© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Digital Image Sharing by Diverse Image Media

Leena Slochana V, Malavika G, P. Vijayaraghavan
Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, Tamilnadu, 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.

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. METHODS AND MATERIAL

A. Related Work

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; hence, researchers tried to enhance the friendliness of VSS schemes for participants. Generally, simple and meaningful cover images are added to noise-like shares for identification,

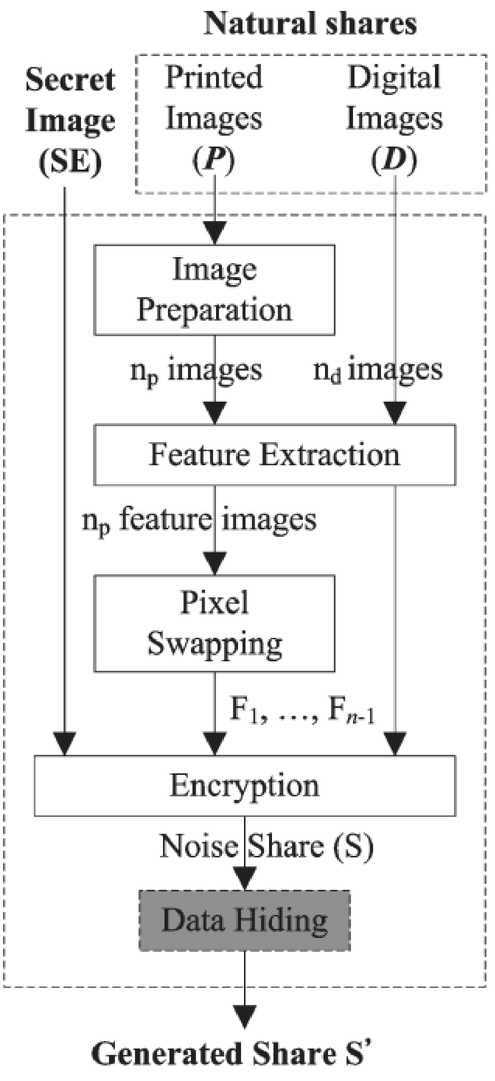
IJSRSET152261 | Received: 16 March 2015 | Accepted: 28 March 2015 | March-April 2015 [(1)2: 246-249]

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. To share digital images, VSS schemes use digital media as carriers, which makes the appearance of the shares more variable and more users friendly. Several papers investigated meaningful halftone shares 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 trade-off between the quality of the shares, the quality of their covered images, and the pixel expansion of the images.

B. **Proposed Work**

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 ciphertext1.



Algorithm

```
Algorithm FE()
Input : N,b,Pnoise
Output :F
1)  1.Divide N into blocks with bxb pixels
2)  2.For each block repeat step 3-11
3)  3.for all x1<=x<=xb,y1<=y<=yb,calculate H^x,y
    by Eqn.(1)
4)  4.Calculate M
5)  5.For all <=x<=xb,y1<=y<=yb,Determinbe f^x,y
    by Eqn.(2)
6)  6.Calculate Qs by Eqn(3)
7)  7.Randomly select Qs pixels where f^ x,y=1 and
    H^ x,y=M, let f^x,y<-0
8)  8.Calculate Qc by Eqn(4)
9)  9. Randomly select Qc candidate pixels wheref
    ^x,y=1
10) 10. Randomly select Qc candidate pixels wheref
    ^x,y=0
```

11) 11.Alter all values of f ^x,y that were selected in steps 9 and 10
12) 12.Output F.

The modules descriptions are as follow:

Image Selection and Image Preparation

Initially Secret Image and Natural Images has been Chosen Natural Images would be Painted and Digital Images. The image preparation processes are used for preprocessing printed images and for post-processing the feature matrices that are extracted from the printed images. The contents of the printed images can be acquired by popular electronic devices, such as digital scanners and digital cameras.

Feature Extraction and Encryption Process

This module describes the feature extraction process that extracts feature images from the natural shares. The module which is the core module of the feature extraction process is applicable to printed and digital images simultaneously Assume that the size of the natural shares and the secret image are w * h pixels and that each natural share is divided into a number of b *b pixel blocks before feature extraction starts.

QRCODE Generation and Network Sharing Process

In this module 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. The Encrypted Image Would is converted in to binary numbers. The Whole binary wouldn't possible to embed into QRCODE.

Encrypted Image Extraction and Decryption process

After Receiver Receives all the Images has to scan the QRCODE by using Smart Phone which contains QRCODE READER Application. When the Scanning process done Receiver got all the keys for splatted binary values. Then Send the key values to Receiver Application by Socket Communication. By using that Keys Receiver has to extract the splatted binary numbers from Collection Framework then Form the Encrypted Images. When Receiver Form the Encrypted Images Decryption Process has be done by similar to Encryption method what Sender done.

Decryption: Input images include *n* -1 natural shares and one noise-like share. The output image is a recovered image.

III. RESULTS AND DISCUSSION

A. Experiment I

This subsection demonstrates the performance of the proposed NVSS scheme in the case of a 4, 4-NVSS scheme. Three natural shares in the experiments. The secret image SE_1 is the well-known picture—"Lena". All natural shares are taken from travel photos of tourists. These images are in true color format and their dimensions are 512 512 pixels. Parameters b and P_{noise} are set to 8 and 0.5, respectively.

B. Experiment II

This experiment evaluates the performance of the proposed NVSS scheme for sharing color and binary secret images by diverse shares. The shares used in the 5, 5-NVSS scheme include three digital images and one hand-painted picture.

The digital images and the color secret image are the same as those used in Experiment I. The hand-painted picture is drawn on A4 paper. The picture is processed by the image preparation process to obtain two digitized shares, one for the encryption process and one for the decryption process.

C. Experiment III

This subsection demonstrates the performance of the 4, 4-NVSS scheme by using the QR code to hide the noise share. Second, we explore the capability of various versions of the QR code to hide the noise share. The secret image used in this experiment is a binary image of size 256 256 pixels.) Demonstrate the implementation results of a noise share and its corresponding QR code (version 25) and the recovered image in the 4, 4-NVSS scheme.

IV. CONCLUSION

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.

Future Work

After Decryption process has been done, Recovered Image will be formed. By using comparing the pixel values of Secret image and Recovered image we can found there is no Pixel Expansion or Pixel corruption in the Recovered image. She is no change between Secret image and Recovered image.

V. REFERENCES

[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] 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.

[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.