Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.717 – 721

RESEARCH ARTICLE

Digital Image Sharing Using Visual Cryptography Techniques

Sunil G. Jare

Electronics and TeleComunnication, S.V.C.E.T Pune, Pune University, India

suniljare3@gmail.com

Prof. Manoj Kumar Singh

Electronics and TeleComunnication, S.V.C.E.T Pune, Pune University, India

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 noise-like share is generated based on these natural shares and the secret image. The unaltered natural shares are diverse and innocuous, thus greatly reducing the transmission risk problem. 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

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 pro-tecting 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.

II. EXISTING SYSTEM

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 dis-play 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.

Disadvantages of Existing System:

First, there is a high transmission risk because holding noise-like shares will cause attackers' suspicion and the shares may be intercepted.

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

III. PROPOSED SYSTEM

The proposed NVSS scheme can share a digital secret image over n 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 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.

Advantages of Proposed System:

To reduce the transmission risk, the dealer can choose an image that is not easily suspected as the content of the media (e.g., landscape, portrait photographs, hand-painted pictures, and flysheets). The digital shares can be stored in a participant's digital devices (e.g., digital cameras or smart phones) to reduce the risk of being suspected. The printed media (e.g., flysheets or hand-painted pictures) can be sent via postal or direct mail marketing services. In such a way, the transmission channels are also diverse, further reducing the transmission risk.

IV. RELATED WORK

Fig. 1 shows 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 mean-ingful appearance. The conventional noise-like shares are not friendly [1]–[4]; hence, researchers tried to enhance the friend-liness of VSS schemes for participants [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 images into 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 user-friendly [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 who is not involved in the transmission of the information sus-pects 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 stego-images.

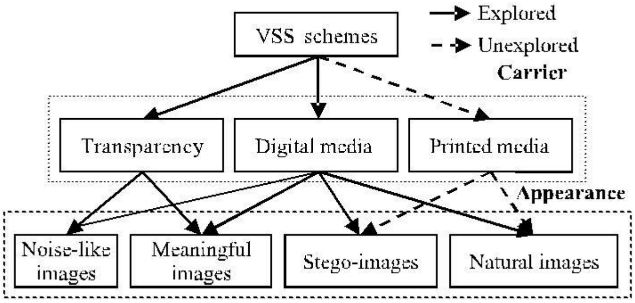

Fig. 1. The classification of the existing VSS research from the viewpoints of carriers.

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.

V. SYSTEM ARCHITECTURE

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

As Fig. 2(a) shows, the encryption process of the proposed (n, n)-NVSS scheme, n 2, includes two main phases: feature extraction and encryption. In the feature extraction phase, 24 binary feature images are extracted from each natural share. The natural shares (N_1,…, $N_{n\ 1}$ include n_p printed images (denoted as ***P***) and n_d digital images (denoted as ***D***), n_p 0, n_d 0, n $_p$ n_d 1 and n n $_p$ n_d 1. The feature images (F_1,…, $F_{n\ 1}$ that were extracted from the same natural image subsequently are combined to make one feature image with 24-bit/pixel color depth.

In the encryption phase, the n 1 feature images (F_1,…, $F_{n\ 1}$ with 24-bit/pixel color depth and the secret image execute the XOR operation to generate one noise-like share S with 24-bit/pixel color depth. 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 the generated share. The n 1 innocuous natural shares and the generated share are n shares in the (n, n)-NVSS scheme. When all n shares are received, the decryption end extracts n 1 feature images from all natural shares and then executes the XOR operation with share S to obtain the recovered image, as shown in Fig. 2(b)

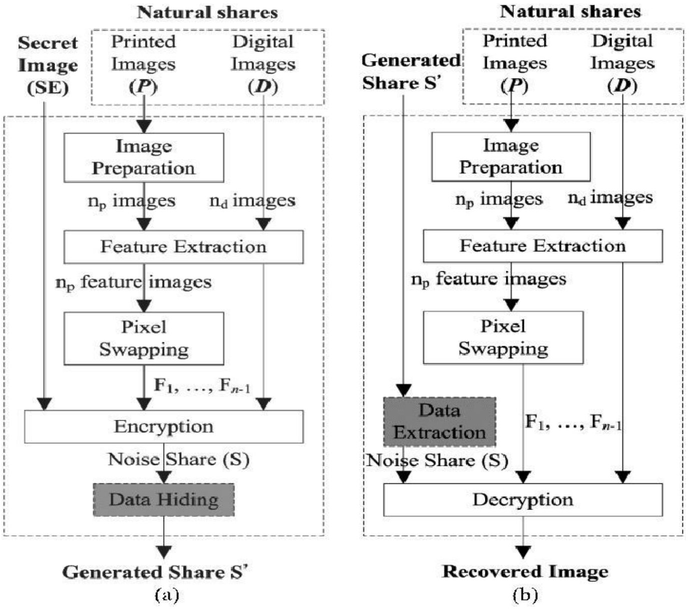

Fig. 2. The encryption/decryption process of the (*n*, *n*)-NVSS scheme: (a) Encryption process, (b) decryption process.

VI. 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 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 Cryp-tology*, 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 algorithm for 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 cryptog-raphy," *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 cryptog-raphy 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 shar-ing 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).*QRCode.com*[Online].Available: http://www.qrcode.com/en/index.html (Accessed).

[20] J. Fridrich, M. Goljan, and D. Soukal, "Perturbed quantization steganog-raphy with wet paper codes," in *Proc. Workshop Multimedia Sec.*, Magdeburg, Germany, Sep. 2004, pp. 4–15.

ACKNOWLEDGEMENT

This is a great pleasure & immense satisfaction to express my deepest sense of gratitude & thanks to everyone who has directly or indirectly helped me in my project work successfully.

I express my gratitude towards project guide **Prof. Manoj Kumar Singh**, & **Prof.P.Balaramdu** Head of Department of Electronics Engineering , Sahyadari College Of Engineering, Pune who guided & encouraged me in my project work in scheduled time. I would like to thanks our **Principal Dr. Zope Sir**, for allowing us to pursue my project in this institute.

Thank you,
Sunil Jare.