International Journal of Research
eISSN: 2348-6848 & pISSN: 2348-795X *Vol-5 Special Issue-13*
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

Secure Sharing Of Digital Image Using Diverse Image Media

Miss. Punam Isankar
(M. Tech. Student)
isankarpunam10@gmail.com

Prof. Snehal Palliwal
(Assistant Professor)
snehal.ece@tgpcet.com

Prof. Nagma Sheikh
(Assistant Professor)
nagma.ece@tgpcet.com

***Abstract**:*

Conventional visual secret sharing (VSS) schemes hide secret images in shares that are either printed on trans-parencies 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. 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.

1. 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.

In this paper, we develop efficient encryption/decryption algorithms for the (*n*, *n*) -NVSS scheme. The proposed algo-rithms 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 remainder of this paper is organized as follows. Section II reviews the research framework. In Section III, we present the proposed NVSS scheme. The encryp-tion/decryption algorithms are proposed in Section IV. In Section V, the security and performance of the proposed NVSS scheme are evaluated by experiments. Finally, we present the conclusions of this work in Section VI

2. 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. 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].

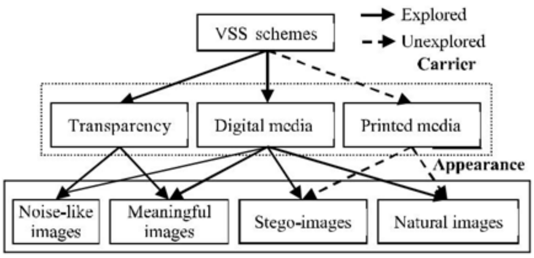

Fig. 1. The classification of the existing VSS research from the viewpoints of carriers.

3.The Proposed Scheme

A. Background

In cryptography, the one-time pad (OTP), which was proven to be impossible to break if used correctly, was developed by Gilbert Vernam in 1917. Each bit or character from the plaintext is encrypted by a modular addition (or a logical XOR operation) with a bit or character from a secret random key of the same length as the plaintext resulting in a ciphertext. The ciphertext was sent to a receiver; then, the original plaintext can be decrypted in the receiver side by applying the same operation and the same secret key as the sender used for encrypting the ciphertext.

In this study, we adopt the notion of the OTP technique to share digital visual secrets. Instead of generating a secret ran-dom key, we extract the secret key from an arbitrarily picked natural image in the 2, 2 -NVSS scheme. The natural image and the generated share (i.e., ciphertext) were distributed to two participants. In decryption process, the secret key will be extracted again from the natural image and then the secret key as well as the generated share can recover the originalsecret image. The 2, 2 -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.

B. Assumptions

The 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 mod-ified 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. 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. Further-more, 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.

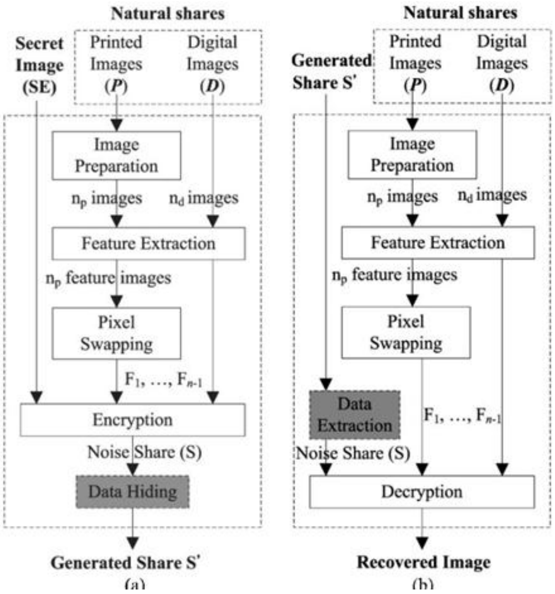

Fig.2. the encryption/decryption process of the (n,n) NVSS process a) encryption process B) decryption Process.

C. The Proposed n, n -NVSS Scheme

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 ($N_1,\ldots, N_{n\ 1}$ 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 ($F_1,\ldots, F_{n\ 1}$ that were extracted from the same natural image subsequently are combined to make one feature image with 24-bit/pixel color depth.

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). Each module in Fig. 2 is described in the following sections.

4. The Proposed Algorithms

A. Feature Extraction Process

This section first describes the feature extraction module that extracts feature images from the natural shares. The mod-ule which is the core module of the feature extraction process is applicable to printed and digital images simultaneously. Then, the image preparation and the pixel-swapping modules are introduced for processing printed images.

1) The Feature Extraction Module

As Fig. 3 shows, the feature extraction module consists of three processes—binarization, stabilization, and chaos processes. First, a binary feature matrix is extracted from natural image N via the binarization process. Then, the stabi-lization balances the occurrence frequency of values 1 and 0 in the matrix. Finally, the chaos process scatters the clustered feature values in the matrix. In the binarization process, the binary feature value of a pixel can be determined by a simple threshold function *F* with a set threshold. To obtain an approximate appearance probability for binary values 0 and 1, the median value M of pixels in the same block is an obvious selection as the threshold.

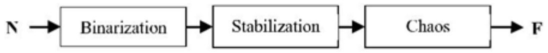

Fig. 3 . The Block Dig. Of Feature Extraction

2) The Image Preparation and Pixel Swapping Processes

The image preparation and pixel swapping processes are used for preprocessing printed images and for post-processing the feature matrices that are extracted from the printed images. The printed images were selected for sharing secret images, but the contents of the printed images must be acquired by computational devices and then be transformed into digital data.

The suggested flow of the image preparation process is shown in Fig. 4. In the first step, the contents of the printed

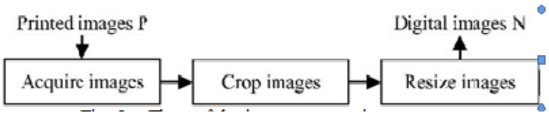

Fig.4. Flow Of The Image Preparation Process.

images can be acquired by popular electronic devices, such as digital scanners and digital cameras. To reduce the difference in the content of acquired images between the encryption and decryption processes, the type of the acquisition devices and the parameter settings (e.g., resolution, image size) of the devices should be the same or similar in both processes. The next step is to crop the extra images. Finally, the images are resized so they have the same dimensions as the natural shares.

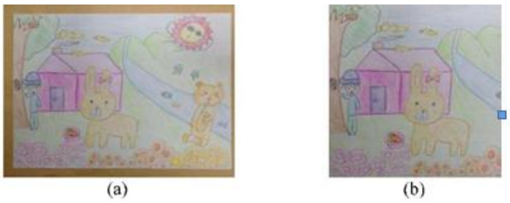

Fig. 5 a) A Hand printed Picture was captured by the digital camera on the iPhone 4s B) The Resultant Picture.

An example of the image preparation process is illustrated in Fig. 5. The hand-painted picture is drawn on A4 paper. First, the picture is captured using a popular smart phone, Apple iPhone 4S, as shown in Fig. 5(a). The picture then is processed using the Paint application in Microsoft Windows 7. Eventually, the picture is cropped and resized as a rectangular image as shown in Fig. 5(b). The resultant picture is used in the experiments in the subsequent section.

Because of the distortions introduced into the acquired digital images during the image preparation process, different distortions are caused by each the encryption process and the decryption process. In other words, the acquired digital images in the encryption and decryption phases are not the same. These distortions result in noise that appears in the recovered images. When a large amount of noise clusters together, the image is severely disrupted, which may makes it impossible for the naked eye to identify it. The pixels-wapping process is used to cope with this problem.

B. Encryption/Decryption Algorithms

The proposed (*n, n*)-NVSS scheme can encipher a true-color secret image by *n* 1 innocuous natural shares and one noise- like share. For one image, we denote a bit with the same weighted value in the same color as a bit plane; then a true color secret image has 24 bit-planes. Thus, the feature images and the noise-like share also are extended to 24 bit-planes. Each bit-plane of a feature image consists of a binary feature matrix that corresponds to the same bit-plane as the secret image.

Before encryption (resp. decrypt) of each bit-plane of the secret image, the proposed algorithm first extracts *n* 1 feature matrices from *n* 1 natural shares. 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.

C. Hide the Noise-Like Share

In this section, steganography and the Quick-Response Code (QR code) techniques are introduced to conceal the noise-like share and further reduce intercepted risk for the share during the transmission phase.

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 using QR code technology.

5. 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,p.p 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). *QR Code.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.