Survey on Biometric Image Sharing Using Cryptography and Diverse Image Media

Ms. Pratidnya Deshmukh
Department of Computer Engineering, P.V.P.I.T.,
University of Pune, Maharashtra, India
pratidnyadeshmukh@gmail.com

Prof. N. D. Kale
Department of Computer Engineering, P.V.P.I.T.,
University of Pune, Maharashtra, India
navnath1577@yahoo.co.in

Abstract— Visual Secret Sharing Scheme is used to transmitting or delivering the secret images over the network. The VSS scheme has a major drawback that is it suffers from high transmission risk because the shares are like noise. As the shares are like noise that causes the attackers attention. In this paper we are using a natural-image based visual secret sharing (NVSS) scheme to reduce the transmission risk problem that occurs in VSS scheme. The NVSS scheme uses the natural images such as paintings, photographs etc as digital shares. As we are using the natural shares instead of noise like shares which reduces the transmission risk to certain limit. This scheme also uses the different media to transmit the shares.

Keywords: *Visual secret sharing scheme, transmission risk, natural images*

*****

I. INTRODUCTION

The internet is a general term which provides many services to user. Users can transmit their messages or information to distance friends or go shopping in virtual shops by using the Internet, so it helps us to reduce our precious time. Many types of protection methods are used for preventing the sensitive message to be stolen such as cryptography, visual sharing, and data hiding.

The conventional cryptography is method which converts the plaintext (original) data into cipher text (unreadable form) data. To read the plaintext receiver has to decrypt the cipher text using secret key. The visual cryptography is a technique which encrypts the secret images into n shares. When all the shares are combined then it will give the secret image but anyone who holds the shares less than n can not reveal the information. Visual secret sharing secret (VSS) scheme is a scheme that is used to share the image securely in a non computer environment [1]. As the number of shares increases, it becomes more difficult to manage the shares, which never provide any information for identifying the shares.The VSS scheme has two drawbacks one is transmission risk and another is meaningless shares are not user friendly.

In (2, 2) VSS scheme the image is divided into two component images. Every pixel of an image component is divided into parts. If the pixel is divided into two parts then it has one white and one black block. Every pixel is in proximity to each other.

This paper is organized as: section II describes the related work in detail, section III describes VSS scheme and in section IV the paper is concluded.

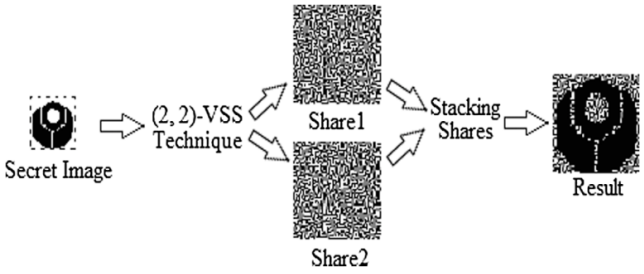

Fig. 1 VSS Scheme.

II. RELATED WORK

K. H. Lee et al. [1] provides (n, n) - NVSS (natural image based VSS) scheme to reduce the transmission risk that occurs in the VSS Scheme by using natural images and diverse media as carrier. This scheme uses the feature extraction process and encryption/decryption algorithms. Secret key is extracted from the randomly selected natural image using feature extraction. In the process of encryption the natural image and the generated secret key is sent to the participants. During the decryption secret image and the generated image reveal the original image. Quick Response Code (QR code) is used to hide the noise like share during the transmission.

P. L. Chiu et al. [2] have studied about simulated annealing based algorithm which is used to solve the threshold VCS problem. This scheme reduces the pixel expansion problem and improves the visual quality.

K. H. Lee et al. [3] proposed a two-phased encryption algorithm for the EVCS (Extended Visual cryptography scheme) for general access structure. The first phase uses the optimization techniques for a given access structure, construct a noise-like shares. The second phase directly

adds a cover image on each share via stamping algorithm. This algorithm is applicable to binary secret/cover images. No computational devices are needed during the decryption phase. This scheme reduces the management problem but not pixel expansion problem.

F. Liu et al [4] describes the Embedded EVCS (Embedded extended visual cryptography schemes) which is constructed by adding random shares of secret image into meaningful covering images. It will improve the contrast of the recovered secret image and produce clear image. Embedded EVCS has many advantages, such as it can deal with gray-scale input images, has smaller pixel expansion, is always unconditionally secure, one participant only needs to carry one share, and can be applied for general access structure.

I. Kang et al [5] introduces the concept of visual information pixel (VIP) and error diffusion to gain a color visual cryptography encryption method that produces meaningful color shares with high visual quality. VIPs are used to synchronize the positions of pixels that carries the information of original images across the color channels so as to retain the original pixel values the same before and after encryption. Error diffusion is a type of halftoning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. Its main use is to convert a multi-level image into a binary image.

T. H. Chen et al [6] tells about friendly random-grid algorithm (FRGVSS) which solves the problem of pixel expansion and converts meaningless shares into meaningful shares images. This is very user friendly and gives wide image format.

Z. Zhou et al [7] have proposed halftone visual cryptography in which the secret binary image is encoded into halftone images or halftone shares. This method uses the rich theory of blue noise halftoning to generate the halftone shares and which applies to the construction mechanism used in conventional VC. The obtained visual quality is better than extended VC.

Z. Wang et al [8] have studied about HVC (Halftone visual cryptography) construction method based on error diffusion. Meaningless shares are encoded into halftone shares taking meaningful information which reduces the suspicion of intruders. The pixel which carries the secret image information is predetermined before a halftone share is generated. Error diffusion improves the image quality of halftone shares and completely remove the error interference of reconstructed secure image.

C. Guo et al [9] describes a multi-threshold secret image sharing scheme based on MSP (monotone span programs). In this scheme we can define different types of pre-define access structure on shadow images. The aim is to construct a multi-threshold access structure in secret image sharing. This scheme also provides the authentication to verify the shadow images.

III. NVSS SCHEME

The NVSS scheme uses the natural images such as paintings, photographs etc as digital shares. As we are using the natural shares instead of noise like shares which reduces the transmission risk to certain limit. This scheme also uses the different media to transmit the shares. This scheme uses the one time pad (OTP) technique. OTP is a technique in which private key is generated randomly and which is used only once to encrypt a message. Encrypted message is then decrypted by the receiver using a matching OTP and key

A. Algorithm selection

Encryption process in proposed (n, n) NVSS scheme consists of two main phases: feature extraction and encryption phase.

1) Feature Extraction Process:

In this phase some features are extracted from natural shares. Wavelet transform method is used to extract the features from images. This is a mathematical method which compresses the image and also processes the digital signals. The extracted feature is an image which is somewhat similar to original image. Extraction reduces the randomness and provides the security of the share. The feature extraction consists of three processes binarization, Stabilization and Chaos. The binarization process is used to extract binary feature matrix from natural image. The stabilization process is used to balancing the occurrence frequency of values 0 and 1 in a matrix. Finally , chaos process is used to add noise in the matrix which changes the order of original matrix.

B. Encryption phase

1) Share Creation:

- In the encryption phase, the *n*- 1 feature images (F1,…, F*n*-1) with 24-bit/pixel color depth and the secret image execute the XOR operation to generate one noise-like share S with 24-bit/pixel color depth.
- Then, to reduce the transmission risk of share S, the share is concealed behind cover media or disguised with another appearance by the data hiding process.
- The resultant share S_ is called the generated share.

 ISSN: 2321-8169
3679 - 3681

2) Recovered Share :

- The *n* -1 innocuous natural shares and the generated share are *n* shares in the (*n*, *n*)-NVSS scheme.
- When all *n* shares are received, the decryption end extracts *n* -1 feature images from all natural shares and then executes the XOR operation with share S to obtain the recovered image.

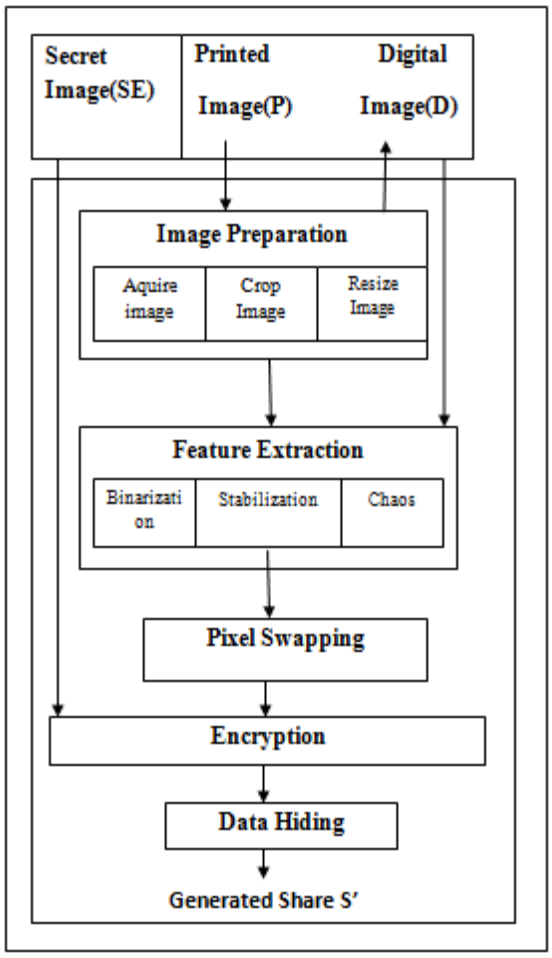

Fig. 1 Encryption Process

IV. Conclusions

The NVSS scheme reduces the transmission risk problem by using the natural images as shares. This scheme shares the images using heterogeneous carriers. The NVSS scheme also uses data hiding techniques such as stenography and QR code. This is a user friendly scheme for both participants and shares.

Acknowledgment

I am extremely thankful to my guide Prof. N.D. Kale for suggesting topic for survey and providing all the assistance needed to complete the work. He inspired me to work in this area.

References

[1] Kai-Hui Lee , Pei-Ling Chiu, "Digital Image Sharing by Diverse Image media", IEEE Transactions on Information Forensics and Security, vol 9, No. 1,pp.88-98,January 2014.

[2] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[3] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.

[4] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun. 2011.

[5] 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.

[6] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693–1703, Nov. 2011.

[7] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[8] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[9] C. Guo, C. C. Chang, and C. Qin, "A multi-threshold secret image sharing scheme based on MSP," Pattern Recognit. Lett., vol. 33, no. 12, pp. 1594–1600, Sep. 2012.