"Transfer of Digital Image by Using Divers Image Media for Security Purpose"

Mangla S. Dantulwar, M. Tech. (EC),
priyadarshni Bhagwati College of Engineering,
Nagpur maharastra, India
manglamungilwar@gmail.com

Puja V. Gawande Assistant Professor
priyadarshni Bhagwati College of Engineering,
Nagpur maharastra, India
p.gawande@gmail.com

Abstract: Transfer of digital image through computer aided environment is a big problem today. visual secret sharing (VSS) schemes is used to hide secret images in shares transparencies or printed form are encoded and stored in a digital form. The drawback of VSS schemes suffers from a transmission risk problem while sharing shares contains in Secret Images. To avoid this problem, we proposed a natural-image-based VSS scheme (NVSS scheme) that shares secret images through various media to protect the secret and the participants during the transmission. The proposed (n, n)- NVSS scheme it has used to 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 painted pictures in digital form or in printed form. The noise-like share is developed based on these natural shares and the secret image. We also introduced possible ways to hide the noise like share to reduce the transmission risk problem for the share.

Keywords: Extended visual cryptography scheme, natural images, transmission risk. Visual secret sharing

I. INTRODUCTION

Visual Cryptography (VC) is a traditional method that encrypts a secret image into n shares, in which each participant holding one or more shares. One who holds less than n shares cannot give any information about the secret image? Secret images can be of numerous types: images, handwritten documents, photographs. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme. Sharing visual secret images in computer-aided environments has become an important issue today. It has two disadvantages: 1) there is a high transmission risk 2) the meaningless Shares are not user friendly. The Extended Visual Cryptography Scheme (EVCS) is user-friendly VSS scheme provided some better solutions to overcome with the associate issue. The proposed scheme can share a digital secret image over n-1 arbitrary natural images. These unaltered natural shares are totally innocuous, thus greatly reducing the interception probability of these shares. 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 increses the security of participants and shares invoved in it.

II. II. THE PROPOSED SCHEME

A. Background In visual cryptography, the one-time pad (OTP) is used , which proved to be impossible to break if used correctly, was developed Conventional visual secret sharing (VSS) schemes hide secret images in shares that are 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 increased interception risk during transmission of the shares. Hence, VSS schemes undergo a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme. To solve this problem, we proposed a natural-image-based VSS scheme (NVSS scheme) that shares secret images through different media to protect the secret and the participants during the transmission phase. The proposed (n,n)- NVSS scheme can share single 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 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 unchanged natural shares are diverse and innocuous, thus greatly reducing the transmission risk problem. We also propose different possible ways to hide the noise-like share to reduce the transmission risk problem for the share.

2.1 Background

Recover the original secret image. In cryptography, the one-time pad (OTP), is used to protect data from unwanted user. The vss scheme is similar to the OTP encryption system. In a VSS scheme, the secret random key and the cipher text that can be used as two shares in the scheme were given to two participants who participate in the scheme. Instead of generating a secret random key, we extract the secret key from an natural image in the NVSS scheme. The natural image and the generated share were distributed to two participants. In decryption process, the secret key will be taken out again from the natural image.

2.2. The Proposed (N, N)-Nvss Scheme

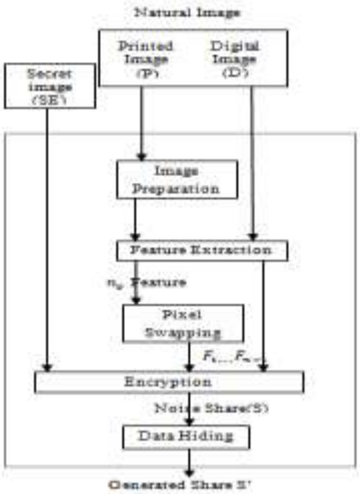


Figure 1: Encryption process

As Fig. 1(a) shows, the encryption process of the proposed (*n*, *n*)-NVSS system there are two main phases: feature extraction and encryption. The natural shares (N1, … , N*n-1*)include np printed images(denoted as ***P***) and nd digital images (denoted as ***D***), np>=0,nd>= 0, np+nd>=1 and *n*=np+ nd+ 1. The feature images (F1,…, Fn -1) were extracted from the same natural image

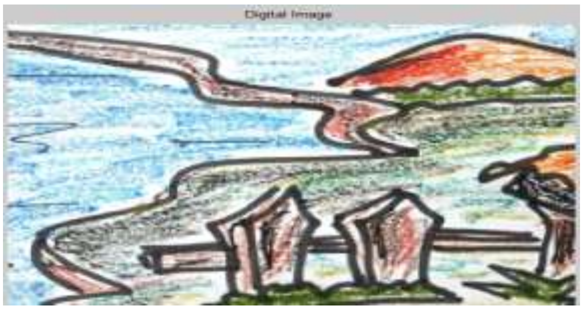
III. III.THE PROPOSED ALGORITHMS

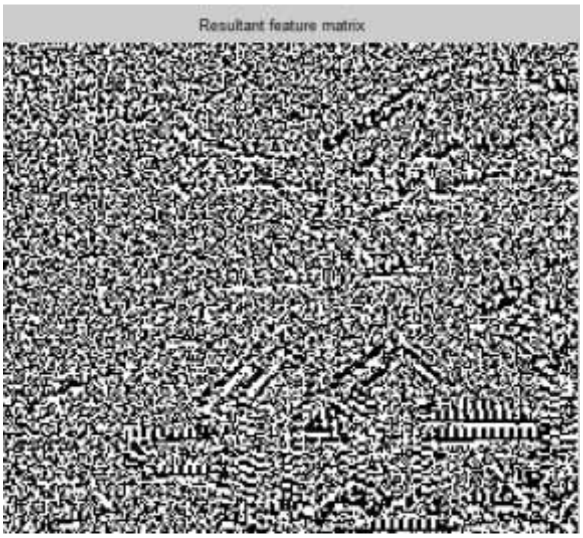
3.1 Feature Extraction Process

This process shows how to extract feature module which further extract feature image from the natural image.

3.1.1 The feature Extraction Module

Consider that the size of the natural shares and the secret image are w*h pixels and each natural share is divided into a number of b*b pixel blocks before feature extraction starts. Feature extraction module has three processes— binarization, stabilization, and chaos processes. In the binarization process binary feature matrix is extracted from natural image N. Then, the stabilization maintains the occurrence frequency of values 1 and 0 in the matrix. Finally, the chaos process scatters the clustered feature values in the matrix. To obtain an approximate appearance probability for binary values 0 and 1, the median value M of pixels in the same block is select as the threshold. Hence, for each block, the extraction function of pixel (x, y) of N is given as follows: fx ,y=F(Hx ,y)= 1, $Hx ,y \geq M$, 0, $otherwise$.





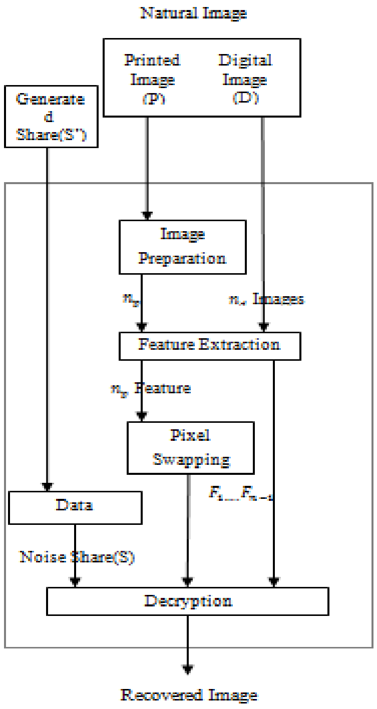


Figure 2: Decryption process

The use of stabilization process is to balance the number of black and white pixels of an extracted feature image. The number of unbalanced black pixels Qs can be calculated by $Qs= f, \forall\ x1 \le x \le x\ b\ \forall y1 \le y2 \le yb$ (2) The chaos process is used to eliminate the texture that comes on the extracted feature images and the generated share.

3.1.2 The Image Preparation and Pixel Swapping Process

Image preparation and pixel swapping processes are used for preprocessing printed images and for post processing of the digital image respectively. The printed images will be used for sharing secret images, but the contents of the printed images will be owned by computational devices and then transformed into digital data.

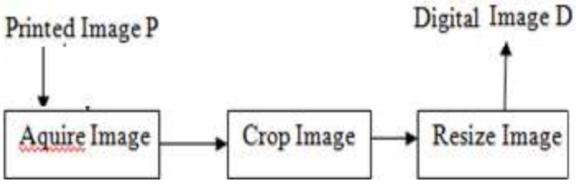


Figure 3: Flow of the image preparation process.

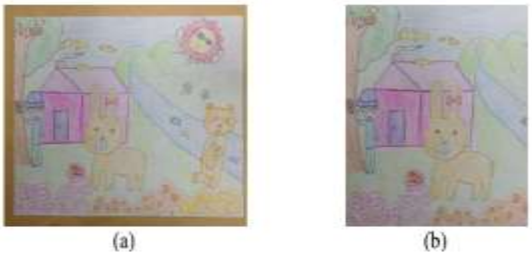


Fig. 3 : An example of the image preparation

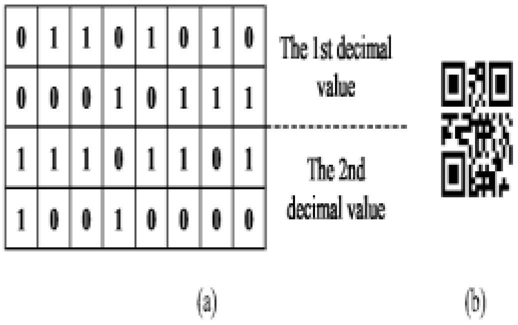
To decrease the difference in the content of the acquired images between the encryption process image the content of the image is owned by the electronic devices such as phone or digital camera. To reduce the differences between the content of encryption and decryption process images, the type of acquisition devices and parameter setting should be same or similar in both process. Then we should crop the extra image before resizing the image for the same dimension of the natural image.

3.2Encryption/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. Before encryption (resp. decrypt) of each bit-plane of the secret image, encryption 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 on the 24 bit-planes. **Encryption:** Input images include *n* -1 natural shares and one secret image. The output image is a noise-like share. **Decryption:** Input images include *n* -1 natural shares and one noise-like share. The output image is a recovered image.

3.3 Hide the Noise-Like Share

In this system steganography and the Quick-Response Code (QR code) methods are introduced to conceal the noise-like share and further decrease the intercepted risk for sharing during the transmission period. In the proposed NVSS scheme, a dealer can hide the generated share by using the available steganography. The information that can be hidden in a cover image is limited to a certain extent and it depends on the hiding method used. To embed the generated share in a cover image, 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 obtained totally, the secret image can be recovered without any distortion.. The QR code, which encodes meaningful information in both the dimensions and in the vertical and horizontal directions, is capable to carry up to several hundred times the amount of data carried by barcodes. The code is printed on physical material and can be read and decoded by various devices, such as barcode readers and smart phones. It is this ubiquitous nature of the QR code that makes it important for use as a carrier of secret communications.



0	1	1	0	1	0	1	0
0	0	0	1	0	1	1	1
1	1	1	0	1	1	0	1
1	0	0	1	0	0	0	0

Fig 4: An Example of the Feature Matrix to the QR Code Encoding

The amount of data that can be stored in the QR code. Encoding process has two steps: First, transform pixels on the share into binary values and give the values in a decimal format second, we encode the decimal values into QR code format. The first Huffman code compression decreases the size of image into a series of bits. The Huffman code then can be use to represent as the series of integers by first padding the Huffman code with zeros to ensure the code can be separated into group of 8 bits. Each of the group is then converted into integers. This is of great use since the QR code is character limited. The decryption phase is opposite the encryption. The natural share can share using the various media such as postal, email, or any other media. Retrieve the information from the image and the QR code. Transform the numeric value into binary form. Convert the binary string into resultant matrix. From the resultant matrix the corresponding secret image can retrieve.

IV. CONCLUSION

The paper proposes a VSS scheme, (n, n)-NVSS scheme, that can share a digital image using diverse image media. The use of diverse image media is to protect from the unknown attackers. The media that include n-1 randomly chosen images are unchanged in the encryption phase and then feature of the secret image and the randomly chosen images are taken accordingly. Therefore, they are totally innocuous. The number of participants does not involve in share, the number of participants can be increased. Compared with existing VSS schemes, the proposed NVSS scheme can be used to effectively reduce transmission risk and provide the highest level of security, both for shares and for participants. This study provides four major contributions. First, attempt to share images via heterogeneous carriers in a VSS scheme. Second, introduce hand-printed images for images-sharing schemes. Thirdly, it provided very useful and important concept and method for using unaltered images as shares in a VSS scheme. Fourthly, method to store the noise share as the QR code. The proposed work is a better solution for high scale secure communication

REFERENCE

[1] Kai-Hui Lee and Pei-Ling Chiu,‖Digital Image Sharing by Diverse Image Media, ‖ieee transactions on information forensics and security, vol. 9, no. 1, january 2014.

[2] M. Naor and A. Shamir, ―Visual cryptography,‖ in Advances in Cryptology, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[3] Tzung-Her Chen and Kai-Hsiang Tsao,‖ User-Friendly Random-Grid-Based Visual Secret Sharing,‖ ieee transactions on circuits and systems for video technology, vol. 21, no. 11, november 2011.

[4] Kai-Hui Lee and Pei-Ling Chiu,‖An Extended Visual Cryptography Algorithm for General Access Structures,‖ieee transactions on information forensics and security, vol.7, no.1, February 2012

[5] Pei-Ling Chiu and Kai-Hui Lee,‖A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes,‖ieee transactions on information forensics and security, vol. 6, no. 3, september 2011.

[6] Pei-Ling Chiu and Kai-Hui Lee,‖ Sharing Visual Secrets in Single Image Random Dot Stereograms.,‖
IEEE transactions on information forensics and security, vol. 6, no. 3, September 2013.

[7] 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.

[8] 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.

[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.

[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]Z. Eslami, S.H. Razzaghi, J. Zarepour Ahmadabadi, ―Secret image sharing based on cellular automata and steganography‖Elsevier Pattern Recognition 43 (2010) 397 – 404.

AUTHOR'S BIOGRAPHIES

Mangla Suresh Dantulwar BE(Elect) pursuing mtech in electronics and communication from priyadarshni Bhagwati College of Engineering, Nagpur maharastra, India, Published a research paper in ICQUEST-2016 (international conference on quality up-gradation engineering, science and technology), Manglamungilwar@gmail.com

Ms Puja V. Gawande Assistant Professor, of ECE Department, priyadarshni Bhagwati College of Engineering, Nagpur maharastra, India. She has completed M.Tech in Electronics Engineering (Communication) & B.E. in electronics and telecommunication engineering. She has experience of 6 yearsin the field of engineering and education. She has published 10 papers in various journals and conference
p.gawande07@gmail.com