**International Refereed Journal of Engineering and Science (IRJES)**
*ISSN (Online) 2319-183X, (Print) 2319-1821*
*Volume 5, Issue 2 (February 2016), PP.50-52*

# Transmission Risk Reduction In Image Sharing Scheme With Diverse Image Media

Priyanka R. Pawar[1], Manjusha S. Borse[2]
*[1] PG Student, Department of ETC Engineering, Kalyani Charitable Trust's- Late G. N. Sapkal College of Engineering, Nashik, Maharashtra.*
*[2]Assistant Professor, Department of ETC Engineering, Kalyani Charitable Trust's- Late G. N. Sapkal College of Engineering, Nashik, Maharashtra.*

**Abstract:-** On transparencies or are encoded and stored in a digital form, conventional visual secret sharing (VSS) schemes hide secret images in shares that are either printed. But it will arouse suspicion and increase interception risk during transmission of the shares, the shares can appear as noise-like pixels or as meaningful images. For the secret itself and for the participants who are involved in the VSS scheme, VSS schemes suffer from a transmission risk problem. To protect the secret and the participants during the transmission phase, to address this problem, we proposed a natural-image based VSS scheme that shares secret images via various carrier media. The proposed (*n, n*) - NVSS scheme can share one digital secret image over *n* - 1 arbitrary selected natural images and one noise-like share. In digital form or in printed form, the natural shares can be photos or hand-painted pictures. The noise-like share is generated based on these natural shares and the secret image. Thus greatly reducing the transmission risk problem, the unaltered natural shares are diverse and innocuous. We also propose possible ways to hide the noise like share 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

Hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form, Conventional visual secret sharing (VSS) schemes. But it will arouse suspicion and increase interception risk during transmission of the shares, the shares can appear as noise-like pixels or as meaningful images. A transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme, VSS schemes suffer. To protect the secret and the participants during the transmission phase, to address this problem, we proposed a natural-image-based VSS scheme (NVSS scheme) that shares secret images via various carrier media. One digital secret image over *n* - 1 arbitrary selected natural images (called natural shares) and one noise-like share, the proposed (*n, n*) - NVSS scheme can share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. On these natural shares and the secret image, the noise-like share is generated based. Thus greatly reducing the transmission risk problem, the unaltered natural shares are diverse and innocuous. To reduce the transmission risk problem for the share, we also propose possible ways to hide the noise like share. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.

### 1.1 Block Diagram

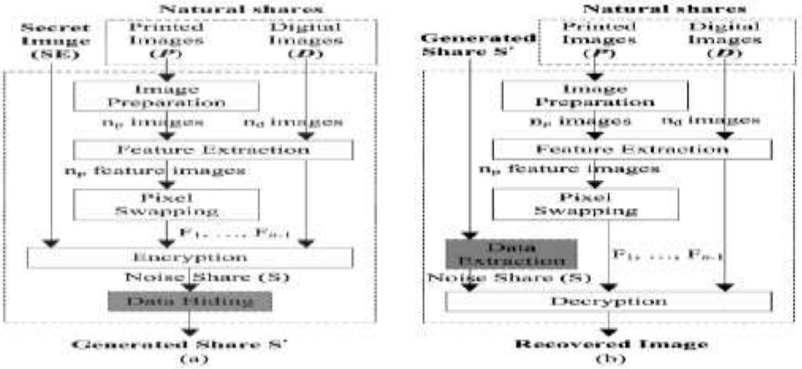

**Fig. 1. Generalized block diagram of the encryption and decryption process of the (n, n) - NVSS scheme.**

## II. RELATED WORK

Reducing the pixel expansion and improving the display quality of recovered images are still major issues in visual cryptography schemes (VCSs), particularly for large *k* and *n*. Moreover, the development of a systematic and practical approach for threshold VCSs is a challenge. In this paper, a pixel-expansion-free threshold VCSs approach based on an optimization technique is proposed in order to encrypt binary secret images. In addition to contrast, we consider blackness as a performance metric in the evaluation of the display quality of recovered images. We first formulate the problem as a mathematical optimization model in order to maximize the contrast of recovered images that are subject to density-balance and blackness constraints. We then develop a simulated-annealing-based algorithm to solve this problem. Furthermore, we try to promote the contrast by slightly relaxing the density-balance constraint. The experimental results show that the proposed optimization-based approach significantly outperforms previous methods in terms of both the pixel expansion factor and the display quality of recovered images.

Conventional visual cryptography (VC) suffers from a pixel-expansion problem, or an uncontrollable display quality problem for recovered images, and lacks a general approach to construct visual secret sharing schemes for general access structures. We propose a general and systematic approach to address these issues without sophisticated codebook design. This approach can be used for binary secret images in non-computer-aided decryption environments. To avoid pixel expansion, we design a set of column vectors to encrypt secret pixels rather than using the conventional VC-based approach. We begin by formulating a mathematic model for the VC construction problem to find the column vectors for the optimal VC construction, after which we develop a simulated-annealing-based algorithm to solve the problem. The experimental results show that the display quality of the recovered image is superior to that of previous papers.

Visual secret sharing (VSS) scheme is a perfectly secure method to divide a secret image into several noise-like shadow images by splitting a secret pixel into black and white sub pixels. Unlike other secret sharing schemes, the VSS scheme can be easily decoded by the human visual sight when staking shadow images. However, noise-like shadows are unusual and suspected by censors when delivered by e-mail or fax. Also, noise-like shadows are difficult to identify and manage when distributed. The problem was solved by adding the extended capability, a meaningful shadow image, in the so-called extended visual secret sharing (EVSS) scheme. In this paper, we present a new EVSS scheme by using gray and white sub pixels to represent the secret pixel. Our proposed scheme still has the capability of visually revealing the secret image by stacking shadow images without the help of hardware and complex computation. When compared to the previous EVSS scheme, our new scheme has less number of sub pixels to represent a secret pixel and the clearer shadow images. Conventional visual secret sharing schemes generate noise-like random pixels on shares to hide secret images. It suffers a management problem, because of which dealers cannot visually identify each share. This problem is solved by the extended visual cryptography scheme (EVCS), which adds a meaningful cover image in each share. However, the previous approaches involving the EVCS for general access structures suffer from a pixel expansion problem. In addition, the visual cryptography (VC) based approach needs a sophisticated codebook design for various schemes. In this paper, we propose a general approach to solve the above- mentioned problems; the approach can be used for binary secret images in no computer-aided decryption environments. The pro- posed approach consists of two phases. In the first phase, based on a given access structure, we construct meaningless shares using an optimization technique and the construction for conventional VC schemes. In the second phase, cover images are added in each share directly by a stamping algorithm. The experimental results indicate that a solution to the pixel expansion problem of the EVCS for GASs is achieved. Moreover, the display quality of the recovered image is very close to that obtained using conventional VC schemes.

Halftone visual cryptography (HVC) enlarges the area of visual cryptography by the addition of digital half toning techniques. In particular, in visual secret sharing schemes, a secret image can be encoded into halftone shares taking meaningful visual information. In this paper, HVC construction methods based on error diffusion are proposed. The secret image is concurrently embedded into binary valued shares while these shares are halftone by error diffusion-the workhorse standard of half toning algorithms. Error diffusion has low complexity and provides halftone shares with good image quality. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images. Factors affecting the share image quality and the contrast of the reconstructed image are discussed. Simulation results show several illustrative examples.

## III. CONCLUSION

The paper proposes a VSS scheme, (*n*, *n*) - NVSS scheme, that can share a digital image using diverse image media. The media that include *n* - 1 randomly chosen images are unaltered in the encryption phase. Therefore, they are totally innocuous. Regardless of the number of participants *n* increases, the NVSS scheme uses only one noise share for sharing the secret image. Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness, both for shares and for participants. 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 hand-printed images for image-sharing 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 reversible data hiding.

## REFERENCES

**Journal Papers:**

[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 generalthreshold visual cryptography schemes,” IEEE Trans. Inf. ForensicsSecurity, vol. 6, no. 3, pp. 992–1001,* Sep. 2011.

[4]. K. H. Lee and P. L. Chiu, *“Image size invariant visual cryptography forgeneral access structures subject to display quality constraints,” IEEETrans. 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]. 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.

[8]. 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. 16931703,* Nov. 2011.