International Journal of
Science Inventions Today
www.ijsit.com
ISSN 2319-5436
Research Article

# VISUAL CRYPTOGRAPHY SCHEME BASED ON PIXEL EXPANSION FOR BLACK & WHITE IMAGE

LEKHIKA CHETTRI

*Dept of Computer Application, Sikkim University, India*

## ABSTRACT

This paper explains the 2 out of 2 visual cryptography schemes based on pixel expansion m=2 in detail. Visual cryptography enables the secure transmission of images in open and insecure media. The scheme explained in this paper is based on k out of k visual cryptography scheme. To prevent the discloser of the secret by forming copy of the first share randomization of sub pixel is performed on the shares. One single share cannot disclose the secret. To extract the secret message both the shares are needed to superimpose one on another. We provide (2, 2) Visual Cryptography (VC) in detail for black and white image based on pixel expansion scheme.

**Keywords:** Pixel, Secret message, visual cryptography, share image, constructed image.

## INTRODUCTION

With the advancement of global computing network in the name of INTERNET and World Wide Web, facilitating sharing plethora of information over the network, the cases of pilferage of information by the undesired recipient have also increased many folds. To prevent pilferage and hacking of information over such communication networks, the researchers have proposed and implemented varieties of security models. The various text security models or algorithms for key exchange to establish a secure communication have been in use since decade. DiffieHellman(D-H) algorithm, introduced by Diffie and Hellman in RS laboratory is based on the Discrete logarithmic mathematic calculation and thus is traceable only in the case when solution to discrete logarithmic mathematics available. D-H suffers from man in the middle attack with heavy pilferage of information. The algorithm has found its application in various visual cryptography field such as in military, museum image security etc. Likewise RSA, Asymmetric Encryption System, Data Encryption Standard(DES), Triple Data Encryption Standard(3DES) All these algorithms hold lot of encryption and decryption computation. The time complexity in the decryption side is also comparatively high. Decryption of messages using these algorithms is possible only with ample of computational knowledge. Decryption of the Secret using the mentioned algorithm is possible to only those who have the respective algorithmic knowledge. In the scenario where computational decryption or decryption using devices are not favorable to the situation or environment, it is to be carried by human visual system, a more systematic and organized schemes of decryption was required that lead to the birth of various visual cryptographic schemes.

The first Visual cryptography scheme was proposed by Adi and Shamir in the year 1996[2]. According to the research the encryption of pictures or text was possible in the form of images. Applying the scheme proposed by them the encryption of any textual or pictorial information are to be done at the pixel level. Encryption performed in the pixel level was explained based on pixel expansion scheme. The decryption is possible through human visual system without any mathematical computation but just by overlaying the shares [2]. The encrypted images in the form of shares are only collection of random noise until all the shares are overlaid. Based on this scheme various other schemes were proposed with improved features..VC for black and white images encrypt images considering images of binary number i.e either 1 or 0. The VC scheme sets value 0 for a white pixel and 1 for a black pixel.

In this paper we explain Visual Cryptography Scheme based on two by two for pixel expansion with m=2 for black and white images. The original image is taken in the form of binary images, 1 for a black pixel and 0 for a white pixel. A single pixel from the original image is sub divided into two sub pixels in the share image. Thus exchanging of such shares even over a vulnerable network does not suffer from secret violation nor suffers from decryption overhead due to heavy mathematical decryption process. Visual cryptography provides the simplicity of decryption and lesser complex method of secret sharing.

## Methodology:

Visual cryptography is one of the new cryptographic techniques used for encrypting pictures, text and different information. The encryption of text or images is done in such a way that decryption can be performed by the human visual system without usage of computer systems [1][3]. Visual Cryptography refers to a secret sharing method that will encrypt the secret message into a number of shares and does not require any computer or calculations for decrypting the secret image rather the secret message will be reconstructed visually by overlaying the encrypted shares. In visual cryptography pixel expansion scheme each pixel is divided into white and black blocks. It a technique to hide information in such a way that if some1 else's gets the hold of a share the intruder cannot break the code.

In k out of k visual cryptography scheme all the k numbers of shares are needed to decode the image while in k out of n threshold visual cryptography scheme only k numbers of shares are needed to decode the image. The decryption needs no prior and no expert knowledge on cryptography. In order to decode the encoded secret message all the k numbers of shares are overlapped one above another [2]. In (2, 2) VCS each pixel is divided into two sub pixels. For a single pixel in the secret message both the shares will have two sub-pixels each. By insufficient number of shares, even a strong cryptanalyst cannot disclose any information and decide whether the shared pixel is a white or a black pixel.

## Basic Model of Visual Cryptography:

Each pixel of image 'I' is represented by 'm' ( m = 2) sub pixels in each of the 'n' (n=2 in our case) shared images. The resulting structure of each shared image is described by Boolean matrix 'S', where S=[Sij] an [n x m] ([2 X 2] )matrix Sij=1 if the jth sub pixel in the ith share is black Sij=0 if the jth sub pixel in the ith share is white.

When the shares are stacked together secret image can be seen but the size is increased by 'm' times. The grey level of each pixel in the reconstructed image is proportional to the hamming weight H(V) of the OR – ed Vector 'V', where vector 'V' is the stacked sub pixels for each original pixel [5]. The black pixel matrix is represented by C0 so to encrypt a black pixel randomly select one of the matrices from C0 and the white pixel matrix is represented by C1 so to encrypt a white pixel randomly select one of the matrices from C1 where

C0 = {all the matrices obtained by permuting the columns of [1 0; 1 0]}
C1 = {all the matrices obtained by permuting the columns of [1 0; 0 1]}

The difference in the image contrast of the original secret image and the secret image enhanced after overlapping of the shares is given by 'α' which is the relative difference in the white and black pixel of the reconstructed image.

## Development of two-by-two Visual Cryptography Scheme with Pixel Expansion:

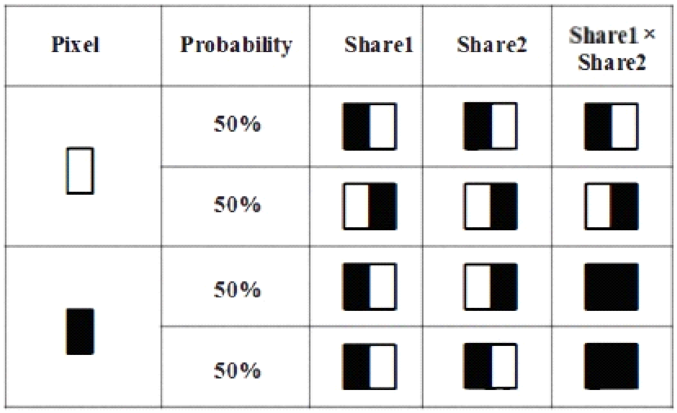
In this approach we use visual cryptography scheme based on pixel expansion. For an image 'I' the secret image will be encoded as a binary string, where 0 represents a white pixel and 1 represents a black pixel. Each pixel from the secret message (Message to be encrypted) is sub divided into more than one pixel i.e. two to represent the pixel of the secret message i.e. each single pixel from the secret image is greater than one.

i.e.Pixels in generated shares > pixels in original image

- No. of columns in constructed image = 2 * no. of columns in original image
- Size of the Constructed image = 2 * Size of Original secret image

This explains the increase in pixels in (2, 2) VCS for pixel expansion m=2 i.e. two sub pixel for each pixel in the secret message.

Every single pixel in the secret image is encrypted using random selection of the possible permutation for all the sub pixel combinations. Thus there is no possible chance to gain any information by looking at a single share1 or share 2. When we stack both the shares there is a loss of 50% contrast in the overlaid image as compare to the original image. This is because of the fact that for a black pixel in the original secret image we get two black sub pixels and for a white pixel we get one black sub pixel and a white sub pixel i.e. we have a grey level of 1 if the pixel is black and a grey level of ½ if the pixel is white. Though there is a loss of 50% contrast in the constructed image the secret message is clearly visible. To maintain clarity and avoid image distortion aspect ratio of the pixels to the sub pixels has to be maintained.



| Pixel | Probability | Share1 | Share2 | Share1 × Share2 |
|---|---|---|---|---|
| □ | 50% | ◧ | ◧ | ◧ |
| | 50% | ◨ | ◨ | ◨ |
| ■ | 50% | ◧ | ◨ | ■ |
| | 50% | ◧ | ◧ | ■ |

**Figure 1**

To represent a white pixel of the secret message one of the two rows under white pixel is selected from fig1 and for a black pixel one of the two rows under black pixel is selected from Fig 1 [3] i.e. a white pixel is shared into two identical blocks of sub-pixels. A black pixel shared into two complementary blocks of sub-pixels. Permutation of the pixel combination is performed such that no information can be reconstructed from any single share. The selection of the permutation combination is based on random selection of the pixel pairs. The random selection of the pixel pair combination prevents shares constructions based on the previously generated shares.

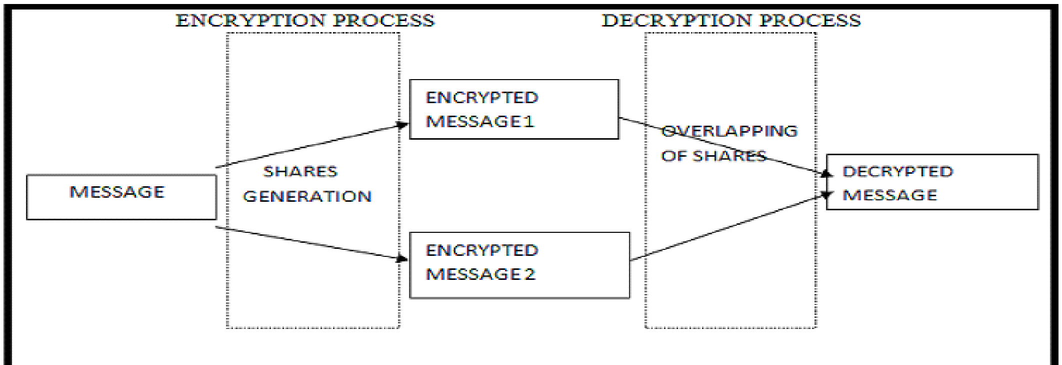


Fig 2: Visual Cryptography Layout

## FACTORS EFFECTING IMAGE QUALITY IN VCS:

'm' – Higher the value of ' m' higher is the loss in resolution. Thus to decrease loss in image resolution decrease the number of' m'.

'α'- Greater is the image resolution greater is the image resolution. Thus the higher relative difference gives greater quality resolution.

'k out of n' - In "k out of n"Visual Cryptography scheme more is the number of k more clear is the reconstructed image, lesser is the number of k higher is the resolution loss.

'Aspect ratio' - number of pixel expansion should also be considered to avoid image distortion [2].

## WORKING ENVIROMENT:

## MATLAB:

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the   time.

## IMAGE ENCODING AND DECODING:

Take a black and white text image as an input to encode. In case of a color image binaries it to get a binary image. A black pixel is represented by 1 and a white pixel by 0. For a better result in case of text images make use of larger size fonts. Encode the text image, encoding each black and white pixel. For each black pixel (1) in the secret image replace it by two sub pixels, for black pixel the sub pixels distribution will be different in one shares different in other i.e. either [1 0] in sahre1 and [0 1] in share2 or by randomly permuting it i.e. [0 1] for share1 and [1 0] for share2.

In case of white pixel (0) in the secret image pixel the sub pixels distribution will be same in both the shares i.e. either [1 0] in sahre1 and [1 0] in share2 or by randomly permuting it to [0 1] for share1 and [0 1] for share 2. The white pixel in the secret image is replaced by a half white and a half black sub pixels making a 100% pure white pixel a 50% white pixel i.e. half black and half white. Thus a white pixel in the secret image becomes a gray pixel in the final overlapped image. This is the reason the reconstructed image loses its contrast as compare to the original image. To decode the image, stack both the shares and the secret message will be reconstructed.

Randomization in MATLAB can be done by

```
ran = randint;     %generates a random scalar either 0 or 1 with equal probability

if(ran==1)
        share1=
        share2=
             .
             .
    Else                    % if ran==0
        share1=
        share2=
             .
             .
end
```

The share combination to encode a 2 out of 2 scheme is -

Prepare matrix based on black or white

```
 s0 = [ 1 0 ; 0 1 ];
 s00= [ 0 1 ; 1 0 ];
```

```
s1 = [ 1 0 ; 1 0 ];
s11 =[ 0 1 ; 0 1 ];
```

## STEPS INVOLVED IN VISUAL CRYPTOGRAPHY SCHEME:

- Start
- Take any secret message (text, picture etc.) in image format.
- Perform visual cryptography encryption technique,
- Perform Pixel expansion
- Generate shares,
- Save all the generated shares,
- Stack all or the defined number of shares.
- Stop.

## EXPERIMENT RESULT

Our experimental result is based on the (2, 2) visual cryptography scheme for m=2. In this scheme the original image is in binary form, provided imagecan be of any size and any format.

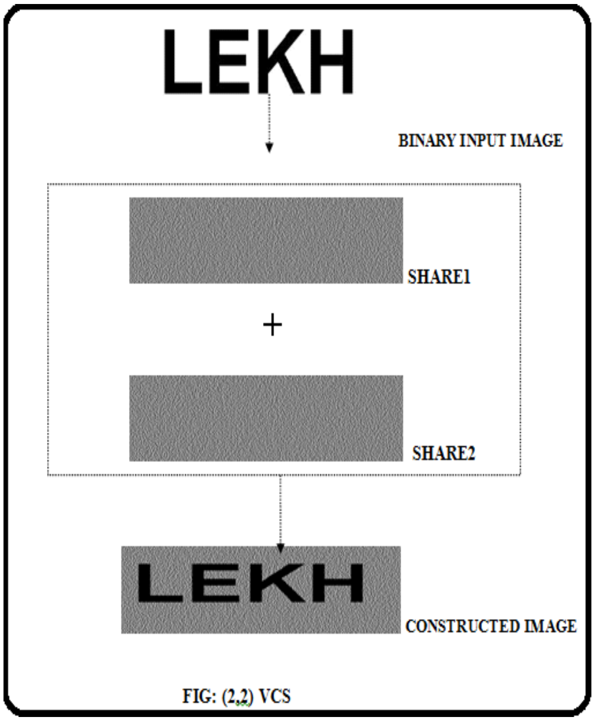


FIG: (2,2) VCS

The contrast of the constructed image from the above figure can further be improved .The contrast can be improved in the above experimental result by setting m= 4 instead for m=2 which maintains the aspect ratio of the sub pixels to its respective pixel.

For (2, 2) with m=4 we can have the sub pixels combination for a white and a black pixel as shown in the figure below. This maintains the aspect ratio of the pixel to its sub pixel and thus enhances the image quality. To improve the constructed image quality we have to maintain the aspect ratio of the pixel to its sub pixels.

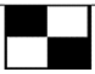
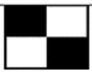
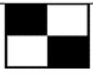
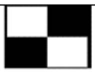
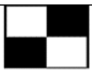
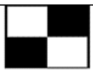
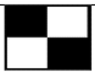
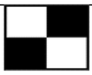
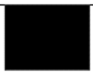
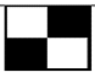
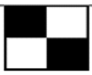
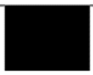
| Original Pixel | Probability | Share 1 Sub-Pixel | Share 2 Sub-Pixel | Share 1 \|\| Share 2 |
|---|---|---|---|---|
| □ | 0.5 |  |  |  |
| □ | 0.5 |  |  |  |
| ■ | 0.5 |  |  |  |
| ■ | 0.5 |  |  |  |

Fig 3: Pixel combination for (2, 2) VCS for m=4

## CONCLUSION

This paper explains the (2, 2) visual cryptography scheme with pixel expansion for black and white image. From the experimental result it is clear that the reconstructed image loses some contrast as compare to the original secret message. It is not wrong to tell that no information can be constructed from a single share. The method enables a tight security to the secret message. In order to increase the contrast the aspect ratio has to be maintained. The procedure can further be extended for higher "k out of k" Visual cryptography scheme.

## REFERENCES

1. S. Cimato, R. De Prisco, and A. De Santis, 'Probabilistic visual cryptography schemes'. The Computer Journal, 49(1):97{107, December 2005.
2. M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYFT'94, LNCS, vol. 950, pp. 1-12,1995.
3. Sokratis K. Katsikas (2006), "Information security", 9th international conference, Springer Publications, pp. 548.
4. John Blesswin, Rema, Jenifer Josel, " Recovering Secret Image in Visual Cryptography", Karunya University,538

5. Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S., “An overview of visual cryptography” , Volume 1, Issue 1, 2010, PP-32 37.