DOI: 10.21917/ijivp.2015.0157

SECURE VISUAL SECRET SHARING BASED ON DISCRETE WAVELET TRANSFORM

S. Jyothi Lekshmi[1] and A. R. Anil[2]
Department of Computer Science and Engineering, Sree Buddha College of Engineering, India
E-mail: [1]jyothilekshmi32@gmail.com, [2]anilar123@gmail.com

Abstract

Visual Cryptography Scheme (VCS) is an encryption method to encode secret written materials. This method converts the secret written material into an image. Then encode this secret image into n shadow images called shares. For the recreation of the original secret, all or some selected subsets of shares are needed; individual shares are of no use on their own. The secret image can be recovered simply by selecting some subset of these n shares, makes transparencies of them and stacking on top of each other. Nowadays, the data security has an important role. The shares can be altered by an attacker. So providing security to the shares is important. This paper proposes a method of adding security to cryptographic shares. This method uses two dimensional discrete wavelet transform to hide visual secret shares. Then the hidden secrets are distributed among participants through the internet. All hidden shares are extracted to reconstruct the secret.

Keywords:

Visual Cryptography Scheme, Discrete Wavelet Transform, Cryptographic Shares, Subbands

1. INTRODUCTION

Nowadays, the transmission of data through the network is increasing rapidly. Visual Cryptography Scheme (VCS) is a technique using in the current technology to transmit the secret information in images i.e., the secret images. This is an important concept in the area of communication technology, information security and production. However security can be introduced in many ways like passwords, authentication, identification, watermarking techniques etc. But, in all these methods, the secret images are protected in single information carrier. If it is lost once, the secret data is destroyed.

Visual Cryptography Scheme (VCS), introduced by Naor and Shamir [1] in 1994, is a type of secret sharing techniques for images. The idea of VCS is to split a secret image into a collection of random shares. The secret image is composed of black and white pixels. Shares separately reveal no information about the original secret image other than the size of it. And transmit these shares to number of participants. Secret can be recovered by superimposing a threshold number of shares without any complex computation.

Therefore VCS is a technique used to encrypt the secret image by splitting the shares into several pieces and distribute it into the corresponding participants. A set of qualified participants can retrieve the secret image by overlapping these shares.

In traditional VCS, input is a secret image and output is collection of shares. It satisfies two conditions, 1) secret images can be recovered by any qualified subset of shares; 2) any forbidden subset of shares cannot gain any information about the secret image. In traditional (k, n) VCS, secret image can be recovered from any qualified set of k shares. Any number of shares less than k is not sufficient to reveal the secret. Here k is the number of participants and n is the number of shares.

This paper proposes a method to protect the cryptographic shares. This is done by hiding the shares in multiple images. Here discrete wavelet transform (DWT) technique is used. Shares are hiding in DWT subbands [5]. Share regeneration process includes extracting shares from cover images and then regenerates the secret by overlapping shares.

Existing XOR based Visual Secret Splitting (VSS) method is used for share generation. First a random share with same size of the image secret is generated. This random share is the first share. The second share is obtained by XOR-ing the image secret with random share [2], [3].

For example,

Table.1. XOR based VSS

Secret data	101101110
Random (Share1)	111000110
Share 2	010101000

To retrieve the original image secret, the shares are XOR-ed. We can also split data in more than two shares. For each new share, we add another series of random bits and XOR them with other shares.

The rest of the paper is organized as follows. Section 2 deals with existing methods. Section 3 describes the proposed system. Section 4 discusses results and section 5 contains conclusion.

2. EXISTING SYSTEM

Visual Secret Sharing using Cryptography [4] is a method to provide security to cryptographic shares. Halftoning, share Generation, Embedding secret, Extracting secret, reveal secret are the five phases in this method. Halftoning is used to convert the grayscale image to binary image. Shares are generated from binary image depending on scheme chosen. There are two methods to generate shares such as General Access Structure (n, n) and Threshold Access Structure (k, n) Cover images are halftoned to generate covering shares. Secret image is embedded into cover image. Reconstructed shares are generated from the embedded shares.

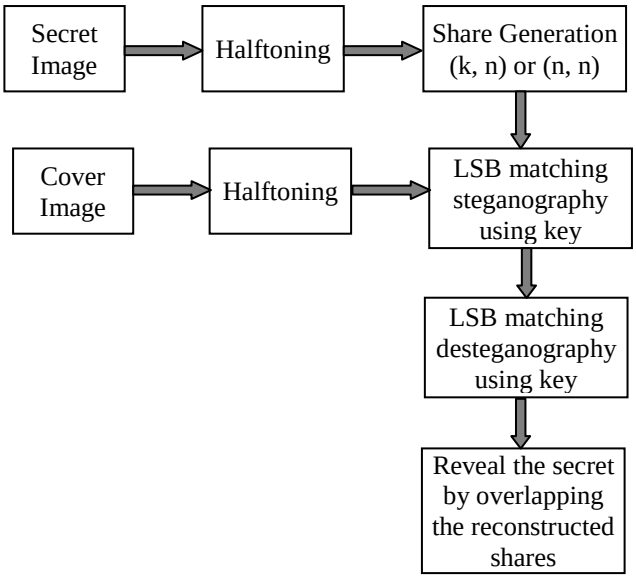


Fig.1. VCS using Cryptography

In this paper [4], Otsus Threshold method is used to generate halftone image. Here embedded shares (EM) are generated using LSB matching steganography. Key is used to generate the offset value. First it converts the secret data into number of bits. Then it reads each pixel of the cover image. If the LSB of the next cover pixel matches the next bit of secret data then no operation is needed else it adds or subtracts one from the cover pixel value at random. By decrypting the shares original shares are recovered and stacked together to reveal secret image. To recover the secret, embedded shares are desteganographed with the help of a key and reverse procedure is applied to reveal the secret.

So the steps are as follows.

- Secret image is halftoned to generate binary image (BI).
- Depending on scheme the original shares (OS) are generated.
- With the help of key original shares are embedded into cover images to generate embedded shares (ES).
- Reconstruct shares (RS) from embedded shares with the help of same key.
- To reveal the secret, overlap the reconstructed shares.

3. PROPOSED SYSTEM

Nowadays, Internet is more popular among people, for communication, information retrieval etc. Sometimes people share their secret information through the Internet. Adding security to this secret data is important.

Visual secret sharing is an efficient method for hiding an image. It is done by dividing the image into multiple meaningless shares. These individual shares do not reveal anything about the secret other than its size. The original secret can be reconstructed by combining all the shares.

This paper is focusing on security of visual secret shares. There exist different methods for data hiding using digital images [6]. The proposed method uses 2 dimensional discrete wavelet transform technique. Shares are hiding in different subbands.

Main operations of proposed method are share generation, share hiding, Extracting shares and secret regeneration.

3.1 SHARE GENERATION

XOR based Visual Secret Splitting (VSS) scheme is used to generate shares.

3.2 HIDE SHARES IN COVER IMAGE

Here the cover image is a color image. Since share generation step creates two shares, two cover images are selected.

Following algorithm is used to hide shares.

1. The cover image is in RGB color space. So convert the image from RGB to YCbCr.
2. Applying a single level two dimensional discrete wavelet transform on luminance component. The luminance image Y is divided into four subbands: Y→(S1, Sh1, Sv1, Sd1) corresponding to the low pass, horizontal, vertical and diagonal subbands. Dimensions S1, Sh1, Sv1 and Sd1 are half of those of Y in each direction.
3. Replace the subbands Sh1, Sv1 and Sd1 by the share. In order to perform replace operation, the size of share should be equal to size of the subbands. So, single share is encoded three times in cover image.
4. An inverse DWT is carried to recompose the Y image. (S1, Share1, Share1, Share1) → Y′.
5. The resulting image Y′ contains hidden share. The Fig.2 describes share hiding process.

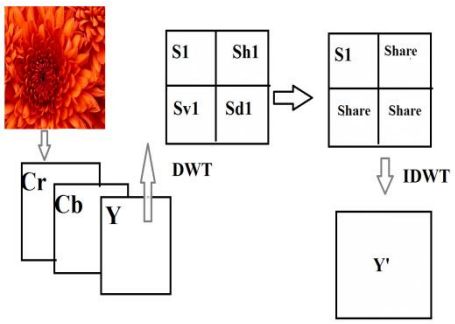


Fig.2. Share hiding in color images

To avoid data loss, three subbands are used to hide a share. This process is repeated to all shares.

The resulting image can distribute to all participants.

3.3 EXTRACTING SHARES

To decode the secret image, shares are needed to extract first. For extracting shares, DWT is applied on images that are distributed among participants.

1. A DWT converts the gray image into subbands. Y′→ (S1, Sh1, Sv1, Sd1)

2. Horizontal, vertical and diagonal subbands are interpreted as three copies of share. Since the data is encoded 3 times, it is extracted thrice.
3. These three value sets are compared, and bits that comes maximum times is taken for each pixel position.
4. Final set of values are reshaped to original size of the share. By doing this procedure all the shares are extracted.

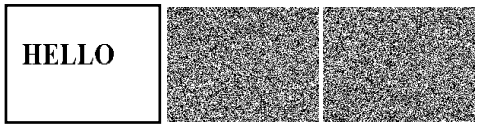
3.4 SECRET REGENERATION

Secret is regenerated by performing XOR operation on extracted shares.

4. RESULTS

The proposed method is efficient when shares are distributed through the network.

Here bitmap images are used as secret images. The Fig.3 shows the secret image selected and shares generated.



(a) (b) (c)

Fig.3. (a) Secret Image, (b) Share 1, (c) Share 2

The secret image is directly given to the system and the cover images are selected.

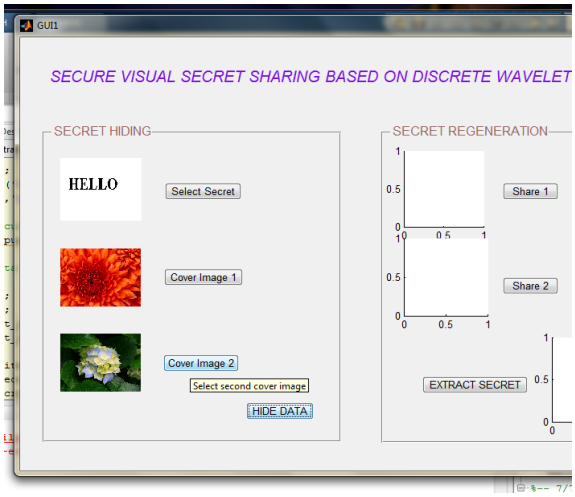


Fig.4. Data hiding

Since the encoded image is a luminance image, it is saved in bmp format.

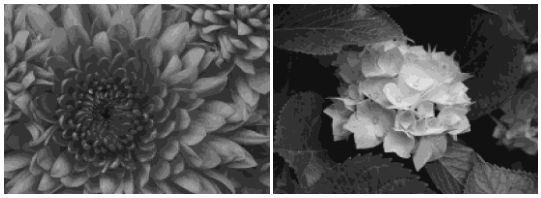


Fig.5. Encoded images for printing

This image is then distributed among participants. These images are given as input to the data extraction phase as shown in the Fig.6.

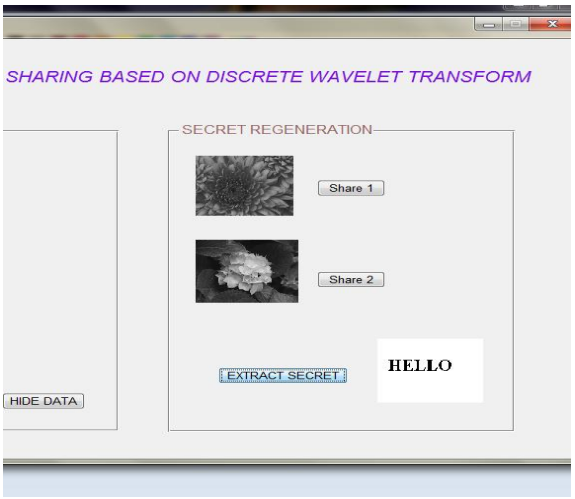


Fig.6. Data Extraction

The extracted secret is also shown in the Fig.7.

Fig.7. Extracted Secret

Here the extracted secret is exactly same as that of original secret.

The evaluation of performance of any visual cryptography schemes, which can done by considering the parameters such as Peak Signal to Noise Ratio (PSNR), Accurate Rate (AR) etc. PSNR is an approximation to human perception of reconstruction quality. A higher PSNR generally indicates that the reconstruction is of higher quality.

The method mentioned in [4] shows that PSNR values of embedded share 1 and embedded share 2 are 9.93dB and 5.51dB. Using the proposed method, MSE calculated for reconstructed secret is 0 and PSNR calculated is infinity, which indicates a high reconstruction quality.

Accurate rates can be evaluated for both the Black pixel area and the White pixel area which is denoted here as ARB and ARW. The formula to calculate the Accurate Rate for Black and White pixel area is given in the following equations.

$$AR_B = \frac{|SR = SI = 0|}{|SI = 0|}$$

$$AR_W = \frac{|SR = SI = 1|}{|SI = 1|}$$

From the above equations, where, SR is the stacking result of share image1 and share image 2, SI is the secret image, symbol 0 denotes black pixel, and symbol 1 denotes white pixel.

ARB calculated for the proposed work is 1 and ARW calculated is 1.

5. CONCLUSION

Since internet traffic is growing, security to secret exchanging through Internet is a major concern. The proposed method is efficient for providing security to cryptographic shares. Shares are generated using XOR based method. These shares are then hidden in cover image. DWT is applied to luminance component of cover image. Then subbands are used to hide share. Inverse DWT is applied to create new Y component which contains hidden shares. This image is distributed among participants. Regeneration of secret includes extraction of shares and performing XOR operation on extracted shares.

6. REFERENCES

[1] Moni Naor and Adi Shamir, "Visual cryptography", *Lecture Notes in Computer Science*, Vol. 950, pp. 1–12, 2006.

[2] Sonali Patil, Kapil Tajane and Janhavi Sirdeshpande, "Analysing Secure Image Secret Sharing Schemes Based on Steganography", *International Journal of Computer Engineering and Technology*, Vol. 4, No. 2, pp. 172-178, 2013.

[3] M. John Justin, B. Alagendran and S. Manimurugan, "A Survey on Various Visual Secret Sharing Schemes with an Application", *International Journal of Computer Applications*, Vol. 41, No. 18, pp. 6-10, 2012.

[4] Shital B. Pawar, N. M. Shahane, "Visual Secret Sharing Using Cryptography", *International Journal of Engineering Research*, Vol. 3, No.1, pp. 31-33, 2014.

[5] Ricardo L. de Queiroz and Karen M. Braun, "Color to Gray and Back: Color Embedding into Textured Gray Images", *IEEE Transactions On Image Processing*, Vol. 15, No. 6, pp. 1464-1470, 2006.

[6] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", *Defence Science Journal*, Vol. 62, No. 1, pp. 11-18, 2012.