International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Encrypting Digital Images and Using Diverse Image Media for Sharing Digital Images

Animol T Joseph[1], Bismin Chacko[2]

[1]Final Year Student, M. Tech. (Cyber Security), KMP College of Engineering, Perumbavoor, Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering, KMP College of Engineering, Perumbavoor, Kerala, India

Abstract: ***Visual Secret Sharing Schemes hide a Secret image in shares that appear noise like picture or noiseless picture. VSS schemes suffer from a transmission risk problem while sharing contains Secret Images because it will awake suspicion and increase interception risk during transmission of the shares. The proposed system consists of 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. For this process the share contain arbitrary number of natural images and one noise like share. The natural shares can be photos or painted pictures in digital form or in printed form. The printed form images convert to digital form for the digital processing and these printed images can be send via postal or any other method. The noise-like share is initiated based on these natural shares and the secret image. The unaltered natural shares are diverse and safe, thus greatly reducing the transmission risk problem. The unaltered content of the natural images cannot easily detect by the suspicious.***

Keywords: Visual secret sharing, NVSS, Natural image, Transmission risk.

1. Introduction

Visual cryptography is a method used to encrypt a secret image into n shares in which every participant holding one or more shares. If one hold less than n share he can't able to reveal any information about secret image. Secret can be in the form of image, handwritten document, photograph. VSS (visual secret sharing) is the method to sharing and delivering secret images.

Today sharing the visual secret image is one of the problems in the computer aided environment. In the conventional share there is random meaningless pixels are used to share ,it will protect the secrecy of the image but it has two drawbacks:1) there is high transmission risk due to high noise like share;2) meaningless shares are not user friendly. If the number of shares increases it becomes more difficult to share the images.

Extended visual cryptography scheme is a user friendly scheme, the share contain many noise-like pixel or display low-quality images. This type of share can be easily detected by the naked eye so it can be tracked by the attackers.

Steganography is another method to conceal the secret image in cover image. This type of stegno-image can be detected by the steganalysis method. Natural-image based VSS (NVSS) scheme is used to reduce the transmission phase. Conventional scheme use only one carrier for sharing the image, in case of NVSS scheme there is a possibility of using diverse image media for sharing digital image. In the NVSS scheme can share the digital image in n-1 arbitrary share natural image and one share. In the proposed system, it does not alter the content of natural image. It extracts the features from the natural image. The unaltered natural share reduces the interception probabilility. The noise-like share concealed by data hiding technique to increase the security level during the transmission phase.

2. The Proposed System

2.1 Background

One-time pad (OTP) method is used to protect the data from the miscellaneous user. In that, each bit or character of the plain text is encrypted by modular addition with the bit pr character from the secret key and resulting cipher text. The cipher text is send to the receiver, at the receiver end the decryption take place by the same secret key used the sender.

Instead of using the secret random key, here extract the secret key from the arbitrarily picked natural image in (n,n)-NVSS scheme. The natural image and the cipher image is distribute to the participants. In the decryption end the secret key will extract from the natural image and then the secret image can recover from that.

2.2 The proposed (n,n)-NVSS Scheme

Fig.1 shows the encryption process of the system. There are main two process 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.The feature images (F1,…, F*n*-1) that were extracted from the same natural image.

In the encryption phase, the *n*- 1 feature images (F1,…, F*n*-1) and the secret image execute the XOR operation to generate one noise-like share S.

Decryption process consists of opposite to the encryption. In this, 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.

3. The Proposed Algorithms

3.1 Feature Extraction Process

This section describes the feature extraction module that extracts feature images from the natural shares.

3.1.1 The Feature Extraction Module

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.

Feature extraction module consists of three processes—binarization, stabilization, and chaos processes. In the binarization process binary feature matrix is extracted from natural image N.Then, the stabilization balances 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

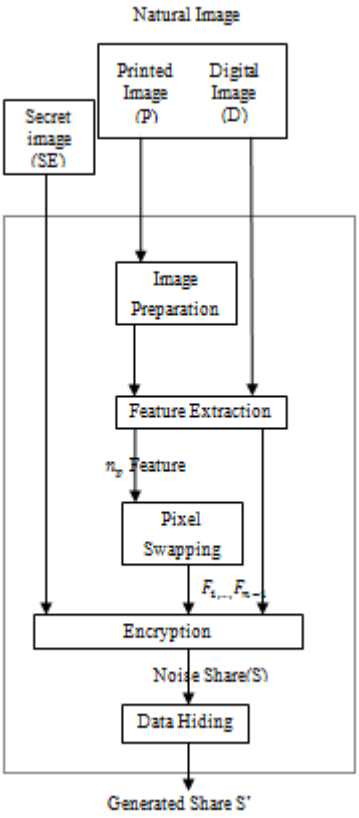

Figure 1: Encryption process

same block is select as the threshold. Hence, for each block, the extraction function of pixel (x, y) of N is defined as follows:

$$f^{x,y}=F(H^{x,y})=\begin{cases} 1, & H^{x,y} \geq M, \\ 0, & otherwise. \end{cases} \quad (1)$$

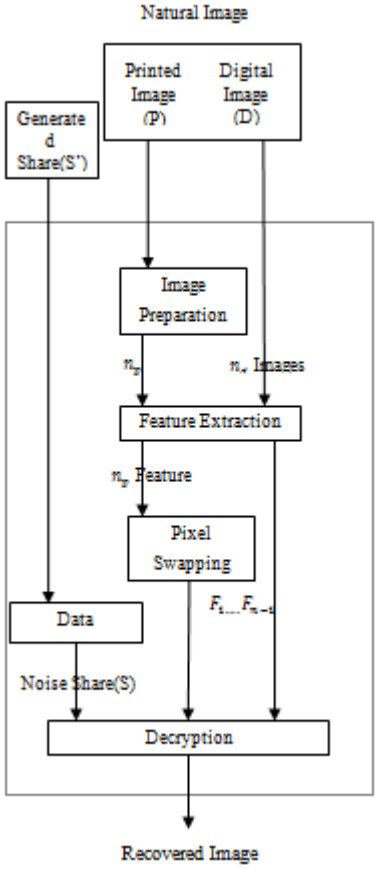

Figure 2: Decryption process

Stabilization process is used 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

$$Q_s=\left(\sum_{\substack{\forall x1 \leq x \leq x_b \\ \forall y_1 \leq y_2 \leq y_b}} f^{x,y}\right) \quad (2)$$

The chaos process is used to eliminate the texture that appears on the extracted feature images and the generated share.

3.1.2 Image Preparation And Pixel Swapping Process

Image preparation is used for the preprocessing of the printed image and the pixel swapping process is used for the post processing of the digital image. Image preparation process is shown in the figure.

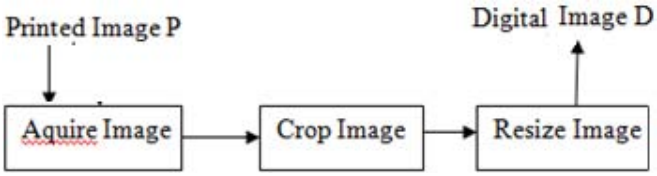

Figure 3.5: Flow of the image preparation process.

The content of the image is acquired 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 crop the extra image. Finally resize the image for the same dimension of the natural image.

3.1.3 Encryption / Decryption algorithm

The proposed (*n*, *n*)-NVSS scheme can encipher a true-color secret image by *n*- 1 natural shares and one noise like share.

Before encryption (resp. decrypt) of each bit-plane of the secret image, the encryption algorithm first extracts *n*-1 feature matrices from *n* - 1 natural shares. Then the bit-plane of the secret image feature matrices execute the XOR operation. Therefore, to encrypt (resp. decrypt) a true-color secret image, the encryption (resp. decryption) procedure must be performed iteratively on the 24 bit-planes.

The input natural shares (N1, ….. , N*n*+1_)of the scheme include np printed images and nd digital images (np > 0, nd > 0, and *n* =np +nd + 1). The np printed images must be processed and transformed into digital form in the image preparation process.

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.

3.1.4. Hide the Noise-Like Share

QR Code (Quick Response) is used to hide the image. QR code is a two dimensional code which encodes meaningful information in both dimensions and in the vertical and horizontal directions. The code is printed on physical material and can be read and decoded by various devices.

Figure: Example of a QR Code

The amount of data that can be stored in the QR code symbol depends on the data type. There are two steps in the encoding process First, transform pixels on the share into binary values and represent the values in a decimal format. Second, encode the decimal values into QR code format.
A single QR code contain maximum of 22627 data bit. Consider the maximum QR code size is C_H, the amount of information in the share is denoted as C_S then the capacity ratio C_R is$[C_S/C_H]$. If C_R >1 then the information can hidden in QR code. If C_R value is less than one then it cannot hide inside the QR code. We need to encode the information which wants to hide. Huffman coding is a popular method for compressing data with variable-length codes. Huffman coding technique is able to encrypt and compress the image contain primary information about the object. Huffman coding is used to compress the encrypted image. The data can then store in the encoded Quick Response (QR) code.

The first Huffman code compression reduces the image into a series of bits. The Huffman code then can be represented 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 group is then converted into integers. This is advantageous since the QR code is character limited.

In 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.

4. 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 protect from the attackers. The media that include *n*-1 randomly chosen images are unaltered in the encryption phase. the feature of the secret image and the randomly chosen images are taken Therefore, they are totally innocuous. The number of participants does not involve in share, ie the number of participants can be increase.

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, attempt to share images via heterogeneous carriers in a VSS scheme. Second, introduce hand-printed images for images-sharing schemes. Thirdly, useful 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 evaluates is a better option for high scale secure communication. The greater chaos does not slow down the system. But it takes more time when it comes to large size data. This increases the computational complexity and overhead. Hence it is required to find a solution.

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 Profile

Animol T Joseph received the B.Tech degree in Information Technology from Anna University Chennai in 2012 and currently pursuing final year M. Tech degree in Computer Science and Engineering with specialization in Cyber Security from KMP College of Engineering, Perumbavoor.

Bismin Chacko received the B Tech and M Tech degrees in Computer Science and Engineering from MG University, kottayam in 2011 and 2013 respectively. Currently working as Assistant Professor in Computer Science and Engineering Department, KMP College of Engineering, Perumbavoor. Research Interest includes MANETs Security, Information Security and Image Processing.