DIGITAL DATA FRIEND: A Secure Framework for sharing data using Diverse Media and image Encryption

Mr. Ashish Singh, Mr. Ajay Gupta
Computer Engineering
Institute of Knowledge college of Engineering, Pune, 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. We also added alpha channel watermarking to check whether the image pixels has been altered by the unauthorized person during transmission. Here we store extra 8-bit for the alpha channel value which is average of R, G and B. Receiver need to compare that 8 bit value after transmission with the original value.**

***Index Terms*— Visual secret sharing scheme, extended visual cryptography scheme, natural images, transmission risk.**

I. INTRODUCTION

VISVAL 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]. 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 However, the stego-images still can be detected by steganalysis methods. 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* - 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. For example, assume a dealer selects *n* -1 media as natural shares for sharing a secret image. 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. 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

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 meaningful appearance. The conventional noise-like shares are not friendly [1]–[4]; hence, researchers tried to enhance the friendliness 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. Several papers investigated meaningful halftone shares [8] 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.

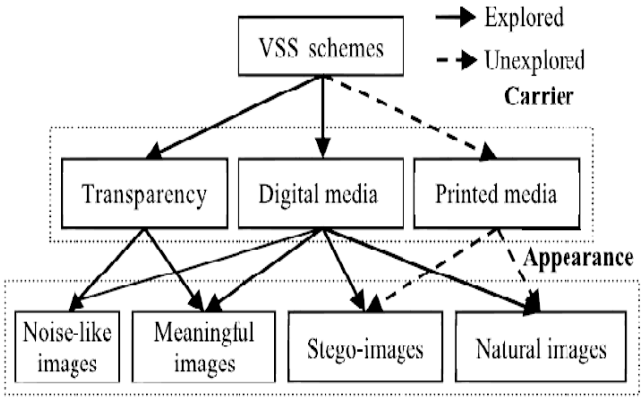

Fig. 1. The classification of the existing VSS research from the viewpoints of carriers.

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. 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. 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. Recently, Chiu et al. tried to share a secret image via natural images. 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 to promote its practicability and explore the possibility for adopting the unaltered printed media as shares.

III. DISCUSSION

a) Key Generation

We use grayscale algorithm and Jarvis thresholding algorithm. Thresholding is the simplest method of image segmentation. From a grayscale image, thresholding can be used to create binary images i.e. image with only black or white colors. It is usually used for feature extraction where required features of image are converted to white and everything else to black. (or vice-versa) Online Guessing Attacks. In Jarvis march we don't need to set the threshold value manually instead threshold value is set by pixels by considering nearby pixels value.

b) Stegnography

The term "Steganography" comes from Greek and means "covered writing." In comparison, "cryptography" means "secret writing" in the original Greek; recognize the distinction? Awareness of the differing definitions helps understanding the difference. While both evoke "secret communications," with steganography, you don't need any key or a key distributor in pure steganography. The basic idea of steganography is to employ "covered writing," meaning to hide your secret message in plain sight, as it were, within a simple/regular message so that other parties are not aware of the communication. In this the data is hidden with the LSB replacement algorithm.

c) Watermarking

We also added alpha channel watermarking to check whether the image pixels has been altered by the unauthorized person during transmission, here we store extra 8-bit for the alpha channel value which is average of R, G and B. Receiver need to compare that 8 bit value after transmission with the original value.

c)Encryption Chaos sequence generation:

We use Henon map equation for this to generate the key. Without this key the unauthorized person can not get the secret original image.

d) Hide the Noise-Like Share

In the proposed NVSS scheme, a dealer can hide the generated share by using existing steganography. The amount of information that can be hidden in a cover image is limited and depends on the hiding method. To embed the generated share in a cover image, generally the dimension of the cover image must be larger than that of the secret image. If the share can be hidden in the cover image and then can be retrieved totally, the secret image can be recovered without distortion. We leave the details of using steganography to hide shares to the reader; our focus is on how to hide the share in printed media.

IV. PROPOSED SYSTEM

NVSS scheme can be extended to the (n, n)-NVSS scheme by adopting n - 1 natural images for generating n - 1 secret keys. In such a way, the visual secret image can be shared by the n - 1 natural images as well as the generated share. proposed (n, n)-NVSS scheme adopts arbitrary $n - 1$ natural shares and one generated share as media to share one digital true color secret image that has 24-bit/pixel color depth. The objective of this study is to reduce the transmission risk of shares by using diverse and innocuous media. We make the following assumptions:

1. When the number of delivered shares increases, the transmission risk also increases.
2. The transmission risk of shares with a meaningful cover image is less than that of noise-like shares.
3. The transmission risk decreases as the quality of the meaningful shares increases.
4. The natural images without artificially altered or modified contents have the lowest transmission risk, lower than that of noise-like and meaningful shares.
5. The display quality of distortion-free true-color images is superior to that of halftone images.

In the 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. The innocuous natural shares can be delivered by participants who are involved in the NVSS scheme, by the owners of the photographs, or via public Internet. Because the natural shares are not altered, it is likely that they will not arouse suspicion during transmission. Even if the natural shares

are intercepted, it will not be possible to verify that there is any hidden information in the images before reaching the decryption threshold. In such a scenario, the transmission of the innocuous
natural shares is more secure than the transmission of shares in another form, such as noise-like or meaningful shares. Another share, which is generated by the secret image and features that are extracted from n - 1 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, based on Assumption 1, the transmission risk of the conventional VSS schemes increases rapidly.

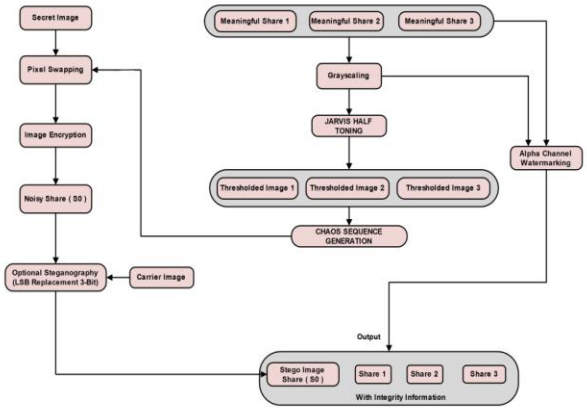

Fig. 2. Proposed system architecture.

On the contrary, regardless of the increasing number of shares, the proposed NVSS scheme always requires only one generated share. Because the natural images have very high security, even though the amount of innocuous natural shares is also proportional to n, the transmission risk of the proposed scheme will increase very slightly as n increases. In the existing VSS schemes, the types of shares include noise-like shares, shares with binary cover images, and shares with halftone cover images; the latter has the best display quality among the above-mentioned types of shares. Furthermore, the display quality of the proposed true-color natural.
Shares is superior to that of shares with halftone cover images. Based on Assumptions 2 and 3, the transmission risk of the true-color natural shares is the lowest among the existing approaches. Based on Assumptions 4 and 5, the proposed (n, n)-NVSS scheme delivers n - 1 unaltered natural shares that have a very low transmission risk, this property greatly reduces the transmission cost of delivering n -1 natural shares of the scheme. Compared with traditional (n, n)-VSS schemes, which must carefully deliver n noise-like shares, the proposed (n, n)-NVSS scheme must deliver only one generated share in a high-security manner. When the transmission cost is limited, the proposed scheme using unaltered natural shares can greatly reduce transmission risk.

V. 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 .This study proposes a useful concept and method for using unaltered images as shares in a VSS scheme.

REFERENCE

[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 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 cryptography," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453, Aug. 2006. [9] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.
[10] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. Image Process.*, vol. 11, no. 6, pp. 585–595, Jun. 2002.
[11] Z. M. Lu, D. G. Xu, and S. H. Sun, "Multipurpose image watermarking algorithm based on multistage vector quantization," *IEEE Trans. Image Process.*, vol. 14, no. 6, pp. 822–831, Jun. 2005.
[12] M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," *IEEE Trans. Multimedia*, vol. 6, no. 4, pp. 528–538, Aug. 2004.
[13] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," *IEEE Signal Process. Lett.*, vol. 13, no. 12, pp. 741–744, Dec. 2006.
[14] J. Tang, S. Yan, R. Hong, G. Qi and T. Chua, "Inferring Semantic Concepts from Community-Contributed Images and Noisy Tags," in *ACM Multimedia*, 2009, pp. 223–232.
[15] J. Tang, H. Li, G. Qi and T. Chua, " Image Annotation by Graph-Based Inference With Integrated Multiple/Single Instance Representations," in *IEEE Trans. Multimedia*, 2010, vol. 12, no. 2, pp. 131–141, 2010.
[16] K. Lerman, A. Plangprasopchok, and C. Wong, "Personalizing image search results on flickr," *CoRR*, vol. abs/0704.1676, 2007.
[17] 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.
[18] 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.