SECRET SHARING SCHEMES WITH DIVERSE IMAGE MEDIA

G. Selvapriya, J. Jayapriya Jayapal

***Abstract*—The main aim of this project is to share an image in a network to avoid a transmission risk problem. Visual Secret Sharing Schemes hide a Secret image in shares that appear noise like picture or noiseless picture. VSS schemes suffer from a transmission risk problem while sharing contains Secret Images because it will awake suspicion and increase interception risk during transmission of the shares. To address this problem, we proposed a natural-image-based VSS scheme (NVSS scheme) that shares secret images via various carrier media to protect the secret and the participants during the transmission phase. This Process involved to Share a Secret image over arbitrary selected natural images (called natural shares) and one sound-like share. The natural shares can be photos or fist-painted pictures in digital form or in printed form. The noise-like share is iniated based on these natural shares and the secret image. The proposed approach gives an excellent solution for solving the transmission risk problem for the VSS schemes. The unaltered natural shares are diverse and safe, thus greatly reducing the transmission risk problem. We also propose possible ways to conseal the noise like share to decrease the transmission risk problem for the share.**

***Index Terms*—Image sharing; Visual secret sharing (VSS); Neural VSS; QR code.**

I. INTRODUCTION

Visual cryptography (VC) 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 the *n* shares reveals the secret image and it can be recognized directly by the human visual system [1]. Secret images can be of various types: images, handwritten documents, photographs, and others. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme. The original motivation of VC is to securely share secret images in non-computer-aided environments; however, devices with computational powers are ubiquitous (e.g., smart phones). Thus, sharing visual secret images in computer-aided environments has become an important issue today.

Conventional shares, which consist of many random and meaningless pixels, satisfy the security requirement for protecting secret contents [1-4], but they suffer from two drawbacks: first, there is a high transmission risk because holding noise-like shares will cause attackers' suspicion and the shares may be intercepted. Thus, the risk to both the participants and the shares increases, in turn increasing the probability of transmission failure. Second, the meaningless shares are not user friendly. As the number of shares increases, it becomes more difficult to manage the shares, which never provide any information for identifying the shares.

Previous research into the Extended Visual Cryptography Scheme (EVCS) or the user-friendly VSS scheme provided some effective solutions to cope with the management issue [5-13]. The shares contain many noise-like pixels or display low-quality images. Such shares are easy to detect by the naked eye, and participants who transmit the share can easily lead to suspicion by others. By adopting steganography techniques, secret images can be concealed in cover images that are halftone gray images and true-color images [14-16]. However, the stego-images still can be detected by steganalysis methods [17]. Therefore the existing VSS schemes still must be investigated for reducing the transmission risk problem for carriers and shares. A method for reducing the transmission risk is an important issue in VSS schemes.

In this study, we propose a VSS scheme, called the natural image–based VSS scheme (NVSS scheme), to reduce the intercepted risk during the transmission phase. Conventional VSS schemes use a unity carrier (e.g., either transparencies or digital images) for sharing images, which limits the practicality of VSS schemes. In the proposed scheme, we explore the possibility of using diverse media for sharing digital images. The carrier media in the scheme contains digital images, printed images, hand-painted pictures, and so on. Applying a diversity of media for sharing the secret image increases the degree of difficulty of intercepting the shares. The proposed NVSS scheme can share a digital secret image over $n \aleph 1$ arbitrary natural images (hereafter called natural shares) and one share. Instead of altering the contents of the natural images, the proposed approach extracts features from each natural share. These unaltered natural shares are totally innocuous, thus greatly reducing the interception probability of these shares. The generated share that is noise-like can be concealed by using data hiding techniques to increase the security level during the transmission phase.

The NVSS scheme uses diverse media as a carrier; hence it has many possible scenarios for sharing secret

***G. Selvapriya**, Mailam Engineering College, Mailam, Villupuram District, Tamilnadu, India,*
***S. Karthik**, Mailam Engineering College, Mailam, Villupuram District, Tamilnadu, India.*

ISSN: 2278 – 1323

images. For example, assume a dealer selects n □1 media as natural shares for sharing a secret image.

II. RELATED WORKS

A. Existing System

In an existing system, Visual cryptography Scheme algorithm has been implemented to split the Secret image in to n number of shares. While Sharing n no of shares through network if any one of the share has been corrupted from unauthorized user. The Receiver couldn't form the Recovered Image.

If it not corrupted from unauthorized users. After receiving all Shares by receivers. They have to do Superimposition of merging process to get back the Recovered images. But the Recovered images have the noisy share look. It wouldn't be Clear Clarity look. 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, the quality of the recovered images, and the pixel expansion of the images [18].

B. Proposed System

In the Proposed NVSS scheme, the natural shares can be gray or color photographs of scenery, family activities, or even flysheets, bookmarks, hand painted pictures, web images, or photographs. The natural shares can be in digital or printed form. . The encryption process only extracts features from the natural shares; it does not alter the natural shares. Another share, which is generated by the secret image and features that are extracted from *natural* shares, can be hidden behind other media and then delivered by a well-disciplined person or via a high-security transmission channel. When the number of shares n increases the transmission risk of the conventional VSS Schemes increases rapidly. The proposed NVSS scheme always requires only one generated share to hide a Secret Image. When the transmission cost is limited, the proposed scheme using unaltered natural shares can greatly reduce transmission risk. NVSS scheme includes two main phases feature extraction and encryption. The feature images that were extracted from the same natural image and the secret image execute the XOR operation to generate one noise-like share S. When shares are received, the decryption end extracts feature images from all natural shares and then executes the XOR operation with share S' to obtain the recovered image.

III. METHODS

The proposed system to implement the partition parallelism we follow below methods:

A. Image Selection and Image Preparation

Initially Secret Image and Natural Images has been Chosen. Natural Images would be Painted and Digital Images. The image preparation processes are used for preprocessing printed images and for post-processing the feature matrices that are extracted from the printed images. The flow of Image Preparation process is: The contents of the printed images can be acquired by popular electronic devices, such as digital scanners and digital cameras. The next step is to crop the extra images. Finally, the images are resized so they have the same dimensions as the natural shares.

B. Feature Extraction and Encryption Process

This module describes the feature extraction process that extracts feature images from the natural shares. The module which is the core module of the feature extraction process is applicable to printed and digital images simultaneously Assume that the size of the natural shares and the secret image are w * h pixels and that each natural share is divided into a number of b *b pixel blocks before feature extraction starts. We define the notations as follows:

- b represents the block size, b belongs to even.
- N denotes a natural share.
- (x,y) denotes the coordinates of pixels in the natural shares and the secret image, 1 <=x <=w, 1 <=y <=h.
- (x1, y1) represents the coordinates of the left-top pixel in each block.
- P□xy denotes the value of color □, □{R,G,B} for pixel (x, y) in natural share N, 0 <=p □ x,y<= 255.
- Pixel value Hx,y is the sum of RGB color values of pixel (x, y) in natural share N and

  Hx,y= R_px,y+ G_px,y+ Bpx,y
- M represents the median of all pixel values (Hx1,y1, . . . ,Hxb,yb _ in a block of N.

F is the feature matrix of N, the element $f\,x,y$ belongs to ***F*** denotes the feature value of pixel (x, y) If the feature value $f\,x,y$ is 0, the feature of pixel (x, y)in N is defined as black. If $f\,x,y$ is 1 the feature of pixel (x, y)in N is defined as white.

Then the bit-plane of the secret image (resp. noise-like share) and n - 1 feature matrices execute the XOR operation (denoted by __ to obtain the bit-plane of the share image (resp. recovered image). Therefore, to encrypt (resp. decrypt) a true-color secret image, the encryption (resp. decryption) procedure must be performed iteratively on the 24 bit-planes. The input natural shares (N1, . . . ,Nn-1) of the scheme include np printed images and nd digital images (np >=0, nd >=0,n= np +nd +1, and n =np + nd +1. The np printed images must be processed and transformed into digital form in the image preparation process. Input Secret image S and feature images FI1……,FIn-1 by applying the XOR operation in each color plane. Finally, the resultant image S' is the output.

Then the encrypted input images include n natural shares and one secret image. The output image is a noise-like share called Encrypted Image [19].

C. QRCODE Generation and Network Sharing Process

In this module Quick-Response Code (QR code) techniques are introduced to conceal the noise-like share and further

ISSN: 2278 – 1323

reduce intercepted risk for the share during the transmission phase. The Encrypted Image Would is converted in to binary numbers. The Whole binary wouldn't possible to embed into QRCODE.Only Certain limited number of Characters should be embed into QRCODE.For that Purpose the whole binary numbers will be split into certain number of separation.That splitted binary numbers would be stored in a collection framework with a specific key. Here Key act as to extract the splitted binary numbers from Collection Framework. After storing all Splitted binary numbers, the key alone has been extracted and embed in to QRCODE. After Forming QRCODE, Network Sharing Process has been done from sender to Receiver. The Sender has to send Natural Shares, QRCODE and Collection Framework. Receiver has to receive the Images, when they prove their Ownership. If Receiver doesn't prove their Ownership, the images not yet received.

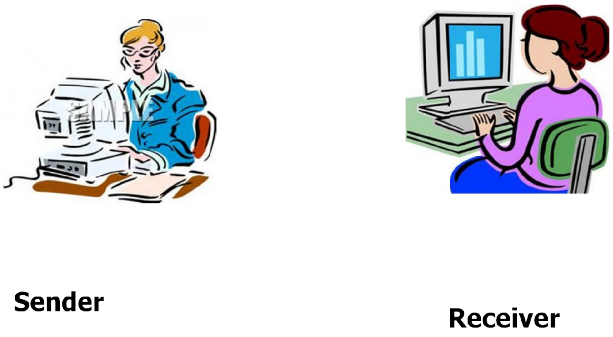

Fig. 1 Image sharing using NVSS.

D. Encrypted Image Extraction and Decryption process

After Receiver Receives all the Images has to scan the QRCODE by using Smart Phone which contains QRCODE READER Application. When the Scanning process done Receiver got all the keys for splitted binary values. Then Send the key values to Receiver Application By Socket Communication. By using that Keys Receiver has to extract the splitted binary numbers from Collection Framework then Form the Encrypted Images. When Receiver Form the Encrypted Images Decryption Process has be done by similar to Encryption method what Sender done [20].

Then the decrypted input images include n natural shares and one noise-like share. The output image is a recovered image.

IV. CONCLUSION

After Decryption process has been done, Recovered Image will be formed. By using comparing the pixel values of Secret image and Recovered image we can found there is no Pixel Expansion or Pixel corruption in the Recovered image. her is no change between Secret image and Recovered image.

It provides four major contributions. First, this is the first attempt to share images via heterogeneous carriers in a VSS scheme. Second, we successfully introduce hand-printed images for images-haring schemes. Third, this study proposes a useful concept and method for using unaltered images as shares in a VSS scheme. Fourth, we develop a method to store the noise share as the QR code.

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] 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.
[4] K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," *IEEE Trans. Image Process.*, vol. 22, no. 10, pp. 3830–3841, Oct. 2013.
[5] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Comput. Sci.*, vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.
[6] 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.
[7] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithmfor general access structures," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 219–229, Feb. 2012.
[8] 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.
[9] 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.
[10] 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.
[11] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 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] T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images," *Digit. Signal Process.*, vol. 21, no. 6, pp. 734–745, Dec. 2011.
[14] D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang, "A novel secret image sharing scheme for true-color images with size constraint," *Inf. Sci.*, vol. 179, no. 19, pp. 3247–3254, Sep. 2009.
[15] X. Wu, D. Ou, Q. Liang, and W. Sun, "A user-friendly secret image sharing scheme with reversible steganography based on cellular automata," *J. Syst. Softw.*, vol. 85, no. 8, pp. 1852–1863, Aug. 2012.

[16] 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.
[17] A. Nissar and A. H. Mir, "Classification of steganalysis techniques: A study," *Digit. Signal Process.*, vol. 20, no. 6, pp. 1758–1770, Dec. 2010.
[18] P. L. Chiu, K. H. Lee, K. W. Peng, and S. Y. Cheng, "A new color image sharing scheme with natural shadows," in *Proc. 10th WCICA*, Beijing, China, Jul. 2012, pp. 4568–4573.
[19] (2013). *QR Code.com* [Online]. Available: http://www.qrcode.com/en/index.html (Accessed).
[20] J. Fridrich, M. Goljan, and D. Soukal, "Perturbed quantization steganography with wet paper codes," in *Proc. Workshop Multimedia Sec.*, Magdeburg, Germany, Sep. 2004, pp. 4–15.

G. Selvapriya has published two papers in national level conference. Research interests lies in the areas of Information Forensics and Security, Cloud Computing, Software Engineering and Web Services.

J. Jayapriya Jayapal, M.C.A., M.Phil., M.E., M.B.A., Assistant Professor, Mailam Engineering College.

ISSN: 2278 – 1323