superimposed on the shares. B.

At the decryption stage:

1) Original shares are extracted from the meaningful shares.
2) These shares are split up into three color channels.
3) Combining the same color channels to obtain gray scale images of red, blue and green.
4) Gray scale images of three channels are combined to get the colored secret image.

The algorithm for creating shares is explained below and then, we can choose any three different colors of which to compose them into n colored shares.

Algorithm:

Input: A W × H halftone secret image P where p (i, j) ϵ P

Output: n shares , m=1, 2, …. ,and n

Process:

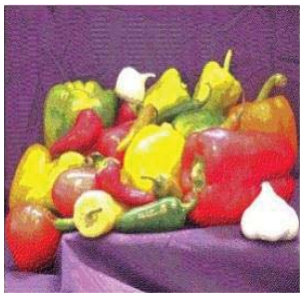
1) Generate sharing matrices ,C^0 and C^1
2) For each pixel p (i, j),
3) Randomly choose a value l, range from 1 to n
4) For m=1, 2, and n

4.1) If the pixel p (i, j) = 0 (white), the pixel value S^m (i,j) =C^0(l, m)

4.2) If the pixel p (i, j) = 1 (black), the pixel value S^m (i,j) = C^1 (l, m)

In the decryption phase, original shares are extracted from the meaningful shares. For each of the watermarked shares, extract the height and width values of secret image from the watermarked share pixels. For each watermarked share pixel, if the LSB of pixel is 0, set secret share pixel at 0; else as 1, likewise we get the entire black and white secret image shares. This procedure is to be carried out for each of the color channels. Then these shares are split up into three color channels and then combining the same color channels to obtain gray scale images of red, blue and green progressively.

Fig.7.Secret Image



Halftone Secret Image

Watermarking Algorithm:

Input: n secret image shares, n cover images

Output: n watermarked shares

Process: 1. Do for each secret image share

a. Read respective cover image

b. Do for each pixel

i. If share pixel is black

i.a. Set LSB of cover image pixel to 1

ii. If share pixel is white

ii.a. Set LSB of cover image pixel to 0


Fig.8.Watermarked Images

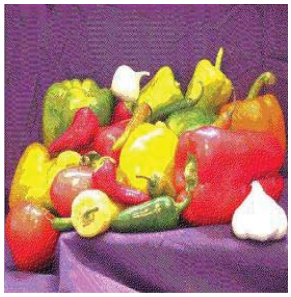


Fig.9. Decrypted Image

III. ANALYSIS OF DIFFERENT TYPES OF VISUAL CRYPTOGRAPHY

1. Traditional Visual Cryptography: The disadvantage of the above schemes is that only one set of confidential messages can be embedded, so to share large amounts of confidential messages several shares have to be generated. This process results in pixel expansion and the shares resemble random noise. Pixel expansion m refers to the number of subpixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one. This method is not applicable to color images.
2. Extended Visual Cryptography: In the above method shares resemble random noise which creates a doubt among hackers. This disadvantage is overcome by extended visual cryptography since the shares are meaningful. The reconstructed original image losses its contrast. This method is applicable to grayscale and color images.
3. Color Visual Cryptography: There are many halftone techniques for color images but error diffusion method of halftone is used to improve the quality of image. In this algorithm the shares are meaningful and reconstructs image which losses its contrast.
4. Progressive Visual Cryptography: This method is applicable for color images without any pixel expansion based on the halftoning technique. PVC is a special encryption technique which can be utilized to recover the secret image gradually by superimposing more and more shares. If we only have a few pieces of shares, we could get an outline of the secret image; by increasing the number of shares being stacked, the details of the hidden information can be revealed progressively. The decrypted image resembles original secret image.

III.CONCLUSION

Visual Cryptography provides one of the secure ways to transfer images on the Internet. Visual Cryptography allows easy decoding of the secret image by a simple stacking of the printed share transparencies. The developments and proposals by different authors in visual cryptography schemes are reviewed here. The different perspectives on visual cryptography such as types of access structures, types of shares, and color models of secret images etc. are discussed. It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share; however, the color secret image can be recognized in even low contrast levels.

REFERENCES

[1] 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.

[2] M. Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT*, 1994, pp. 1–12.

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

[4] Zhongmin Wang and Gonzalo R. Arce," Halftone visual cryptography through error diffusion".

[5] Anantha Kumar kondra, Smt. U.V. Ratna Kumari, Firoj Hussain Shaik, " Colour Image Visual Cryptography using Error Diffusion", IJAIR, Vol.1, Issue 2,July 2012.

[6] Z. M. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics, Security, Vol. 4, No. 3, pp. 383–396, Sep. 2009.

[7] Fersna , Athira V, "Progressive visual cryptography scheme without pixel expansion for color images",IJARCCE, Vol. 4, Issue 6, June 2015.