www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12788-12791

Extended Approach of Visual Secret Sharing for Digital Images

Khemutai Tighare[1], Chetan Bawankar[2]

[1]Student, Computer Science and Engineering, WCEM
Nagpur, India
ktighare971@gmail.com

[2]HOD, Computer Science and Engineering, WCEM
Nagpur, India
chetan251htc@gmail.com

Abstract: ***In visual secret sharing (VSS) secret image is encrypted in shares, with each participant involved in technique holding one or more shares, all the shares are required to reveal any information. 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. With increasing number of shares, it becomes more difficult to manage the share. The proposed scheme shared secret image by generating only two noise-like color shares using natural image. These noise-like color shares are hided in two cover images to increase the security level.***

Keywords: Visual Secret Sharing, Natural Image, Transmission risk

1. 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]. The k out of n visual cryptography scheme is a type of cryptographic technique where a digital image is divided into n number of shares by cryptographic computation. In the decryption process only k or more than k 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.

The method for reducing transmission risk is an important issue in VSS scheme. Proposed scheme generate two noise-like color shares using secret image and natural image. The natural image can be photos or hand-painted pictures in digital form. Instead of altering the contents of the images, the proposed scheme extracts features from natural image. This unaltered natural share is totally innocuous, thus greatly reducing the interception probability of shares. The generated two noise-like color shares are concealed using data hiding techniques and converted to meaningful shares in order to increase the security level during the transmission phase. The main objective of the proposed scheme is to reduce the incepted risk during the transmission phase.

2. 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 shares [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 is sufficient to reconstruct the image. If k number of shares is 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].

Blundo proposed Visual Cryptography schemes for gray level images[13].

Savita Patil used the concept of visual information pixel synchronization and error diffusion to attain a color visual cryptography encryption method that produces color shares [14].

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

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 and the pixel expansion of the image.

3. 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 two meaningful shares in proposed scheme.

The One Time Pad invented by Gilbert Vernam. In OTP the key has same length as the plaintext and chosen completely in random. At sender side modular addition or logical XOR is perform between each bit of plaintext and each bit of key to generate ciphertext. This ciphertext is sent to the receiver, then the original plaintext can be obtain at the receiver side by applying the same operation and the same key used by the sender for encryption

In proposed scheme the idea of OTP is used. In encryption process instead of generating a secret random key, we extract feature from natural image and perform XOR with secret image to produce two meaningful shares. In decryption process, the features again extracted from natural image using feature extraction and then the extracted feature as well as two meaningful shares recovers the secret image.

3.1 Feature Extraction Process

There are some existing methods which can be used to extract feature from image. One can use any of the feature or more than one feature of image.

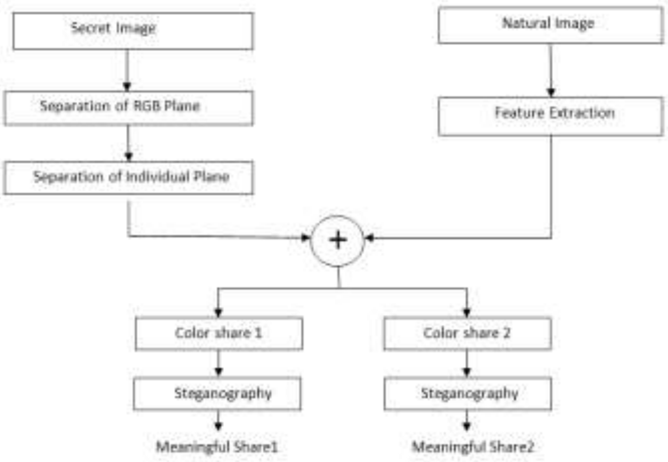

Figure 1: Encryption

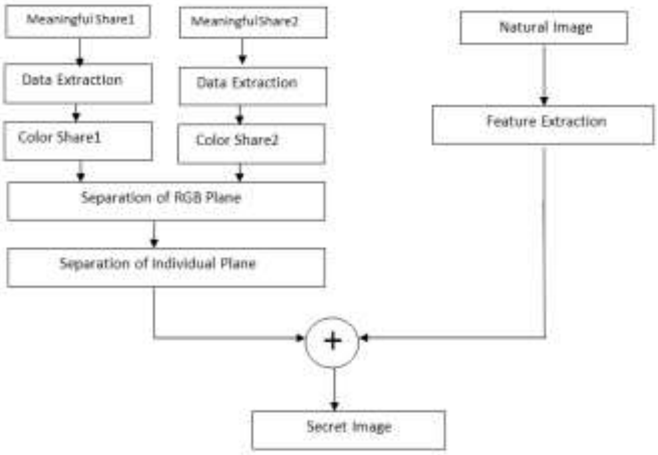

Figure 2: Decryption

In proposed scheme we use edge detection algorithm as a feature extraction method. You can use any edge detection method such as Sobel, Prewitt etc, to extract feature from natural image.

3.2 Encryption

The 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 extracted feature and the individual plane of secret image execute XOR operation to generate two noise like color shares. These two noise like color shares are concealed in cover images using Steganography to increase security level. Input images include natural image and secret image. Output images are two meaningful shares.

3.3 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].

A Steganography technique is used to conceal the noise-like color shares and further reduce intercepted risk for the share during the transmission phase.

3.4 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, data extraction is used to extract two noise-like color shares from meaningful shares. The features are again extracted from natural image using feature extraction and then from the two noise-like color shares the original secret image is recovered. Input images include natural image and two meaningful shares. The output image is secret image.

To increase further security both meaningful shares can transmit through different media such as one transmits through network and another sent by post.

4. Experimental Result

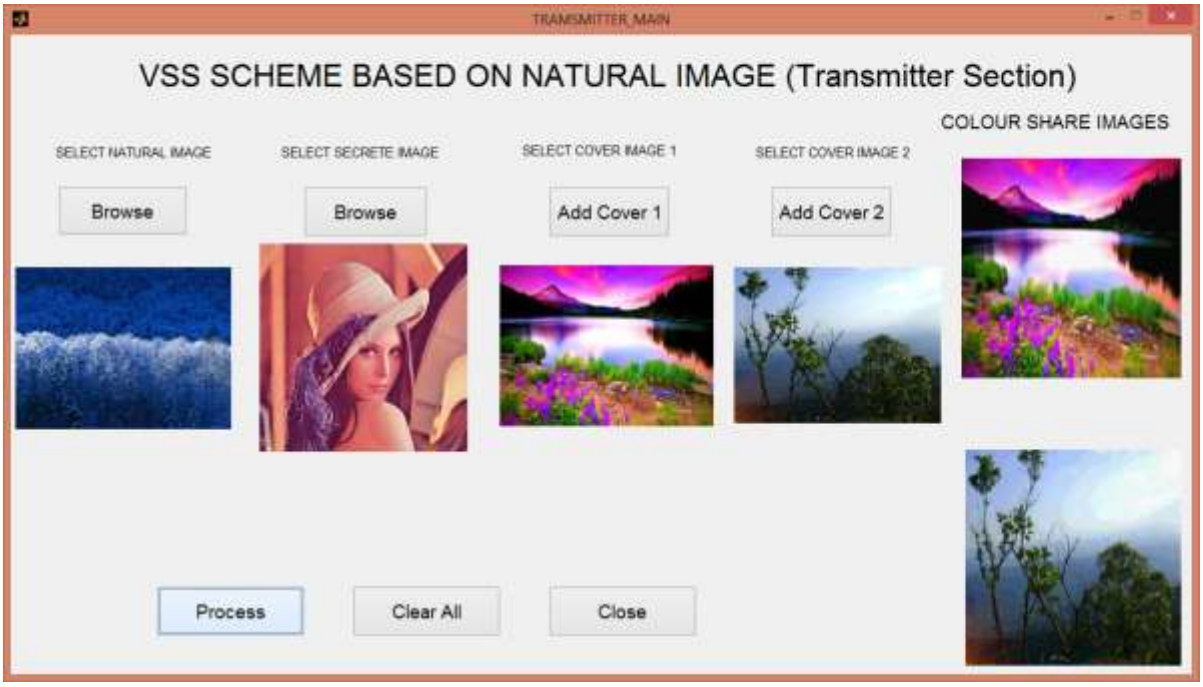

Figure 3: Transmitter

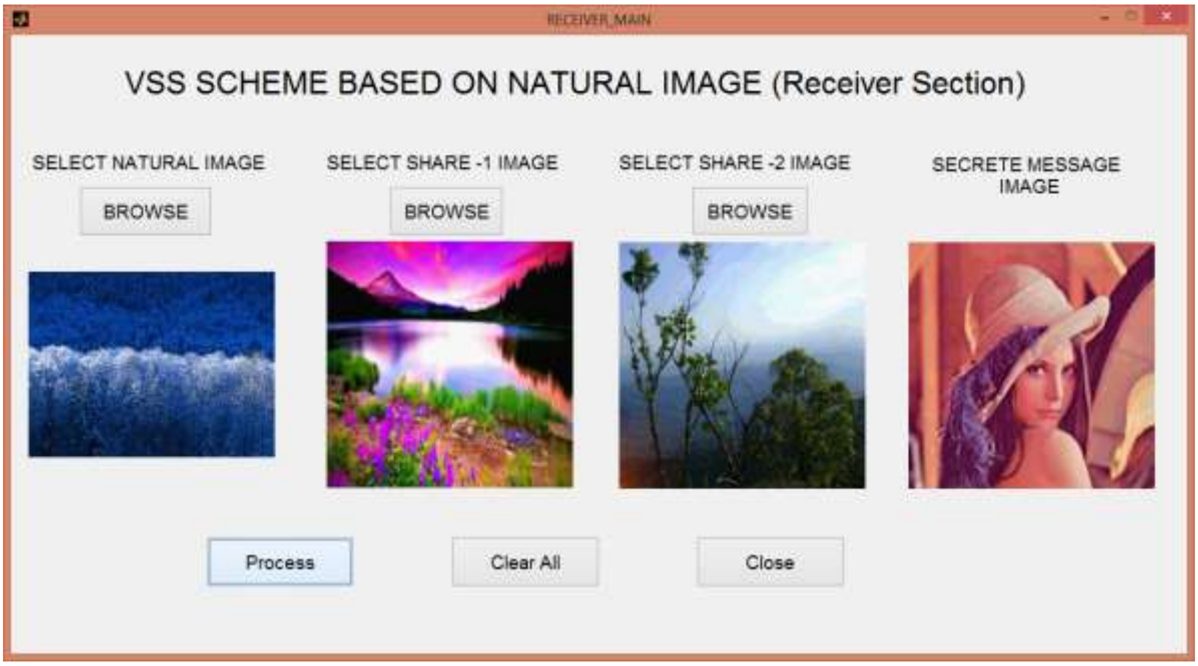

Figure 4: Receiver

usion

In VSS an image is broken up into n shares so all the noise-like share requires to deliver carefully in high security manner. Noise shares are subjected to the transmission risk. In proposed scheme only two noise-like shares are generated, which further hided using Steganography, thus reducing the transmission risk compared to conventional VSS.

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),pp.137-141,2009.

[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,pp. 11-18,January 2015 doi:10,14429/dsj.62.1436.

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

[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.

[13] C. Blundo, A. D. Santis, and M. Naor, "Visual cryptography for grey level images," Inf. Process. Lett., vol. 75, no. 6, pp. 255–259, 2000

[14] Savita Patil and Jyoti Rao,"Extended Visual Crptography for Color Shares using Random Number Generator," International Journal of Advanced Research in Computer and Communication Engineering Vol. 1,pp 399-410 Issue 6, August 2012

Author Profile

Khemutai Tighare has received her B.E. in Information Technology from Rajiv Gandhi College of Engineering Research and Technology Chandrapur, Nagpur University in 2013. Currently, she is doing Master of Technology in Computer Science and Engineering from WCEM Nagpur, Nagpur University. Her area of interest includes network security and digital image processing.