International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secret Digital Image Sharing Using Natural Image Based VSS Scheme

Pinky .V

M. Tech Student, Dept. of Computer Science & Engineering Mount Zion College of Engineering, Pathanamthitta, Kerala, India

Abstract: ***Visual cryptography is a technique of sharing secret images. This technique encrypts a secret image into number of shares. Combining these shares generates the original image and it can be directly recognized by the human visual system. Visual Secret Sharing scheme is a method of distributing and sharing the secret image amongst a set of users. In conventional visual secret sharing scheme, the shares May holding the security parameters for protecting the secret image but it will leads to suffering the problem of transmission risk. This is the main problem in conventional VSS scheme. To solve this problem here introduce a new scheme of secret digital image sharing via natural image based VSS scheme. In this proposed scheme the shares are encrypted by using the strong AES encryption technique after that this encrypted share is embedded into the natural image. For recovering the original image, it is necessary to decrypt the encrypted share. This method not only reduces the transmission risk problem but also enhance the security of the secret image.***

Keywords: Visual Cryptography, Visual Secret Sharing Scheme, Transmission Risk Problem, Natural Image based VSS scheme, Encryption/Decryption technique**.**

1. Introduction

In communication system security of secret image is very important. In today's world data become more valuable and security is the major problem which comes from text data to multimedia data. When using secret images, security issues should be considered because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed.

The Visual cryptography scheme (VCS) is an effective and secure method that encrypts a secret image into shares. Visual Cryptography is a special kind of cryptographic scheme where the decryption of the encrypted secret is done by the human vision and not by complex mathematical calculations. Visual Cryptography deals with any secrets such as printed or pictures, etc. These secrets are fed into the system in a digital (image) form. The digital form of the secrets is then divided into different parts based on the pixel of the digital secret. These parts are called shares. The shares are then combined together correctly to reveal the secret.

In conventional visual secret sharing scheme, secret image is encrypted into shares then encoded and stored in digital form. The shares are look like noise-like pixels. It will cause high transmission risk problem because of holding noise-like shares. These shares are not user friendly. Existing scheme focuses only on using transparencies or digital media as carriers for a VSS scheme. The researchers tried to enhance the friendliness of VSS schemes for participants and also reduce the transmission risk.

The proposed natural image based VSS scheme transmits secret digital images via various natural images. It reduces the transmission risk problem during transmission of shares. Here shares are transmitted via natural images. Natural images can be color photographs of scenery, web images, or photographs. In the proposed scheme diverse media is used for sharing digital images. Using a variety of media for sharing the secret image increases the difficulty of altering the shares. These unaltered natural shares are greatly reducing the interception probability of shares. The proposed Natural image based VSS scheme not only enhances user friendliness and manageability, but also reduces transmission risk.

The remainder of this paper is organized as follows. Section 2 provides related study of previous works. Section 3, reviews proposed system implementation. Section 4 reviews result and performance analysis. Finally, concludes this work in Section 5.

2. Related Study

The term "Visual Cryptography" is introduced by Naor and Shamir in 1994. They developed a scheme called the (*k*, *n*)-threshold visual secret sharing scheme. The major feature of their scheme is that the secret image can be decrypted simply by the human visual system without using any complex computation. This method generates shares out of the secret image, and to decode the secret image requires as many as k, where $k \leq n$, or more shares printed out on transparencies and combined together. Otherwise, there is no way the secret image can be revealed out of the shares. This method is perfectly secure.
The main advantage of this scheme is that easy to implement, and the decryption of the secret image requires neither the knowledge of cryptography nor complex computation. This method suffers the pixel expansion problem and also suffers the management problem.

Chen and Tsao designed VC scheme by RGs in which the size of each generated share is the same as the input image. Their method is based on recursively encoding secret image to generate the shares one by one. This can be applied to divide a secret image among multiple shares with each share

has same size as the input image. The secrets on the input image can be revealed and recognized by naked eye by superimposing the shares; however, the management of the noise-look shares is a problem. VC using Random Grid is a solution for generating non-expansible transparencies. Random Grid Visual Secret Sharing Scheme is proposed to overcome the problem of Pixel Expansion.

The main advantage of this scheme is that it will provide a friendly interface to manage the numerous noise-look shares created by the VC scheme. And also the pixel expansion problem is solved. The management of noise-look share is a problem in this scheme and it cannot manage huge amount of data properly.

The management problem in above scheme is solved by Extended Visual Secret Sharing Scheme. This scheme uses cover image on each share so that it is easy to maintain for both sender and receiver. It is also known as the friendly VC scheme. The advantages of this method are that it will be the General approach to clarify the Pixel Expansion problem and it is easy to know in which cover which image is hidden. Also it is easy for receiver also to combine cover image and extract secret image. The disadvantage is that EVCS send noise like image in shares, that time if receiver can't get the share properly, so it is difficult for receiver to obtain secret image. Security is a problem. Visual quality is poor.

The existing VSS schemes introduces transmission risk problem during the transmission of shares. A method for reducing the transmission risk is an important issue in VSS schemes.

3. Proposed System Implementation

3.1 System Architecture

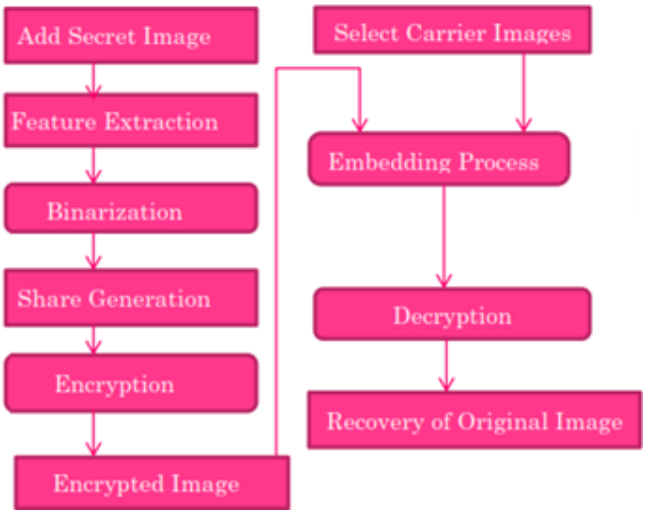

Figure 1: System Architecture

In Natural image based visual secret sharing scheme, the digital image of secret image is generated by the process of binarization. These shares are transmitted during the transmission phase. Before transmission, selecting the natural images such as color photographs of scenery, family activities, or even flysheets, bookmarks, hand-painted pictures, web images, or photographs where the encrypted shares are embedded. Here use an efficient AES encryption/decryption algorithm. After that the original digital image is recovered by the process of decryption techniques. The main procedures in NVSS scheme are: Feature Extraction, Binarization, Share Generation, Encryption, Embedding encrypted shares, and Decryption.

3.1.1 Feature Extraction Process

In feature extraction process feature s from images are extracted. The resultant feature matrix is used for next section. The feature extraction module consists of binarization, stabilization, and chaos.

3.1.2 Binarization

In binarization process, the binary feature matrix of an image is extracted. Here in this process the binary feature value of a pixel can be determined by a threshold value. That value is determined by calculating the mean value of the pixel block. Then comparing the threshold value with the pixel block value, if the threshold value is greater the pixel value then the binary matrix has the value 1 otherwise put 0. The result of binarization is binary or digital image. The stabilization process is used to balance the number of black and white pixels of an extracted feature image in each block. The chaos process is used to eliminate the texture that may appear on the extracted feature images and the generated share.

3.1.3 Share generation

In share generation process here two shares are generated from the binary image. The two shares may consist of transparencies or black pixels. Addition of noise is performed here.

3.1.4 Encryption

AES Encryption technique is used to encrypt the shares generated from the binary image. The user may take a value as the key to encrypt the shares. In the existing method XOR Encryption technique is used. Advanced Encryption Standard is a symmetric key cipher technique used to secure and encrypt operating systems, hard drives, networking systems, files, e-mails, and other similar data. In cryptography, AES consist of three block ciphers taken from a larger collection. Each cipher has a 128-bit block size with three different key sizes of 128, 192, and 256 bits. The AES cipher does a number of transformation rounds repetitiously, which converts the input plain text into an output of cipher text. There are several processing steps for each round with one round that relies exclusively on the encryption key. Then, a set of reverse rounds are applied to convert the cipher text back into plain text. The AES encryption only uses one 128-bit key to encrypt and decrypt data.

3.1.5 Embedding encrypted shares

After the encryption technique the encrypted cipher is embedded in to the natural images. Natural image consists of large number of pixels in RGB format. The LSB technique is used for embedding shares.

3.1.6 Decryption:

The AES Decryption technique is used to decrypt the cipher text using the same key used in the encryption technique.

And also the same natural images are taken in right order to decrypt the image. In decryption process original image is recovered.

3.2 System working

The major steps involved during the design of proposed system are :
Step 1: Selection of Secret image
Step 2: Binarization of Original Image resulting binary or digital image.
Step 3: Share Generation phase. Shares are generated from the binary image.
Step 4: Then selection of natural image such as photographs or web image.
Step 5: Encryption of Shares using AES Encryption method.
Step 6: Embedding the encrypted shares into natural image by using LSB technique.
Step 7: Decrypting the shares.
Step 8: Reconstructing the original binary image.

3.3 Module description

The main modules included in this proposed scheme are: Image Preparation, Share Construction, Encryption Technique, and Decryption Technique.

3.3.1 Image preparation

The image preparation process consists of three main Methods: binarization, stabilization, chaos. In binarization process, the binary feature matrix of an image is extracted. Here in this process the binary feature value of a pixel can be determined by a threshold value. The result of binarization is binary or digital image. The stabilization process is used to balance the number of black and white pixels of an extracted feature image in each block. The chaos process is used to eliminate the texture that may appear on the extracted feature images and the generated share

3.3.2 Share generation:

In share generation process here two shares are generated from the binary image. The two shares may consist of transparencies or black pixels. Addition of noise is performed here.

3.3.3 AES Encryption:

AES Encryption technique is used to encrypt the shares generated from the binary image. The user may take a value as the key to encrypt the shares. In the existing method XOR Encryption technique is used. Advanced Encryption Standard is a symmetric key cipher technique. Each cipher has a 128-bit block size with three different key sizes of 128, 192, and 256 bits. After the encryption technique the encrypted cipher is embedded in to the natural images. Natural image consists of large number of pixels in RGB format. The LSB technique is used for embedding shares.

3.3.4 AES decryption:

The AES Decryption technique is used to decrypt the cipher text using the same key used in the encryption technique. And also the same natural images are taken in right order to decrypt the image. In decryption process original image is recovered.

4. Result and Performance Analysis

Here evaluate the performance of proposed Natural Image based VSS Scheme and analyses the result generated.

Figure 2: Binarization process of original image.

After the binarization process binary image is generated. Based on a threshold value the binary matrix is designed from the pixel block value of original image.

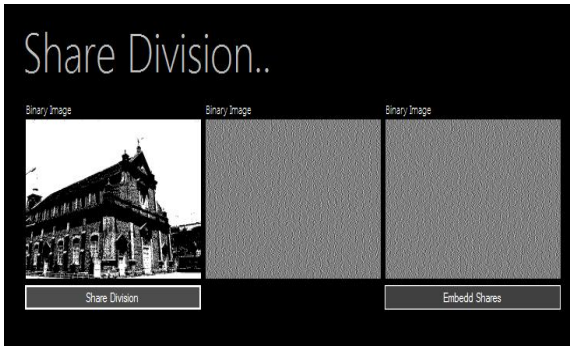

Figure 3: Share generation from binary image.

Shares are generated from the original binary image. Here two shares are generated from the binary image. So selecting two natural images for embedding shares. During share generation noise is added to the shares.

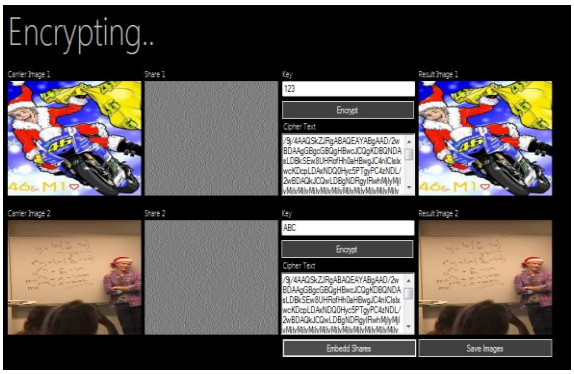

Figure 4: Encryption of Shares and Encrypted share is embedded into natural image.

After selecting natural images, the two shares are encrypted using the AES encryption algorithm. Here the user wants to selects a value as the key used to encrypt the shares. This key is used to perform the AES encryption technique. That key is also used for the decryption technique. After the encryption,

the encrypted share is embedded into the selected natural images. For embedding the shares, LSB technique is used. After embedding the shares the images are stored in selective folders.

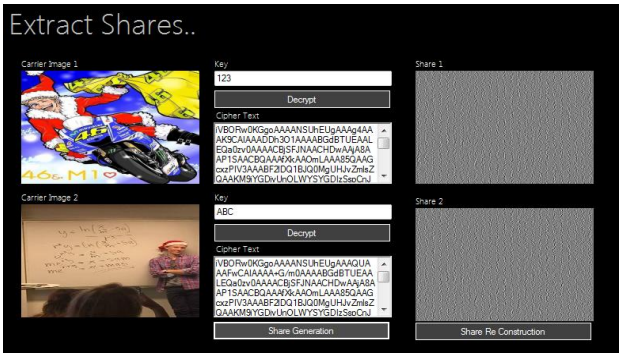

Figure 5: Extracting Shares from natural image and decryption of encrypted shares

The encrypted shares are embedded into the natural images. So for performing decryption on shares, the encrypted shares must be extracted from the natural image. After that the encrypted share undergoes decryption. Then decrypted shares are designed. The AES Decryption technique is used to decrypt the cipher text using the same key used in the encryption technique. And also the same natural images are taken in right order to decrypt the image.

Figure 6: Reconstruction of secret digital image

The decrypted shares are combined to form the original secret digital image. This proposed system efficiently reconstructs the original secret digital image. The transmission risk problem is solved in this proposed system.

5. Conclusion and Future Work

Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness, both for shares and for users. The proposed natural image based VSS scheme transmits secret digital images via various natural images. It reduces the transmission risk problem during transmission of shares. Here shares are transmitted via natural images. Natural images can be color photographs of scenery, family activities, or even flysheets, bookmarks, hand-painted pictures, web images, or photographs. The main advantages of proposed scheme are it greatly reduce the transmission risk problem, provides high level of user friendliness and manageability. The future work of this paper is, in the proposed system there may be a chance to loss image. To avoid this we develop a lossless image based sharing scheme.

6. Acknowledgment

The author gratefully acknowledge the valuable comments and suggestions of the reviewers, which have improved the presentation and also thankful to the reference paper authors. And the author is especially grateful to Prof. Smitha for her kind help during the review process of this paper.

References

[1] M. Naor and A. Shamir, “Visual cryptography,” in *Advances in Cryptology*,vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.
[2] R. Z. Wang, Y. C. Lan, Y. K.Lee, S. Y. Huang, S. J. Shyu and T. L. Chia,”Incrementing visual cryptography using Random Grids” , Opt. Commun., vol. 283, no. 21, pp. 4242-4249, Nov 2010.
[3] C. N. Yang and T. S. Chen, “Extended visual secret sharing schemes: Improving the shadow image quality,” *Int. J. Pattern Recognit. Artif. Intell.*, vol. 21, no. 5, pp. 879–898, Aug. 2007.
[4] K. H. Lee and P. L. Chiu, “An extended visual cryptograpgy algorithm for general access structures,” IEEE Trans. Inf. Forensics Security , vol. 7.no. 1,pp. 219-229, Feb. 2012.
[5] F. Liu and C. Wu, “Embedded extended visual cryptography schemes ,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307-322, Jun. 2011.
[6] I. Kang, G. R. Arce, and H. K. Lee, “Color extended visual cryptography using error diffusion,” IEEE Trans. Image Process.,vol. 20, no. 1, pp.132-145, Jan. 2011.

Author Profile

Pinky. V received the degree in Computer Science & Engineering from the Travancore Engineering College, Oyoor, Kerala in 2013, Kerala University. She is now doing M.Tech in Computer Science & Engineering in Mount Zion College of Engineering, Pathanamthitta, Kerala, and M.G University.