Extended Scheme of Visual Secret Sharing for Digital Images

Khemutai K. Tighare
Department of Computer Science and Engineering
Nagpur University
Nagpur, India
e-mail: ktighare971@gmail.com

Chetan Bawankar
PG Department of Computer Science and Engineering
Nagpur University
Nagpur, India
e-mail: chetan251htc@gmail.com

***Abstract*—**In visual secret sharing (VSS) secret image is encrypted in shares, with each participate involved in technique holding one or more shares, all the shares are required to reveal any information. Conventionally shares are either printed on transparencies or are encoded and stored in digital form. The shares may appear as noise like pictures and will arouse suspicion and increase interception risk during transmission. Thus VSS scheme suffer from a transmission risk problem and also meaningless shares are not user friendly. With increasing number of shares, it become more difficult to manage the share. Using Steganography secret images can be concealed in cover images but the stego images still can be detected by steganalysis method. In the given scheme, Extended Scheme of Visual Secret Sharing for Digital Images (ESVSS), secret image is shared using digital images.

Keywords-*visual secret sharing scheme, steganograph.;*

*****

I. INTRODUCTION

In today's world security is big issue and securing important data is very essential, so that the data cannot be intercepted or misused for any kind of unauthorized use. The hackers and intrudes are always ready to get personal data or important data of a person or an organization, and misuse them in various ways. For this reason, the field of cryptography is very important and the cryptographers are trying to introduce new cryptographic method to secure the data as much as possible i.e. encryption of data and hiding data from unauthentic usage is very important.

The word Steganography, with origin in Greek, means "covered writing," in contrast with cryptography, which means "secret writing". Steganography means concealing the message itself by covering it with something else. The covering media can be text, image, audio and video [3] [5].

The technique which is used to transmit or deliver the secret image over the network is known as visual secret sharing scheme. In visual secret sharing scheme an image is broken up into n shares so that only someone with all n shares can decrypt the image, while n-1 shares reveal no information about original image. Each share is printed on a separate transparency and decryption is performed by overlying the shares. When all shares are overlaid the original image will appear.

This basic model can be extended into a visual variant of the k out of n secret sharing problem [2]. In k out of n, scheme of visual cryptography, a secret binary image is cryptographically encoded into shares of random binary patterns i.e. image is divided into n number of shares by cryptographic computation. In decryption process only k or more number of shares can reveal the original information. Less than k number of shares can not reveal the original information. But there is also a high transmission risk because holding noise like shares will cause attackers attention and the shares may be intercepted.

Conventional shares, which consist of many random and meaningless pixels, satisfy the security requirement for protecting secret content but there is high transmission risk. The method for reducing transmission risk is an important issue in VSS scheme

ESVSS scheme can share a secret image over arbitrarily chosen digital images (here after called shares) and one noise like share generated using secret image and digital images. Instead of altering the contents of the images, the proposed approach extracts features from each share. These unaltered shares are totally innocuous, thus greatly reducing the interception probability of these shares. The generated share is noise like that can be concealed using data hiding techniques to increase the security level during the transmission phase. The main objective of the proposed scheme ESVSS is to reduce the incepted risk during the transmission phase.

II. RELATED WORK

Researchers used Steganography techniques so that the secret message is embedded into an image (or any media) called cover image and then sent to the receiver who extract the secret message from the cover image. After embedding the secret message, the cover image is called stego-image. This image should not be distinguishable from the cover image, so that the attackers can't discover any embedded message.

Visual cryptography is a technique that encrypts a secret image into n shares, with each participant holding one or more shares. Anyone who holds fewer than n shares cannot reveal any information about the secret image. Stacking n shares reveal the secret image and it can be recognized directly by the human visual system. Sharing and delivering secret image is also known as visual secret sharing. Drawback of VSS scheme is that it suffers from high transmission risk as the shares are like noise which cause attackers attention and the shares can be intercepted. As the number of shares increases, it becomes more difficult to manage the shares, which never provide any information for identifying the share[1].

Researchers extended k out of n secret sharing to apply on color images. They proposed an algorithm to divide a digital color image into n number of shares where minimum k number of shares are sufficient to reconstruct the image. If k number of shares are taken then the remaining shares are (n-k). In an image if certain position of a pixel is 1, then in (n-k)+1 number of shares in that position of that pixel there will be 1. In the remaining shares in that position of the pixel there will be 0.a

random number generator is used to identify those (n-k)+1 number of shares[8].

Researchers enhanced the friendliness of VSS scheme by adding a simple and meaningful cover images to noise like share but the problem with this enhancement is that the recovered images are have reduced display quality. Researches has focused on gray level and color images to develop a user friendly VSS scheme that adds cover images into meaningless shares[9]-[12]. To share digital images, VSS scheme use digital media as carriers, which makes the appearance of the shares more variable and more user friendly. Several papers investigated meaningful halftone shares [9]-[11] and emphasized the quality of the shares more than the quality of the recovered images. These studies had serious side effects in terms of pixel expansion and poor display quality for the recovered images, although the display quality of the shares was enhanced. Hence, researchers make a tradeoff between the quality of the shares and the quality of the recovered images.

III. PROPOSED WORK .

Compare to conventional VSS scheme all the noise like share must be delivered carefully in high security manner, while it is required only for one noise like share in proposed scheme.

ESVSS scheme includes both encryption and decryption processes. Fig.1 shows the ESVSS scheme in detail.

A. *Feature Extraction Process*

There are some existing method which can be used to extract features from images. To ensure security totally new method can be used. One can use any of the feature or more than one feature of digital images.

The feature extraction consist of three processes: binarization, stabilization, chaos processes. First, binary feature matrix is extracted from digital image via the binarization process. Then, stabilization balances the occurrence frequency of values 1 and 0 in the matrix. Finally the chaos process scatters the cluster feature values in the matrix. In the binarization process, binary feature value of a pixel can be determined by threshold function with set threshold. The stabilization process 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 image and the generated share[1].

B. *Encryption*

Encryption transforms a plain text message into cipher text. To encrypt a plain text message, the sender performs encryption, i.e. applies the encryption algorithm [7].

In the encryption phase, the n-1 feature image and the secret image execute XOR operation to generate one noise like share S. 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 a generated share. Input images include n-1 digital images and one secret image. The output image is noise like share.

C. *Data Hiding*

The S share is noise like share. Steganography and Quick-Response code (QR code) techniques can be used to concealed this noise like share and further reduce intercepted risk for the share during the transmission phase.

1)Quick Response code(QR code)

The QR code is two dimensional code, which encodes meaningful information in both dimensions and can carry to several hundred time the amount of data carried by barcodes. The code is printed on physical material and can be read and decoded by various devices, such as barcode readers and smart phones. QR codes are capable of handling of data such as numbers, alphanumeric character, kanji, kana, binary and control codes.

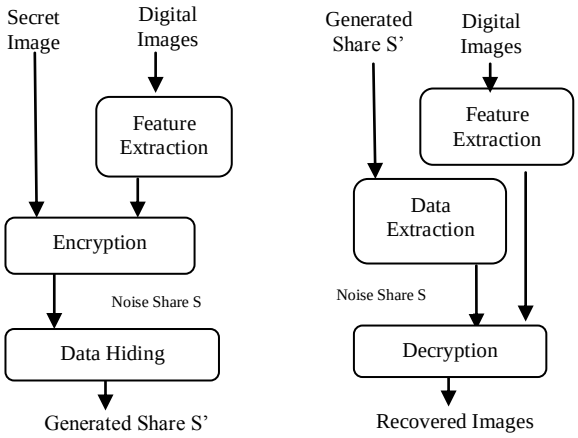

Fig 1. ESVSS scheme

2) Steganography

Steganography is the technique of hiding information and making the communication invisible. In this way, no one who is not involved in the transmission of the information suspects the existence of the information. Therefore, the hidden information and its carrier can be protected [4].

Steganography techniques-

a) Spatial Domain

Spatial domain technique, embed messages in the intensity of the pixels directly LSB is the widely used spatial domain Steganography technique. It embed the bits of message in the LSB of image pixels. But the problem with this technique is that if the image is compressed then the embedded data may be lost. Thus there is fear for loss of data that may have sensitive information.

b) Frequency Domain

Frequency domain methods hide messages in significant areas of the cover image which makes them more robust to attacks such as compression, cropping or image processing methods than LSB approach and moreover they remain imperceptible to the human sensory system as well. Many transform domain variations exist, one of which is discrete cosine transform (DCT) [6].

c) Compression Domain

In compression domain secret data is embedded into compression codes of the cover image which is then send to the receiver.

D. *Decryption*

Decryption is exactly opposite of encryption. It transforms a cipher text message back into plain text. To decrypt a

received encrypted message, the recipient performs decryption i.e., applies the decryption algorithm [7].

In the decryption phase, the secret key will be extracted again from digital images and then the secret key as well as the generated share can recover the original secret image. Input images include n-1 digital images and one noise like share. The output image is recovered image.

IV. CONCLUSION

The proposed scheme may reduce transmission risk as it is independent of increasing the number of participants. Only one noise share is generated for any number of shares.

REFERENCES

[1] Kai-Hui Lee and Pei-Ling Chiu,"Digital image sharing by diverse image media," IEEE Transactions on Informatiom Forensics and Secutity, vol.9, No.1, pp.88-98, January 2014

[2] M.Naor and A. Shamir,"Visual cryptography," in advances in cryptology, vol.950,New York, NY,USA:Springer-Verlag,1995.pp.1-12.

[3] Behrouz A. Forouzan, Cryptography And Network Security,2nd ed., McGraw-Hill Education(India), Private Limited,2008,pp.8-10.

[4] Shashikala Channalli, Ajay Jadhav, "Steganography an art of hiding data," International journal on Computer Science and Engineering Vol.1(3),2009,137-141..

[5] A.Nissar and H.Mir, "Classificaton of steganalysis technique:A study," Digit. Signal Process, vol.20, no.6, pp.1758-1770,Dec.2010.

[6] Babloo Sahu and Shuchi Sharma,"Steganographic techniques of data hiding using digital images," Defence Science Journal, vol. 62, No. 1, January. 2012,pp. 11-18,doi:10,14429/dsj.62.1436.

[7] Atul Kahate,Cryptography And Network Security,2nd ed.,McGraw-Hill Education Private Limited 2009, pp.38-44.

[8] Shyamalendu Kandar and Arnab Maiti,"K-n secret sharing visual cryptography scheme for color image using random number," International Journal of Engineering Science and Technology Vol.3 No.3 Mar 2011.

[9] 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.

[10] 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.

[11] 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

[12] 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.