Image Hiding Using Diverse Image Media

Prajakta Nikam
Department of Information Technology,
MIT college of Engineering,
Pune, India
nikam.prajakta7@gmail.com

Kishor Kinage
Professor, Department of Information Technology, MIT college of Engineering,
Pune, India
kishor.kinage@mitcoe.com

***Abstract* -Visual secret sharing (VSS) schemes encrypt secret images in shares. Shares are printed on transparencies and look like noise pixels or as meaningful images. These shares are suspected and increase possibility of attack during transmission of the shares. Hence, VSS schemes have a transmission risk problem. As number of shares increases there is problem of share management. To solve this problem, we proposed a Digital-image-based VSS scheme (DVSS scheme) that shares secret images via digital and printed images to secure the secret during the transmission phase. The proposed (*n, n*) - DVSS scheme can split one digital secret image over *n* - 1 arbitrary selected digital and printed images to generate one noise-like share. The unaltered printed and digital images are diverse and safe, thus greatly reduce the transmission risk problem. We also propose data hiding techniques to hide the noise like share. Data hiding helps to minimize the problem of transmission risk and management of share. Here we are using two data hiding algorithm The algorithms are QR code and DLFSR. We are trying to analyze performance DVSS for QR code and DLFSR .**

Keywords- Visual secret sharing scheme, transmission risk, extended visual cryptography, halftone images

I.INTRODUCTION

Visual Cryptography is a secret-sharing method that encrypts a secret image into several shares but does not requires computer or calculations to decrypt the secret image. The secret image is recovered simply by overlaying the encoded shares. Visual cryptography technique is invented by Moni Nair and Adi Shamir in 1995[1]. Visual secret sharing scheme,where an image is broken into n shares. All n shares could decrypt the image, while any n − 1 shares does not give any idea about the original image. Each share was printed on a different transparency, and decryption was performed by overlapping the shares [2].

Secret images can be of various types: photographs, images and others. Sharing secret images is also called as a visual secret sharing (VSS) scheme. This scheme has some disadvantages: Management of shares become difficult as number of share increase. These random looking noise like shares are vulnerable to attack by attacker in middle so there is high transmission risk. Extended visual cryptography scheme (EVCS) is visual secret sharing scheme solves the problem of shares management. EVCS uses meaningful cover images to hide the share. But while recovering secret image extra noise is introduced in image and degrade the quality of secret image. Using steganography techniques, secret images can be hidden in cover images that are halftone gray images and true-color images However, the stego-images still can be revealed by steganography analysis methods. A method for reducing the transmission risk is an important issue in VSS schemes.

II. RELATED WORK

Visual Cryptography (VC) is a method for sharing secret image. This method was proposed by Naor and shamir [1]. VC scheme divides the secret image into share images. This share images are look like a noise images. The shares are printed on transparencies. By stacking transparencies directly, the secret images can be recovered and visible to human eyes without any computational devices and cryptographic knowledge. One share cannot recover secret image. VC is a good solution for sharing secrets when computer is not used for the decoding process. This scheme has some disadvantages: Management of share become difficult as number of share increase. These random looking noise like shares are vulnerable to attack by attacker in middle so there is high transmission risk.

Extended visual cryptography scheme (EVCS) is another visual cryptography scheme first introduced by Naor[3].EVCS has meaningful shares and VCS contains random shares. EVCS takes secret image and n original shares images as input and outputs n shares. All n shares are meaningful images. Only qualified subset of shares can recover the secret image. Any forbidden subset of share cannot obtain any information of secret image. EVCS overcome the disadvantages of VCS because all shares in EVCS are meaningful images hence these shares are less vulnerable to attack. Bad visual quality of the shares and recovered secret image is one of the disadvantage of EVCS. Another disadvantage is that pixel expansion is large and requires complementary share images.

Embedded EVCS is a visual cryptography scheme invented by Feng Liu and Chuankun Wu. Secret image is encrypted by taking n gray scale image as input and convert them into n covering share. Covering shares are splited into blocks of s subpixel. Mo and M1 are matrices of a traditional VCS. Rows of M0 and M1 are embedded into the blocks of covering share. Finally outputs n shares. Concept of Dithering matrix is used to generate covering share. Embedded EVCS has many advantages such as it deals with gray scale input image, has smaller pixel expansion, and does not require complementary share images.

Halftone visual cryptography is a technique for visual cryptography invented by Zhi Zhou [4].In this technique halftoning method such as the error diffusion on a grey level image is used to obtain halftone image (HI) .This image is given to first participant. Complementary image $(\overline{HI})$ is obtained by reversing all black/white pixels of HI to white/black pixels and $\overline{HI}$ assigned to second participant. In each share secret pixel is encrypted into halftone cell. Select only two pixels from each share .Pixel position is same in each share. These selected pixels are secret information pixels are needed to modify based on following rule:

a) If pixel is white, a matrix is randomly selected from the collection of matrices Co of conventional VC.

b) If pixel is black, matrix is randomly selected from C1 .

Halftoning method is better than conventional VC method for quality of share.

III. PROPOSED WORK

Here, we propose a methodology to hide secret image using *n-1* printed and digital images. Different steps like image preparation, feature extraction, encryption/decryption and share hiding are used to hide the secret. These steps are explained in following subsections.

A.Image Preparation Process

In image preparation process images can be captured by popular electronic device, such as digital cameras. The type of acquisition devices and the parameter settings of the devices must be same in encryption and decryption process. The next step is to crop the images. The images are resized.

Here, our main objective is to reduce the transmission risk of shares.In next subsection we give description of encryption process of the proposed (*n, n*)-DVSS scheme, $n \geq 2$. Encryption process has two main phases: feature extraction and encryption.

B. Feature Extraction

In the feature extraction phase, 24 bit binary feature images are extracted from each natural share. The natural shares has n_p printed images and n_d digital images, where $n_p \geq 0, n_d \geq 0, n_p + n_d \geq 1, n = n_p + n_d + 1$[2].

Feature extraction process extract features from images. Feature extraction has three main phases: Binarization, Stabilization, Chaos. Notations are defined as follows:

- N shows a natural share.
- b denotes size of block where b $\in$ even
  (x, y) are the coordinates of pixels in the secret image and natural shares $1 \leq x \leq$ w, $1 \leq y \leq$ h
- (x_1, y_1) are the coordinates of the left-top pixel in each block.
- $p_\phi^{x,y}$ shows the value of color ϕ, $\phi \in$ {R,G,B} for pixel (x, y) in natural share N, $0 \leq p_\phi^{x,y} \leq 255$.
- $H^{x,y} = p_R^{x,y} + p_G^{x,y} + p_B^{x,y}$.
- M denotes the median of all pixel values $(H^{x_1,y_1}, ..., H^{x_b,y_b})$ in a block of N.
- $\boldsymbol{F}$ denotes feature matrix of N, the element $f^{x,y} \in F$ denotes the feature value of pixel (x, y). If the feature value $f^{x,y}$ is 0, the feature of pixel (x, y) in N is defined as black. If $f^{x,y}$ is 1 the feature of pixel (x, y) in N is defined as white.

In the binarization process, the binary feature value of a pixel can be calculated by using a simple threshold function f with a set threshold. The median value M is used to calculate the threshold. Hence, $f^{x,y}$ is calculated as $f^{x,y}$ is 1 if $H^{x,y} \geq M$ otherwise 0 [2].

Main objective of stabilization process is balancing the number of black and white pixels of an extracted feature image in each block. The number of unbalanced black pixels Q_s can be estimated as follows[2]:

$$Q_s = (\Sigma f^{x,y}) - \frac{b^2}{2}$$

Q_s pixels whose $f^{x,y} = 1$ is randomly selected and then the value of these pixels is set to 0. This process used to balance number of black and white pixels in each block .

The chaos process is used to remove the texture that may present in the extracted feature images and the generated share. Noise is added into original feature matrix which gives disordered matrix. First, randomly choose Q_c black feature pixels $(f^{x,y} = 0)$ and Q_c white feature pixels $(f^{x,y} = 1)$ from each block, then change the values of these pixels. P_{noise} be the probability to add noise in the matrix. The value of Q_C is calculated by using following formula[2]:

$$Q_C = \frac{b^2}{2} \times P_{noise}$$

C. Encryption/Decryption Process:

Before encryption we first extract $n-1$ feature matrices. All feature images are combined to make one feature image with 24-bit/pixel color depth. In the encryption phase[2], all *n*- 1 feature images with 24-bit/pixel color depth are XOR with secret image to generate one noise-like share S with 24-bit/pixel color depth. Finally share S is hidden by using data hiding

techniques named as QR code and DLFSR. Data hiding techniques reduce the transmission risk problem. Fig.1 and Fig.2 shows encryption and decryption process respectively.

Final output of encryption process is share S' also called as generated share. Input to decryption process include $n-1$ feature images and the generated share S'. The output is recovered image

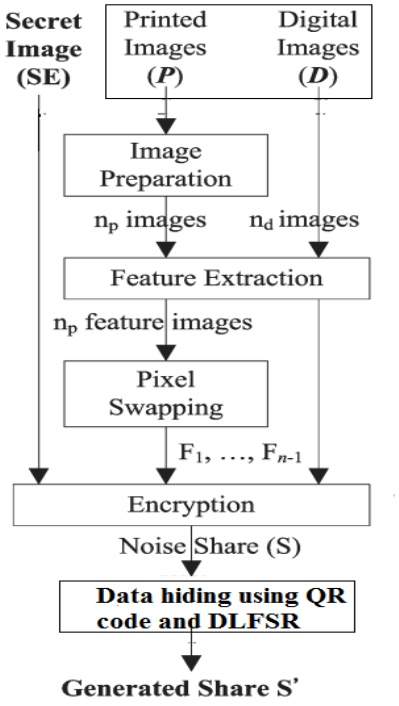

Fig 1.Encryption process of (*n, n*)-DVSS scheme

The notations used in the DVSS scheme Encryption/decryption process are as follows:

- ϕ shows a color plane of an image, $\phi \in$ {R,G,B}.
- S is the input image; S_ϕ denotes an element of S in color-plane ϕ.
- S' is the output image; S_ϕ denotes an element of S in color-plane ϕ.
- FI_α is a feature image of natural share N_α.
- $FI_{\alpha,\phi}$ is an element of feature images in color-plane ϕ.
- ρ denotes the seed of the random number generator G.

Input to encryption/decryption process include n_p printed images and n_d digital images.

Step 1: Initializes random number generator G by seed ρ and it is used in feature extraction and pixels-wapping processes.

Step 2: Set all feature images $FI_{\alpha,\phi} \leftarrow 0$

Step 3: Feature extraction is used to extracts a binary feature matrix from a natural share .One feature image with a 24-bit depth per pixel is extracted from each natural share.

Step 4: Extracted matrix is added to corresponding bit and color planes of a feature image.

Step 5: Pixel-swapping process is performed on each feature image. Pixel-swapping is performed by randomly selecting a pair of pixels and swapping the values of two pixel in a feature image

Step 6: Perform XOR operation between input image S and all feature images .

Step 7: Output image S'

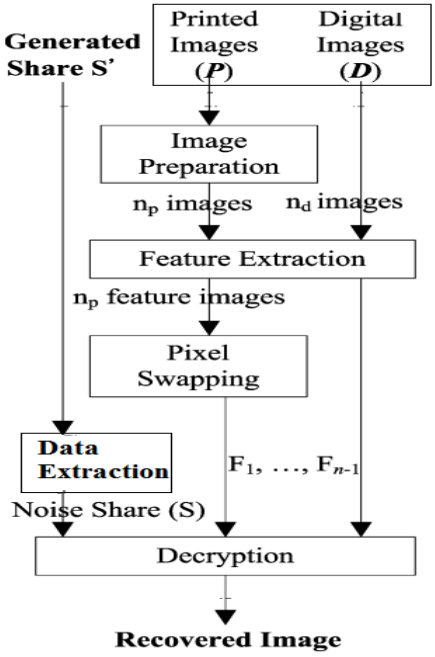

Fig 2. Decryption process of *(n,n)*-DVSS scheme

D.Share Hiding

1) Quick Response code

Here, Steganography and the Quick-Response Code (QR code) [2] are used to hide the noise-like share .This helps to reduce transmission risk problem. QR code encodes meaningful information in both dimensions as well as in the vertical and horizontal directions. QR code carry hundred times more data than barcodes. It is decoded and read by various devices, such as smart phone and barcode readers .

Notation for share hiding algorithm are defined as follows:

- C_S is the amount of information in the share
- C_H is the maximum capacity of the selected hiding media and where $C_S \geq C_H$.
- The capacity ratio $C_r = [C_s / C_H]$.

- $C_r = 1$ means the share can be totally hidden in the hiding media.
- If $C_r > 1$ then the share cannot be hidden in the media. Stego bit is formed by encoding C_r consecutive bits into a single bit . Majority of C_r bits decides the value of stego-bit.

In the share-hiding process if $C_r > 1$ then information in the feature matrix F is reduced to fit within the capacity of C_H .Remove C_r consecutive bits from the front of string S_F .Calculate the value of stego-bit S_b by majority. The stego-bit is appended to bit string F_{QR} . F_{QR} is converted to the numeric string S_{QR}.

The share extraction is used in the decryption phase, to extract hidden information from the stego-share. This process extract share matrix F from numeric string S_{QR}.

2) Data hiding using Linear feedback shift register (DLFSR)

Steganography is data hiding technique that hides data in images. Data is hidden inside image using least significant bit (LSB) variation also called as LSB embedding[11]. In LSB embedding changing the LSB will only modify the integer value of the byte by one. This minute change is not observable. Image appearance is not changed.

The difference between DLFSR and LSB embedding is that DLFSR uses seed ranking based on suitability of cover images .Information about L.F.S.R can be seen in [12] . Follow the below procedure to hide the noise share inside cover image:

Step1:The user first encrypts data using the recipient's El Gamal public key.

Step2:Calculate LFSR

Step3:Set the initial value randomly for m-bit L.F.S.R, also called as a seed.

Step4:Using LFSR and seed generate random permutation

Step5:Permute the encrypted data using the permutation obtained above

Step6:Permuted encrypted data and LFSR information is embedded in pixels of cover image

IV. CONCLUSION

In this paper we propose (*n, n*)-DVSS scheme, that can hide a digital image using diverse image media. The secret image is hidden by using $n-1$ randomly chosen images. Therefore, they are less vulnerable to attack. VSS scheme has problem of management of shares. DVSS scheme generate only one share. It also reduces the transmission risk problem so DVSS is effective than VSS scheme .We are developing methods to store the noise share.These methods are QR code and DLFSR.. Here we are trying to analyze performance of DVSS for QR code and DLFSR. Parameters for performance analysis are size of encrypted image, time for encryption and decryption, size of recovered image.

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]. K. H. Lee and P. L. Chiu, "Digital Image Sharing by Diverse Image Media" IEEE Trans. Inf. Forensics Security, vol. 9, no. 1, Jan. 2014.

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

[4]. 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.

[5]. Subba Rao Y.V , Brahmananda Rao S.S , Rukma Rekha N ," Secure Image Steganography based on Randomized Sequence of Cipher Bits",Eighth International Conference on Information Technology,2011

[6]. 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.

[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]. 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.

[9]. 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.

[10]. 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.

[11]. R. Chandramouli, N. Memon, "Analysis of LSB based image steganography techniques," Image Processing, vol. 3, pp. 1019-1022, October 2001.

[12]. Alfred J. Menezes, Paul C. van Oorschot , and Scott A. Vanstone "Handbook of Applied Cryptography" CRC Press 1996.