Image Media Diversity in a Security Survival for Digital Image Sharing Schemes

Ekeshwari A. Rangari[1], Prof. Vishwajit K. Barbudhe[2]
PG Student, Department of Electronics and Telecommunication Engineering, Jagadambha College of Engineering & Technology,Yavatmal, India[1]
Asst. Prof., Department of Electronics and Telecommunication Engineering,Jagadambha College of Engineering & Technology,Yavatmal, India[2]
Ekeshwari.rangari@gmail.com[1], vbarbudhe@gmail.com[2]

Abstract- The previous technique of sharing the digital image i.e. Visual Secret (VSS)suffers from a transmission risk problem while sharing. To reduce such a problem, this paper gives the solution for solving it. The natural-image-based VSS scheme (NVSS scheme) is the proposed technique used to reduce the transmission risk problem and also to protect the participant while sharing the digital image. In NVSS scheme, one digital image, n-natural images and one carrier image are needed. The natural images(or natural shares) can be digital image and printed image.As the value of n increases, the NVSS scheme usesonly one noise share for sharing the secret image.With the help of extracted features, secret image will be encrypted where process carried by (n-1) natural shares. This encrypted result will be hided by using the QR code. The recovering of the secret image at the receiver will be done by the Share Extraction Algorithm or decryption process.The transmission risk is reduced by transmitting the natural images usingdiverse media.

Index Terms- Visual secret sharing scheme, Extended Visual Cryptography scheme, natural images, natural shares, secret digital image, etc.

1. INTRODUCTION

The Extended Visual Cryptography Scheme (EVCS) is a user-friendly scheme. Visual Cryptography (VC) is a special image encryption technique. It is different from traditional cryptography, because it does not need complex computation to decrypt. In the decryption process of this method, where without any complex cryptographic computation encrypted. Visual cryptography is a simple and powerful method which can provide high security for confidential information. In EVCS method, constructing a set of noise-like shares that are pixel expansion free. Then directly adds a cover image on each share via a stamping algorithm. So, the pixel expansion can be removed entirely and the message is encoded into a binary pattern. In each Share image, each message pixel is represented by a fixed size binary pattern which is called as a share, in which two of the four sub pixels selected randomly are black. The pixel expansion problem therefore consists because of sub pixels.

The disadvantages of Extended Visual Cryptography Scheme (EVCS) are as follow:

- In VSS schemes, the decryption process need not require computation; it may be difficult to analyze every share without computers.
- It would not investigate combinations and/or statistical data of pixels in shares.
- Storage and transmission of the shares requires an amount of storage and bandwidth resources which equivalent to the size of the secret times the number of shares.
- Expansion of the original pixels on the secret images in encryption, which makes lower level of contrast of the reproduced images.

Halftone shares are generated, because the secret information is embedded into the Halftone shares and it will give the result as recovered good quality of image. The shares contain many noise-like pixels or display low-quality images. Such shares are easy to detect by the naked eye. This meaningless shared data were embedded into the cover image to form stego images.

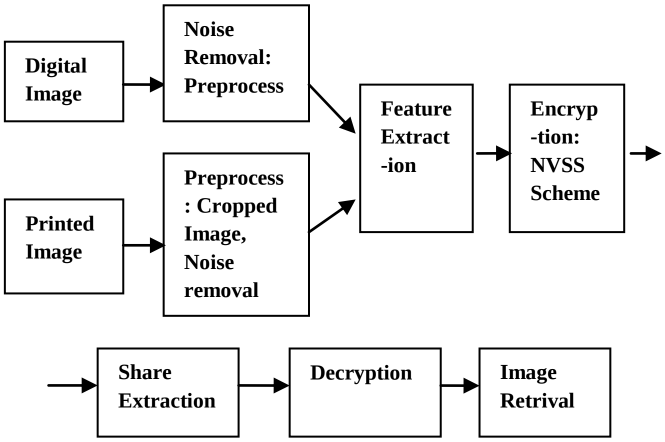
Digital Image
Noise Removal: Preprocess
Printed Image
Preprocess : Cropped Image, Noise removal
Feature Extract -ion
Encryp -tion: NVSS Scheme
Share Extraction
Decryption
Image Retrival

Fig. 1.The (n, n)-NVSS process

In this paper,a natural image based visual secret sharing (NVSS) scheme is proposed. The process of this (n, n)-NVSS scheme is shown in figure 1. The main aim of NVSS scheme is to securely share secret images in aided environments. Thisscheme is used to provide security to the secret image. We develop efficient encryption/decryption algorithms. These algorithms are applicable to digital and printed media.In this technique, 'n'natural images, one carrier image, and one secret image (n+2)are used for secret sharing. At transmitter side, the encryption process is done. For this, the natural images 'n' are distributed among the participants. For encrypting secret image,the key is required and is generated from 'n' natural images. This encrypted result will be hided by using the QR code. At the receiver,the recovering of the secret image will be done by the Share Extraction Algorithm or decryption process. The diverse media is used for transmitting the natural image which reduces the transmission risk problem.

2. RELATED WORK

The conventional schemes generate the noise-like shares are not user friendly and have the serious drawbacks. Hence, the researchers tried to overcome these drawbacks and enhance the friendliness of VSS schemes toparticipants. The simple andeasy cover images are added to noise-like shares for identification of the image. In a Simulated Annealing Algorithm for General Threshold Visual Cryptography, an optimization technique is proposed in order to encrypt binary secret images but whichmaximizes the contrast of recovered images. 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 our secret and other digital images, VSS schemes use digital media as carriers, which makes the appearance of the shares more variable and more user-friendly[1]-[7].

The Halftone visual cryptographyhave investigated meaningful halftone shares and emphasized the quality of the shares more than the quality of the recovered images. But these studies had the serious drawbacks as pixel expansion and contrast loss of original image, although the display quality of the shares was enhanced [8], [9].

The Color Extended Visual Cryptography Using Error Diffusion produces meaningful color shares with high visual quality but the colorful secret messages having low contrast.In random grid algorithm, the secret image is encrypted. It can adjust distortion to extremely small and also improves on the problems of decoding. Here, each pixel is associated a grey level ranging from white to black and each pixel is handled separately. The participants can correctly recover the image shared by the dealer. Any set of forbidden participants cannot gain any information on the value of the grey level of the shared pixel. [10]-[12].

The steganography technique isused to hide secret images in cover images and making the communication invisible. Digital shares have been successfully hidden by using steganography. Therefore, the hidden information and its carrier can be protected but each shadow reveals no information about the original image. Although the shares are totally prevented from being seen 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 [13]-[15].

3. THE PROPOSED SCHEME

In our proposed system, (n, n) - NVSS scheme has been implemented. Here both printed image and digital image have been taken to create the noise-like share. This natural image needed to be extracted feature for further process. Theencryption process can perform with the featured image and secret image. By applying (n, n) NVSS scheme,encrypted image or (n-1) natural share is developed.

The flow diagram of (n, n)-NVSS scheme is shown in figure 2. The feature extraction has been performed for two natural shares, so as the natural share's pixels are more efficiently compressed. These extracted features are encrypted with secret image. This process is performed by (n, n) - NVSS scheme. Then the encrypted image will be hided using share hiding algorithm. This process is performed with the Quick-Response Code (QR code) technology. QR code is a two-dimensional code. The QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. 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. In decryption process, share extraction algorithm is performed and at last, decryption algorithm applied to recover the secret image.

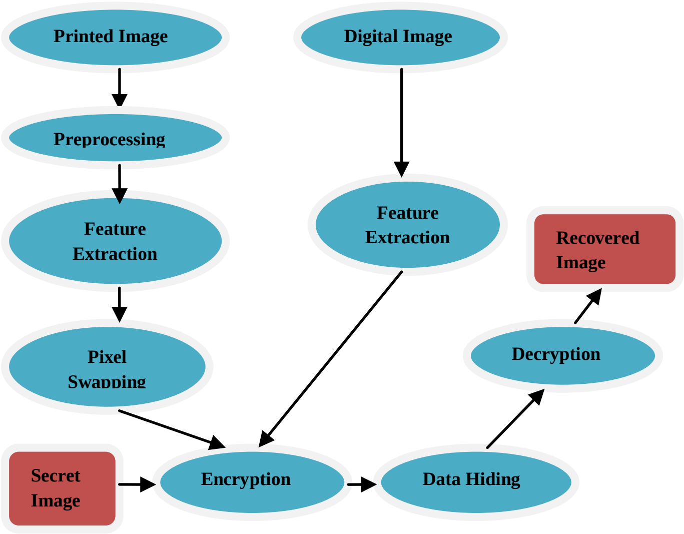

Fig. 2.The flow diagram of (n, n)-NVSS scheme

The objectives of the Natural-image-based Visual Secret Sharing Scheme are as follows:

- To preprocess the natural shares.
- To extract the features in the natural shares.
- To encrypt the secret image with the extracted features of natural shares.
- To perform data hiding and share extraction process.
- To decrypt and retrieve the original secret image.

4. MODULE DESCRIPTION

In the (n, n) - NVSS scheme, there are five modules Image Preprocessing, Feature Extraction, Encryption, Data Hiding, Decryption. They are described here,

4.1 Image Preprocessing

In our Proposed Method, Printed image will be preprocessed by cropping the input image. Cropping is performed by manually and stored for further processing. Then the cropped image will beresized with predicted size.

4.2 Feature Extraction

Feature Extraction is carried by Binarization of the natural share. With the binarization result, the stabilization process has been done. The stabilization process is used to balance the number of black and white pixels of an extracted feature image in each block. In this process, the number of black and white pixels in each block is equal. These clustered pixels have the same feature value. The chaos process is used to eliminate the texture that may appear on the extracted feature images and the generated share. The original feature matrix will be disordered by adding noise in the matrix.

4.3 Encryption:

Before Encryption process, pixels-swapping process is performed for printed image share which promotes tolerance of the image distortion caused by the image preparation process. The proposed (n, n)-NVSS scheme can encipher a true color secret image by n-1 innocuous natural shares and one noise like share. Input images include n-1 natural shares and one secret image. The output image is a noise-like share. Finally XOR operation performed for each color plane with the secret image.

4.4 Data Hiding:

In this data hiding section, Quick-Response Code (QR code) techniques are introduced to hide the noise-like share and reduce intercepted risk during the transmission. The code is printed on physical material and can be read and decoded by various devices, such as barcode readers and smart phones. It suitable for use as a carrier of secret communications. The string can be encoded to the QR code (a stego-share) by QR code generators. The QR code, which encodes meaningful information in both dimensions the vertical and horizontal directions. It can carry the information up to several hundred times the amount of data carried by barcodes

4.5 Decryption:

In the decryption process, the reversal of encryption process is done. Again feature extraction and pixel swapping performed to predict the secret image. When all ‘n’ shares are received, the decryption end extracts n-1 feature images from all natural shares and then executes the XOR operation to obtain the recovered image. That means the image decryption retrieves the original image from the encrypted one.

5. CONCLUSION

In this paper, the (n, n)-NVSS scheme 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. It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share; however, it can recognize the colorful secret messages having even low contrast. The major contribution of this study is that it reduces the pixel expansion problem and to increase the contrast. And also reduces the transmission risk problem because of diverse image media selected to share the secret image.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," inAdvances inCryptology, 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 Computer 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.

[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," Digital 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 sharing scheme with reversible steganography based on cellular automata," *J. Syst. Softw.*, vol. 85, no. 8, pp. 1852–1863, Aug. 2012.

[16] 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.

BIOGRAPHY

Ekeshwari A. Rangariis an Asst. Prof. in the Department of Electrical Engineering in Jagadambha College of Engineering and Technology, Yavatmal, Maharashtra (India). Her research includes Communication Engineering, Electronics Engineering, and Digital Electronics.

Prof. Vishwajit K. Barbudheis an Asst. Prof. in the Department of Electronics and Telecommunication Engineering in Jagadambha College of Engineering and Technology, Yavatmal, Maharashtra (India). His research includes Computer Networking, and Signal Processing. He has published forty papers in international journal, two papers in IEEE Xplore, and two papers in IEEE conference. He has attended six international conferences, six national conferences and six Short Term Training Program (STTP) one-week workshops. He has honored as an expert in international journal. He is working as a member and reviewer in international journal and international conference.