Digital Image Sharing By Diverse Image Media

Miss.Shubhangi Alekar[1], Miss. Shaila Labade[2], Miss.Komal Nemane[3], Miss.Reshma Gawade[4], Mr.Surayavanshi P.[5]
Department of Computer Engineering
[1,2,3,4,5] H.S.B.P.V.T College Of Engineering,Kashti

Abstract- *Conventional visual secret sharing (VSS) schemes hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form. The shares can appear as noise-like pixels or as meaningful images; but it will arouse suspicion and increase interception risk during transmission of the shares. Hence, VSS schemes suffer from a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme. 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. The proposed (n, n) - NVSS scheme can share one digital secret image over n -1 arbitrary selected natural images (called natural shares) and one noise-like share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. The unaltered natural shares are diverse and innocuous, thus greatly reducing the transmission risk problem. We also propose possible ways to hide the secret to reduce the transmission risk problem for the share. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.*

Keywords: Visual secret sharing scheme, extended visual cryptography scheme, natural images, transmission risk.

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. 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 have become an important issue today.

In this paper, we develop efficient encryption/decryption algorithms for the (n, n) -NVSS scheme. The proposed algorithms are applicable to digital and printed media. The possible ways to hide the generated share are also discussed. The proposed NVSS scheme not only has a high level of user friendliness and manageability, but also reduces transmission risk and enhances the security of participants and shares.

II. RELATED WORK

The classification of VSS schemes from the carriers' viewpoints. Existing research focuses only on using transparencies or digital media as carriers for a VSS scheme.The transparency shares have either a noise-like or a meaningful appearance. The conventional noise-like shares are not friendly [1]–[4]; hence, researchers tried to enhance the friendliness of VSS scheme forparticipants [5]–[7]. Generally,simple and meaningful cover images are added to noise-like shares for identification, making traditional VC schemes more friendly and manageable. However, the EVCSs reduce the display quality of the recovered images.Research has focused on gray-level and color secret images to develop a user-friendly VSS scheme that adds cover imagesinto the meaningless shares [8]–[13]. To share digital images,VSS schemes use digital media as carriers, which makes the appearance of the shares more variable and more userfriendly [13]. Several papers investigated meaningful halftone shares [8]–[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, the quality of the recovered images, and the pixel expansion of the images.

In another research branch, researchers used steganography techniques to hide secret images in cover images [14]–[16]. Steganography is the technique of hiding information and making the communication invisible. In this way, no one whois not involved in the transmission of the information suspects the existence of the information. Therefore, the hidden information and its carrier can be

protected. Steganography has been used to hide digital shares in VSS schemes. The shares in VSS schemes are embedded in cover images to create Fig. 1. The classification of the existing VSS research from the viewpoints of carriers. stego-images. Although the shares are concealed totally and the stego-images have a high level of user friendliness, the shared information and the stego-images remain intercepted risks during the transmission phase [17].

Recently, Chiu et al. tried to share a secret image via natural images [18]. This was a first attempt to share images via natural images; however, this work may suffer a problem—the textures of the natural images could be disclosed on the share. Moreover, printed images cannot be used for sharing images in the previous scheme. So far, sharing visual secret image via unaltered printed media remains an open problem. In this study, we make an extension of the previous work in [18] to promote its practicability and explore the possibility for adopting the unaltered printed media as shares.

III. HARDWARE IMPLEMENTATION

Hardware Resources Required

Speed	-	1.1 GHz
RAM	-	256 MB (min)
Hard Disk	-	20 GB
Floppy Drive	-	1.44 MB

IV. ROPOSED SYSTEM

In this paper, we develop efficient encryption/decryption algorithms for the (n, n) -NVSS scheme. The proposed algorithms are applicable to digital and printed media. The possible ways to hide the generated share are also discussed. The proposed NVSS scheme not only has a high level of user friendliness and manageability, but also reduces transmission risk and enhances the security of participants and shares.

The proposed NVSS scheme can share a digital secret image over n 1 arbitrary natural image (hereafter called natural shares) and one share. These 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 images. In this paper, we develop efficient encryption/decryption algorithms for the (n, n) -NVSS scheme. The proposed algorithms are applicable to digital and printed media. The possible ways to hide the generated share are also discussed.

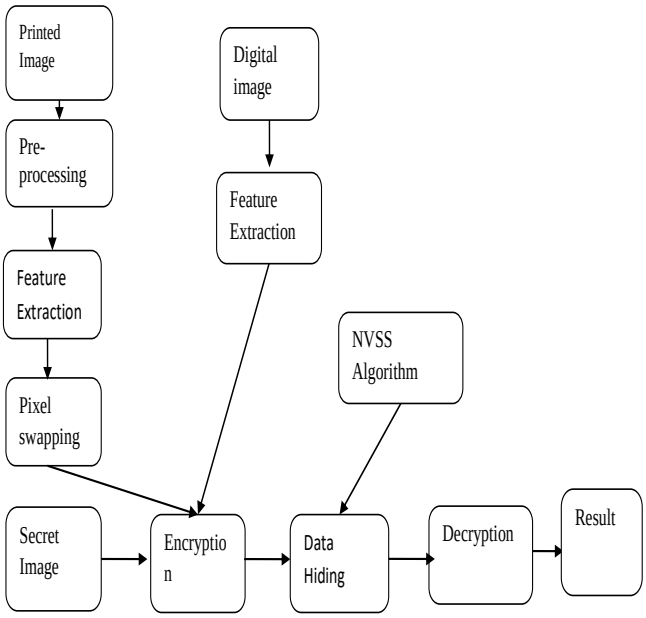

Fig : Praposed System

V. CONCLUSION

This study provides four major contributions. First, this is the first attempt to share images via heterogeneous carriers in a VSS scheme. Second, we successfully introduce digital 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] Kai-Hui Lee and Pei-Ling Chiu," Digital Image Sharing by Diverse Image Media", IEEE transactions on information forensics and security, vol. 9, no. 1, 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] Sunil G. Jare, "Digital Image Sharing Using Visual Cryptography Techniques", Sunil G. Jare et al,

International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April- 2015, pg. 717-721

[4] 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.

[5] 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.

[6] 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.

[7] Priyanka R. Pawar, Manjusha S. Borse, "transmission risk reduction in image sharing scheme with diverse image media"

[8] R.H. adekar, N.M. jadhav, N.D. Pergad," digital image sharing by diverse image media using nvss technique" , 2016 IJARIIE-ISSN(O)-2395-4396 Vol-2 Issue-1

[9] Mayuri Sonkusare, Prof. Nitin Janwe "Analysis of Digital Image Sharing By Diverse Image Media" ,Mayuri Sonkusare et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3784-3786

[10] (2013). QR Code.com [Online]. Available: http://www.qrcode.com/en/index.html (Accessed)