International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Survey on: Secure Data Transmission by images.

Mr. Rishabh Badnore [1], Mr. Tejas Pote [2], Mr. Raj Gaikwad [3], Mr. Umesh Chaudhari [4] , Mr. A. N. Bandal [5]

[1,2,3,4,5]*Department of Computer Engineering, STES' SINHGAD INSTITUTE OF TECHNOLOGY, Lonavala Savitribai Phule Pune University, Maharashtra, India*

ABSTRACT: *Conventional visual secret sharing (VSS) schemes generate noise-like random pixels on shares to hide secret images. However, 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 participant and the images growing, in turn growing the chance 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. 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 overcome this problem we have proposed a natural based VSS scheme which shares a secrete image via different carrier media to protect to protect the secret and the participants during the transmission phase. The projected (n, n) - NVSS system can split one digital secret image over n^1 arbitrary selected natural images and one noise-like image share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. The noise share is generate based on natural images and secrete images huge reduces the transmission problem. We also give possible ways to hide the noise like share to reduce the transmission problem for the share. Experimental results point to that the proposed approach is an outstanding solution for solving the transmission risk problem for the VSS schemes.*

Key Words: Visual secret sharing scheme, extended visual cryptography scheme, Natural images, Transmission risk.

1. INTRODUCTION

Visual cryptography is a technique that encrypts a share image into n shares. Anyone who is having less than n shares cannot get any information about the secrete image. Collecting all images or stacking the n shares reveal the information about secrete image which can be recognized by the human visual system. Secret images can be of any type like images, handwritten, documents, photograph, and other.

Conventional shares, which consist of many meaningless and random pixels, which satisfy the security requirement for protecting secret contents [1], but they suffers from main two drawback: first during the transmission, because holding a noise like share cause attackers and shares may be intercepted which causes transmission failure. Second, the meaningless shares are not user friendly. Because as the number of shares increases, it become more difficult to identifying the shares. Previous research into Extended Visual Cryptography Scheme or VSS scheme provided effective solution related to management issues [10]. By using steganography techniques secret images can be cloaked in cover images which are halftone gray images and true color images [9]. For this reasons the existing VSS schemes still must be investigated for sinking the transmission risk problem.

In this study, we introduce a VSS scheme or natural image based VSS scheme to minimize the interception risk during transmission phase. Usual VSS schemes use a unity carrier or digital image for sharing images which confines the practicality of VSS schemes. In the given process we explore the possibility of using diverse media for sharing digital images. The carrier media use in this process contains digital images, printed images, hand painted picture and so-on.

The NVSS process scheme can share a digital secret image over n-1 random natural images and one share. Instead of varying the content of the natural images, the proposed approach extracts features from each natural share. These unchanged natural shares are totally safe, thus greatly tumbling the interception probability of these shares. The generated image that is noise can be secreted by using data hiding technique to amplify the security level during the transmission phase.

In this paper, we expand efficient encryption/decryption algorithms for the (*n, n*) -NVSS scheme. The projected algorithms are relevant to digital and printed media. The possible ways to conceal the generated

share are also discussed. The NVSS project not only has a high level of user responsiveness and manageability, but reduces transmission risk and enhances the security of contributor and segments.

1.1 Overview

Our second section Author includes overview of our survey with various type of operations and technology.

1.1 LITERATURE SURVEY

Author/citation	Type of study	Limitations
Pei-Ling Chiu and Kai-Hui Lee.	In cryptography, hide the secret images and recovered images as original format. In visual secret sharing study in recovered original images.	Visual cryptography recovered quality images.
Kai-Hui Lee and Pei-Ling Chiu	To study in Binary secret images in non-computer aided decryption environments.	Pixel-expansion problem.
InKoo Kang, *Member, IEEE*, Gonzalo R. Arce, *Fellow, IEEE*, and Heung-Kyu Lee, *Member, IEEE*	The extended visual cryptography scheme for pixel expansion problem.	Pixel-expansion problem.
Color meaningful shares, digital halftoning, error diffusion, secret sharing, visual cryptography	A color secret message into color halftone image shares for visual secret. original pixel values the same before and after encryption	pixel expansion in the size of encrypted shares
Feng Liu and Chuankun Wu	able to improve the secret image without any cryptographic	pixel expansion in EVCS
Zhongmin Wang, *Student Member, IEEE*, Gonzalo R. Arce, *Fellow, IEEE*, and Giovanni Di Crescenzo	embedded into binary valued shares with halftoned by error	contrast loss in the reconstructed images
Xiaotian Wu, Duanhao Ou , Qiming Liang , Wei Sun	Embedded images with recovere original images.	To identify secret image encryption.
Cheng Guo a, Chin-Chen Chang b,c,⇑, Chuan Qin	a multi-threshold secret image sharing scheme.	Image sharing groups with multi-threshold access structure
Tzung-Her Chen and Kai-Hsiang Tsao	RGVSS must be designed in VS	pixel expansion

1.2 RELATED WORK

Presented study focuses only on with transparencies or digital media as carriers for a VSS scheme. The simplicity shares have either a noise-like or a meaningful form. The conservative noise-like shares are not gracious [2]; hence, researchers tried to improve the friendliness of VSS schemes for participant [3]. Normally, easy and significant coat images are added to noise-like shares for detection, making conventional VC schemes more friendly and convenient. Though, the EVCSs decrease the display quality of the recovered images. Research has focused on color and gray-level secret images to build up a user-friendly VSS scheme that adds cover up images into the meaningless shares [10]. To digital images share, VSS techniques use digital media as mover, which makes the form of the shares more variable and more user friendly [10]. Several investigated papers shows meaningful halftone shares [5] and emphasized the excellence of the shares extra than the class of the recovered images. These studies had grave side effects in terms of pixel expansion and deprived display excellence for the improved images, though the display quality of the shares was improved. Hence, researchers create a tradeoff between the

quality of the shares, the quality of the recovered images, and the pixel growth of the images. In an additional research bough, researchers used steganography technique to secret images in wrap images [9]. Steganography is the method of hiding information and making the message unseen. So, the concealed information and its carrier can be secluded. Steganography has been use to hide digital shares in VSS schemes. The shares in VSS schemes are fixed in cover images to make stego-images. Although the shares are covered totally and the stego-images have an elevated level of user friendliness, the communal information and the stego-images stay intercepted risks during the broadcast stage. Recently, Chiu et al. tried to share a secret image via customary images. This was a first effort to share images via usual images though, this work may undergo a problem the textures of the usual images could be disclosed on the share. Furthermore, printed images cannot be used for distributing images in the preceding scheme. So far, distributing visual secret image via unchanged printed media leftovers an open problem. In this revise, we make an addition of the preceding work in to encourage its viability and discover the option for adopting the unaltered printed media as shares.

1.3 ALGORITHM

In secret image sharing has different algorithm are used.

1.3.1 Feature Extraction

The feature extraction has detect the images all things. It has we get pixel values which has total height* width pixel values. The gray scale image is important because we have to get original pixel images called as background images.

1.3.2 NVSS

Natural images visual secret has set of different algorithm.it has divide the natural images in different share. These every share are make to one image and hide the secret image behind natural image. The algorithm show in mathematical format.

1.4 Mathematical Module

$$Imag = \int_0^n secret\ imag + \int_0^n Natural\ imag \qquad (1)$$

User has sets to secret and natural images sets.

$$val(RGB) \in Imag \qquad (2)$$

$$Output = cover \oplus Imag \qquad (3)$$

Final output generated by XOR operation using cover image and Image sets.

2. CONCLUSION

The paper propose a VSS scheme, (*n, n*)-NVSS scheme, that can share a digital image using diverse image media. The media that include *n*1 arbitrarily selected images are unchanged in the encryption stage. Therefore, they are totally inoffensive. Despite of the number of participant *n* increases, the NVSS scheme uses only one noise share for sharing the secret image. Compared with obtainable VSS schemes, the projected NVSS scheme can efficiently decrease broadcast threat and give the maximum level of user sociability, for both shares and for participants. This revise provides four main contributions. First, this is the first effort to share images via heterogeneous carriers in a VSS scheme. Second, we productively set up hand-printed images for images-haring schemes. Third, this study proposes a practical concept and technique for using unchanged images as shares in a VSS scheme. Fourth, we build up a technique to amass the noise share as the QR code.

3. REFERENCES

1. 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.

2. 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.

3. 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.

4. 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.

5. F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 2011.

6. 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.

7. 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.

8. 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.

9. 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..

10. 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..