VISUAL CRYPTOGRAPHY SCHEME FOR COLOUR IMAGES BASED ON MEANINGFUL SHARES

Karthik K

M.Tech in CSE (PT)
NMAMIT, NITTE – 574110

Sudeepa K B

Associate Professor, Dept of CSE
NMAMIT, NITTE - 574110

***ABSTRACT* - A region based visual cryptography scheme deals with sharing of image based upon splitting the image into various regions. The main concept of visual secret sharing scheme is to encrypt a secret image into n meaningless share images. It cannot leak any information about the original image unless all the shares are obtained. The original image is obtained by superimposing all the shares directly. In this paper we propose a region based visual secret sharing scheme for color images with no pixel expansion and high security.Visual Cryptography is a special technique which is used to send the images securely over the network. Simple Visual Cryptographic technique is insecure. This cryptographic technique involves dividing the secret image into n shares and a certain number of shares (m) are sent over the network. The decryption process involves stacking of the shares to get the secret image. In the current work, we have proposed a cryptographic technique for color images with encryption and decryption model. The shares are developed using XOR operation. The key generated for decryption process is sent securely over the network. This approach produces less distorted image and the size of the decrypted images is same as the original image.**

Keywords: Visual cryptography, visual secret sharing, Pixel expansion, Human visual system.

1. INTRODUCTION

In this Era, where sharing of information have become indispensable and is part of most of the activities being performed on internet. With the growth of Internet the need for secure sharing of images has become extremely important. There are basically two important components in cryptography, data hiding and secure transfer of data. Visual Cryptography is an emerging scheme which is proving to be efficient for both issues of secure image sharing. This technique is based on Human Visual System and hence do not include complex mathematical computations. The basic model of visual cryptography was given by Naor and Shamir for Binary images. In this scheme the secret image is divided into n number of shares out of which the number of shares (m) is sent over the network to the required destination, any m-1 number of shares will not be able to reveal the secret image. Pixel is the smallest unit of an image. Here a 256-bit pixel of a digital image is taken and is divided into Red, Green and Blue.

Visual Cryptography is the scheme which encrypts image using cryptographic technique, but decrypt original image without any cryptographic computation. This scheme is secure and easy to implement. The cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Visual Cryptography is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Visual Secret Sharing (VSS), one of the secret communication technologies, aims to share a secret image with several participants by a dealer. VSS is a precise technique that encodes a secret image into noise-like sharing images and reconstructs the original secret by superimposing all of the qualified shared images.

Firstly an image and key is fed into cryptosystem. The encryption algorithm produces a cipher image which is sent into receiver through a communication channel. When the cipher image reaches the destination, the receiver enters the key and the original image is decrypted. Figure 1 shows the block diagram of the cryptosystem. The key we used is the symmetric key same as the size of input image. Important factor used to determine the efficiency of any cryptographic scheme is:

- The quality of the reconstructed image

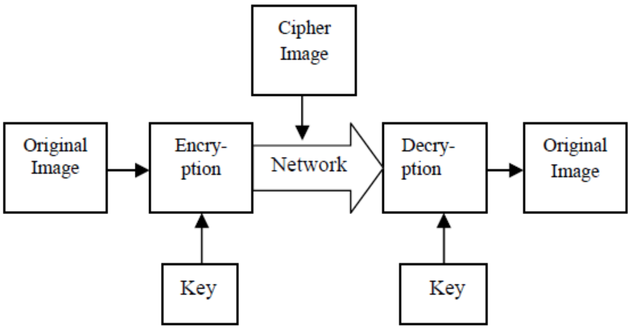


Figure 1: block diagram of cryptosystem

Any loss of information during the reconstruction phase leads to reduction in the quality of the recovered image.

2. LITERATURE SURVEY

Visual cryptography, introduced by Noar and Shamir [5], is a type of secret sharing techniques for images. The idea of visual cryptography scheme is to split an image into collection of shares which separately reveals no information about the original secret image. The image is composed of black and white pixels, and can be recovered by superimposing all the shares without any computations involved. By applying the Noar and Shamir 2-out-of-2 visual cryptography algorithm, two shares are created, which separately reveals no information about the original secret image. It can only be recovered when both of the shares are obtained and superimposed. Note that the size of the image is expanded by the factor of 4.

According to [5] leaking no information about the original secret image means that from any given share of the secret image, an unbounded adversary which has unlimited computational power should not be able to gain any information about the secret image other than the size of it. In practice, a visual cryptography scheme is considered *insecure* if the shape pattern or color of just a portion of the secret image can be recovered efficiently from any given share. This technique can be extended to n-out-of-n visual cryptography scheme. This technique makes use of the human visual system to perform the OR logical operation on the superimposed pixel of the shares. For example, the two blocks of 2x2 pixels shown on the Fig. 2.1. Will be viewed as the two black pixels and the two white pixels in each pixel block are averaged out. Now if we print these two pixel block separately onto a transparencies and superimpose them, the result is shown on the Fig. 2.1. This effect is equivalent to performing a pixel-wise OR logical operation on each of the four pairs of pixels between these two transparencies. One of the unique and desirable properties of a visual cryptography scheme is that the secret recovery process can easily be carried out by superimposing a number of shares.

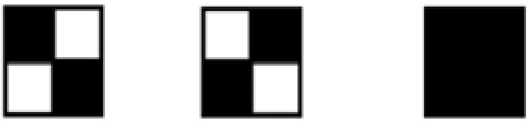


Figure 2.1: 2x2 pixel blocks and there superimposition.

In Tsung-lieh [7] et.al proposed a secret sharing scheme which is described for binary image, with no pixel expansion. This scheme adopted two rectangular share images to share two rectangular secret images. The rotation degree was 180 for revealing the second secret image. In this scheme the encryption process include three stages:

- DSP (dividing and separating process)
- SP (sticking process)
- CMP (camouflaging)

In DSP , the first function is to divide each secret image into blocks with n x n size, and the second function was to separate each block of the secret image into two subsets obtained by DSP to generate the share images, and two subsets of secret image were stuck to obtain both the share image respectively. The first subset of secret image 2 was directly stuck on the corresponding position of secret image 1. While the second subset of secret image 2 is rotated 180 degree and stuck to the corresponding position of share 2. The function of the CMP (camouflage) is to make the density of the black pixel on each block of one share image to be equal by referencing the maximum block density of all blocks. An example for the decryption process of the secret image is shown in Fig. 2.2. The first secret image was revealed by directly stacking share of secret image1 and the share of secret image 2. To reveal the second secret image, share image of secret image 1 was stacked with the share image of secret image 2 by rotating it to 180 degree. Though the scheme has no pixel expansion it still faces the problems like time complexity that it takes long time and low contrast of image.

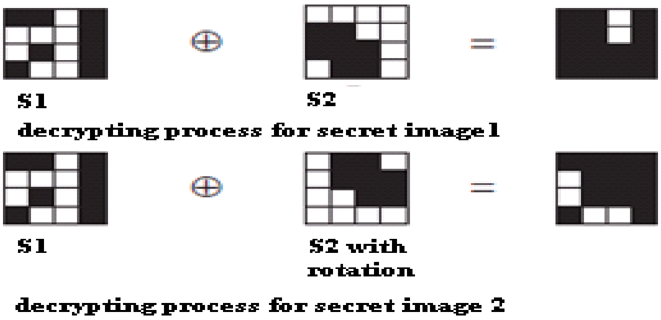

⊕
=
S1
S2
decrypting process for secret image1
⊕
=
S1
S2 with rotation
decrypting process for secret image 2

Figure 2.2: The decryption process

Besides the work on black and white images, a natural extension for this research problem is to perform secret sharing on color images. In [2] Bert W. Leung, Felix Y. Ng, and Duncan s. wong proposed three visual cryptography scheme for color images which have been dithered on each of the three primitive colors, namely cyan, magenta and yellow. They conducted a security analysis with two level security features. They found that the security of the scheme depend crucially on the color composition of the original secret image. They showed that this scheme support two level security control only if the original secret image contains only two color chosen from the specific set of colors. If the original secret image contains any other colors, they found that the adversary will have a high chance of compromising the scheme. Therefore they showed an attacking technique for this scheme. An attacking technique is shown below from which the attacker will not be able to compromise the secret if the original secret image contains only one of the following pair of colors:

{White, Black}

{Cyan + Magenta, yellow}

{Cyan + Yellow, Magenta}

{Magenta + Yellow, Cyan}

In this paper, we proposed a Region Based Visual Cryptography Scheme for Color Images, in which the image is divided into various regions like background and one or more foreground objects. And for each region then encryption operations are performed to obtain n shares. The decryption process is performed with human visual system which does not require any complex computation.

3. THE PROPOSED SCHEME

The image that carries secret information is converted into multiple secret shares using encryption model and the original image is obtained from the shares by decryption model. Both models use secret keys to increase security. The Specialty of this scheme is to generate any number of shares and to maintain the visual quality of the image.

A. The Encryption Model

Shares are obtained from the original secret image by using the generalized format as explained in the encryption model. The encryption model comprises of first finding the number of shares (n) to be generated. The user can give any value for n. Before separating the shares, the basic matrices are first constructed based upon the number of shares to be created. A random Key is generated at the encryption side based on block size n x n. Usually the block size will be 4 x 4 or 8 x 8.

1. Construction of Basic Matrices

The original image A is the input; If we want to create 2^b number of shares then b number of basic matrices are constructed, where b >= 2. The basic matrices are obtained by dividing each and every pixel value in A by b. For example, let the pixel value in A is 127, b is 3. 127/3 = 42.33. So the corresponding pixel value in the first and second basic matrix is 42 and the third basic matrix is 43. Therefore 42+42+43 = 127. If b = 3 then the number of shares to be produced are $2^3 = 8$. The shares can be constructed by XOR-ing basic matrices on different combination.

Algorithm1: Encryption model

Input: The original image A, Secret Key K.

Output: Shares S_1, S_2....S_n

```
    1. Construct basic matrices B1', B2', Bb'
    2. If the shares are 4
Perform B1 = 128 - B1', B2 = B2'

       If the shares are 8,

Perform B1 = 128 - B1', B2 = B2', B3 = 64 – B3'

If the shares increase, the alternative basic matrices will be subtracted correspondingly by 128, 64, 32… so on.

    3. Divide the basic matrices into blocks.
     For each block do the following to create shares

S1 = B1XOR K            S2 = B1 XOR B2

S3 = B2 XOR S1          S4 = S1 XOR S2

S5 = S2 XOR S3          S6 = S3 XOR S4

………………..            Sn= Sn-3 XOR A

    4. Combine the blocks of each share.

    5. Encode the shares and transmit.
```

The original image A and the secret key K is read from the user. Column permutation can be performed on the original image before basic matrices are constructed to increase security. The basic matrices are constructed as in step 2 in Algorithm 1. The necessary basic matrices are constructed based on the number of shares to be produced. Shares are generated by using the step 4 in Algorithm 1. The key K is XORed with the first share. All the shares are encoded and transmitted. The Block diagram of the proposed scheme is shown in Fig. 3.1.

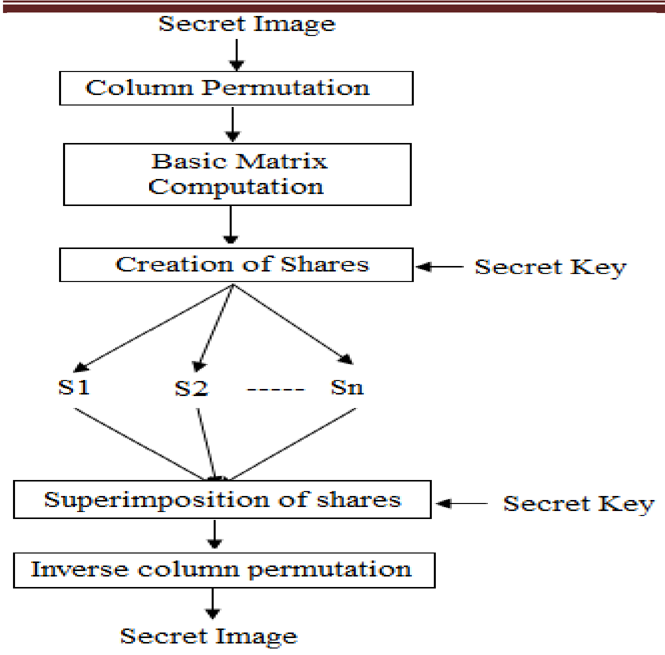


Figure 3.1: Block diagram of proposed scheme

B. The Decryption Model

Once all the shares are received at the receiver end, the shares are superimposed (XORed) in order to get the original image. The secret key K also XORed with shares.

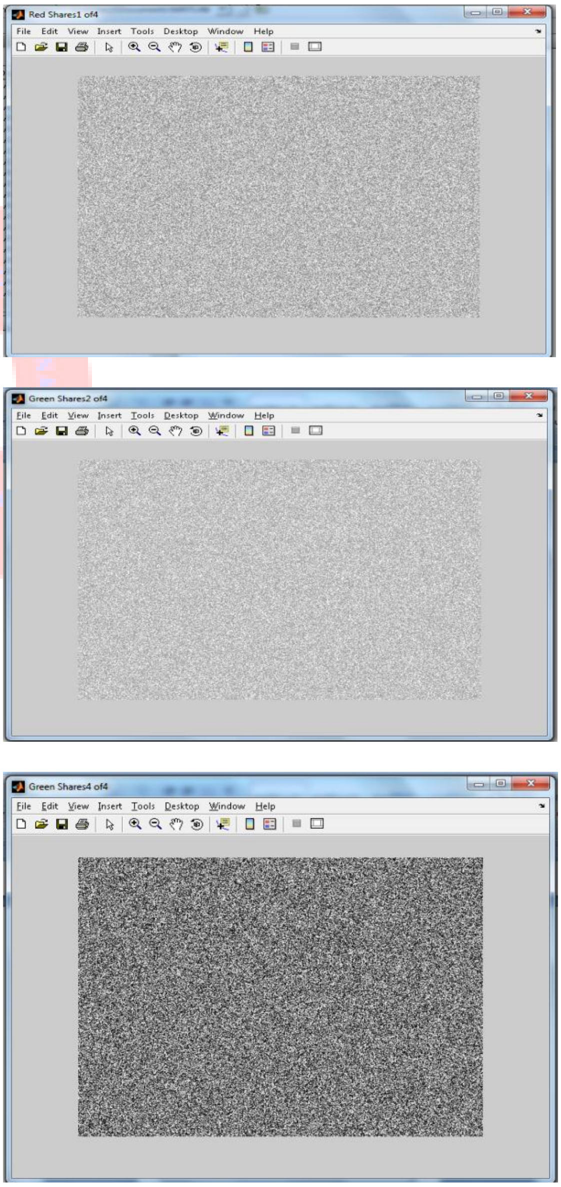
$$D = S1 \text{ XOR } S2 \text{ XOR } S3 \ldots \text{ XOR } Sn \text{ XOR } K$$

The decrypted image D has same visual quality as original image A in the sender side. If the receiver has all the shares and key then only he can decrypt. Otherwise he can't get any details about original image.

4. EXPERIMENTAL RESULTS

A good visual secret sharing scheme must have lower pixel expansion and higher contrast. Our proposed scheme generates a number of shares on the input image. We paid more attention to evaluate the contrast of revealed images and the security result of the generated share images. We used MATLAB tool to generate the code according to the algorithm. The algorithm is tested for different color images. The experiment results guarantee that no pixel expansion, high visual quality and reasonably high security. Fig. 4.1 shows an example original image. Fig. 4.2 shows the 4 shares after encryption. Fig. 4.3 shows the final image after decryption.

Figure. 4.1: Shows an example original image


Red Shares1 of4
File Edit View Insert Tools Desktop Window Help
Green Shares2 of4
File Edit View Insert Tools Desktop Window Help
Green Shares4 of4
File Edit View Insert Tools Desktop Window Help

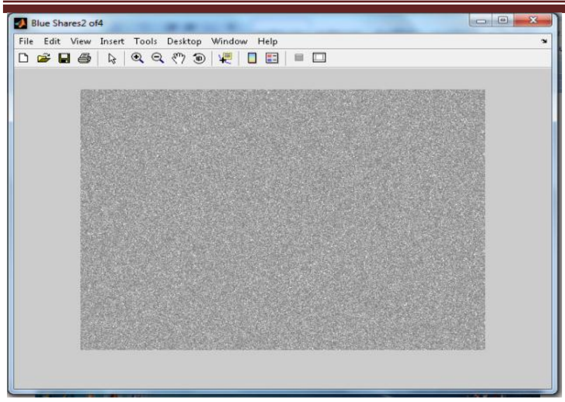


Figure.4.2: Shows the 4 shares after encryption.

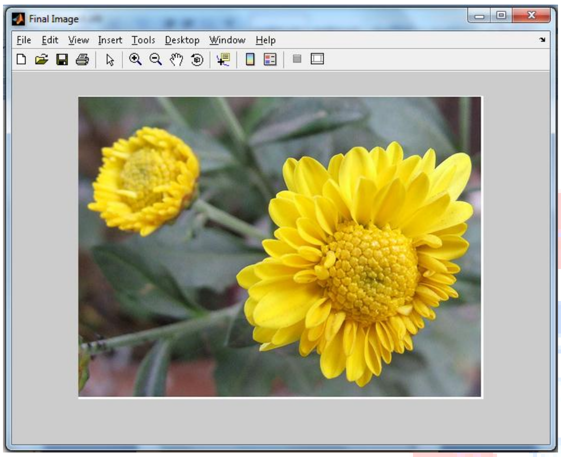


Figure 4.3: Shows the final image after decryption.

5. CONCLUSION

We established a Region Based Visual Cryptography Scheme for Color Images. The objective function is secret sharing of information. In this paper, a visual secret sharing scheme with no pixel expansion has been proposed. It can be used to create multiple shares without any pixel expansion. To reveal the secret image, n share images were just stacked and the recovery images could be recognized by the Human Visual System, no other devices were needed to reveal the secret image. If the receiver has all the shares and key then only he can decrypt. Otherwise he can't get any details about original image. Thus our proposed scheme achieved the purpose of the visual secret scheme by not only solving the critical problem of pixel expansion, but it also concentrated on security. The column permutation operation and secret key further increase security. Further research for this proposed scheme will be carried out for compressed color images like JPEG.

REFERENCES

[1] *International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2013*

[2] www.ijarce.com *– Region based visual cryptography scheme for color images.*

[3] *Bert W. Leung, Felix Y. Ng, Duncan S. Wong, " On the security of a visual cryptography scheme for color images", Pattern* Recognition, 2009.

[4] www.ijest.info/ijesto10-02-06-83.pdf - *A new visual cryptography scheme for color images.*

[5] *M. Naor and A. Shamir, "Visual Cryptography" , Proc. Adv. Cryptography: Eurtocrypt, LNCS 95, 1995.*

[6] www.ijircce.com/OB_visual.pdf - *Visual Cryptography for enhancing the security of images. [7] Tsung-Lieh Lin , Shi-Jinn Horng a, Kai-Hui Lee , Pei- Ling Chiu, Tzong-Wann Kao, Yuan-Hsin Chen, Ray-Shine Run, Jui- Lin Lai, Rong- Jian Chen, "A novel visual secret sharing scheme for multiple Secrets without pixel expansion", Pattern Recognition, 2010.*